AGENCIA
DE
PROTECCIÓN DE DATOS

MEMORIA
2000

MEMORIA DE 2000 - PRESENTACIÓN

El año 2000 ha venido marcado, en materiade protección de datos, por dos hechos de especial trascendencia.La entrada en vigor de la Ley Orgánica 15/1999, de 13 dediciembre, de Protección de Datos de Carácter Personal,en el mes de enero, que sustituyendo a la Lortad, se convierteen el principal texto normativo sobre la materia en nuestro país, y la Sentencia del Tribunal Constitucional 292/2000, de fecha30 de noviembre de 2.000, por la que el órgano supremode interpretación de nuestra Constitución vienea definir el derecho a la protección de datos, como underecho independiente en nuestro sistema constitucional. Estepronunciamiento del Tribunal Constitucional ha venido a coincidiren el tiempo con la proclamación de la Carta de DerechosFundamentales de la Unión Europea, hecha en la Cumbre deNiza el 7 de diciembre del mismo año. El artículo8 de la citada Carta establece el derecho a la protecciónde datos también como un derecho independiente al que definey configura con gran precisión.

En tono normativo menor, aunque relevantepor la repercusión que ha tenido en nuestra sociedad, principalmenteen los titulares de ficheros informatizados, debe señalarseque en el 2.000 entró en exigencia la normativa que elReal Decreto 994/1999, de 11 de junio, preveía para todoslos ficheros informatizados en cuanto a la implantaciónde medidas de seguridad de nivel básico y la posteriorobligación de implantar medidas de seguridad de nivel mediopara determinados ficheros. Ello ha supuesto en la prácticaque con motivo de dar cumplimiento a la implantación demedidas de seguridad algunos responsables de ficheros hayan descubiertolas restantes exigencias legales y con tal motivo se han puestoal día en el cumplimiento de todas ellas.

El nuevo marco legislativo ha conllevado lógicamente el incremento de las acciones de la APD para difundir el conocimientode la normativa aplicable y facilitar su mejor comprensión,no sólo a los ciudadanos, sino también a los titularesde ficheros y encargados de tratamientos que han de ajustarsea su cumplimiento.

En este orden de cosas el Director de la APD ha impartido diversas conferencias y ponencias sobre temas variosque derivan de la legislación de protección de datos,en cursos, cursillos, seminarios, jornadas e incluso cursos dedoctorado que organizadas por diversas instituciones, se han venidocelebrando a lo largo del pasado año por toda la geografíade nuestro país. En total el número de intervencionesha sido 39, lo que supone una conferencia o ponencia cada semana, si se toma como referencia los días hábiles.

Otro tipo de actos, que tenían como finalidad dar a conocer las actividades de la APD, como es elcaso de la presentación de la Memoria de la misma, se hanaprovechado asimismo para difundir la nueva legislación.La Memoria de 1.999 se presentó el 15 de junio de 2.000en la sede del Consejo de Consumidores y el acto estuvo precedidode una exposición por el Director de la Agencia de lasnovedades legislativas y un fructífero intercambio de opinionescon los miembros de aquella institución.

Con el mismo fin de dar a conocer la nueva normativa y facilitar su cumplimiento a grandes colectivos sefirmaron el pasado año sendos protocolos de colaboracióncon la Unión Profesional que engloba a los Consejos Generalesde Colegios Profesionales, con el Consejo Superior de Cámarasde Comercio, Industria y Navegación y con el Consejo Generaldel Notariado, a petición de sus órganos rectores.

La preocupación de todos por el derecho a la protección de los datos personales es cada díamayor y se refleja también en el ámbito universitariocon la organización de cursos de especializacióny títulos de master. Con el fin de atender a la formaciónde los alumnos que acuden a los mismos, la APD ha firmado convenioscon la Universidad Complutense de Madrid y con la Universidadde Comillas para recibir a sus alumnos en períodos de prácticascon carácter permanente. También, referido al cursopasado, se firmó un Convenio con la Universidad de Pau(Francia) y el Centro de Estudios Europeos. El interés de los ciudadanos por mejorconocer el alcance del derecho a la protección de datosse hace palpable en las casi 20.000 consultas formuladas a laAPD a través del área de Atención al Ciudadanoy los más de 1.000.000 accesos que ha tenido la páginaweb de la Agencia a través de Internet, lo que es causadeterminante de nuestra preocupación por su actualizaciónpermanente y el dotarla de nuevos contenidos útiles.

Las jornadas que habitualmente organiza la APD con alguna institución para profundizar en el estudiode algún tema de actualidad en materia de protecciónde datos tuvieron el año 2.000 como sede la UniversidadPública de Navarra con la que se coorganizaron. Se dedicaronlas Jornadas al estudio de la "Protección de datosen el sector de las Telecomunicaciones con especial referenciaa Internet". Como es ya conocido nuestro legislador ha transpuestoal Derecho interno la Directiva 97/66/CE relativa al tratamientode los datos personales y a la protección de la intimidaden el sector de las telecomunicaciones, a través de LeyGeneral de Telecomunicaciones de 24 de abril de 1.998 y del RealDecreto 1736 de 31 de julio de 1.998. Esta legislación,que no sustituye a la general en materia de protecciónde datos, sino que la complementa en el sector de las telecomunicaciones,requiere sin duda dedicarle un especial estudio dada la complejidadde la misma y las obligaciones que comporta para los titularesde ficheros y tratamientos. A esto se dedicaron los trabajos deestas Jornadas, que sirvieron además para acercar la APDa la Comunidad de Navarra.

Se continuó también en el pasado año con nuevos planes sectoriales de Inspecciónccon el fin de conocer la adecuación de diversos sectoresa las exigencias de la LOPD, así como sus concretos problemas,y en definitiva ayudarles a mejor cumplir con la normativa sobreesta materia a través de unas recomendaciones que al finalse remiten al sector inspeccionado para su difusión a todossus miembros. Así se hicieron públicas las recomendacionesdirigidas a los sectores inspeccionados el año anterior:Agencia Estatal de Administración Tributaria, DirecciónGeneral de Tráfico, Sector de Investigación privada,sector sanitario, referido al Registro Nacional de SIDA, HospitalMilitar Gómez Ulla y Hospital Psiquiátrico de Fontcalent.En el año 2.000 se terminó el plan de inspecciónal sector de la telefonía móvil iniciado el añoanterior y se llevaron a cabo nuevos planes de inspecciónen los sectores del comercio electrónico, la gestiónde

tarjetas en grandes superficies comerciales y el Consorciode Compensación de Seguros.

De las recomendaciones producidas en el 2.001 dará cuenta la próxima Memoria.

En el año 2.000 he comparecido en dos ocasiones ante la Comisión Constitucional del Congresode los Diputados. La primera comparecencia, a petición propia, tuvo como objeto la presentación de la Memoriadel ejercicio anterior, así como responder a las iniciativasde los Grupos Parlamentarios. De los temas planteados destacaronlas referencias a la entrada en vigor de la Ley Orgánica15/1999 y a su compatibilidad con las normas que desarrollaronla LORTAD. También se hizo especial hincapié enla necesidad de fomentar actuaciones informativas para facilitarel conocimiento de la nueva Ley.

La segunda, a solicitud de los Grupos Parlamentarios se centró, básicamente, en el análisis yconsecuencias de la Sentencia 292/2000 del Tribunal Constitucional.

Estas comparecencias consolidan los precedentes sobre el control parlamentario de las actividades de la Agenciay suponen una exigencia adicional respecto de su actuación independiente.

La actividad de la APD, en sus diversas funciones ha experimentado un notable incremento en el año 2.000.Así se ha producido un avance en la demanda de inscripcionesde ficheros, alcanzando la cifra de 10.512 solicitudes de inscripción de ficheros, lo que ha supuesto la realización de 25.760operaciones de inscripción, dado el que cada solicitudcontiene más de una notificación a efectos registrales.Si comparamos las inscripciones del año 2.000 con el mismoperíodo del año anterior veremos que el aumentollega a la cifra del 400 %. La globalización que experimentala sociedad en general y especialmente la realidad que suponela Unión Europea tiene su reflejo también en lastransferencias internacionales de datos declaradas a la Agenciaque alcanzó la cifra de 1.352. Ello supone que debemospermanecer vigilantes a fin de que los ficheros que se transfiereno los tratamientos que se realizan fuera de nuestras fronterasse lleven también a cabo con total cumplimiento de lasgarantías legales.

Del mismo modo, las denuncias de los ciudadanos,y consecuentemente las actuaciones previas de inspección y subsiguiente tramitación de procedimientos, tanto contraresponsables de ficheros privados como en el supuesto de aquellosde titularidad pública han experimentado un creciente incremento.Basta señalar que el Director de la APD dictó enel pasado año un total de 622 resoluciones definitivasen vía administrativa, consecuencia de denuncias, procedimientosy recursos de reposición. Ello generó la imposiciónde multas por importe de 1.737.600.000,- pesetas a responsablesde ficheros de titularidad privada y la incoación de 31nuevos expedientes a diversas Administraciones Públicas.

La actividad desarrollada durante el año2.000 en la esfera internacional ha sido intensa y creciente.Dentro de ella caben destacar las reuniones de trabajo con Delegacionesde Autoridades de Protección de Datos de Nueva Zelanday Polonia, esta última con encuentros en Varsovia y Madrid.

Se ha participado asimismo en las reuniones celebradas por el Grupo de Trabajo del artículo 29, enel que participan todas las Autoridades de control de datos delos países miembros de la Unión Europea, siendosus principales funciones las de asesorar a la Comisiónde las Comunidades en estas materias y encontrar estandares parala armonización de las legislaciones internas. Tambiénse ha asistido a las reuniones de las Autoridades Comunes de Controlestablecidas en los Convenios Schengen y Europol y las del Grupode Protección de Datos en el ámbito de las Telecomunicaciones(Grupo Berlín).

Por otra parte, es importante destacar la participación de la APD en la Conferencia de Primaverade los Comisionados Europeos de Protección de Datos quese celebró en abril en Estocolmo (Suecia) donde presentamostres ponencias, así como en la Conferencia Internacionalde Autoridades de Protección de Datos que tuvo lugar enVenecia (Italia) en el mes de septiembre y en donde la APD contribuyódirectamente con dos ponencias.

Es de interés mencionar tambiénla reunión celebrada por el Grupo de Ficheros Policialesasí como del Grupo de Proyecto de Protección deDatos Personales (CG-PD) en el seno del Consejo de Europa quese llevó a cabo en otoño en París.

En el mes de noviembre se produjo el I Encuentro Ibérico entre las Autoridades de Protección de Datosportuguesa y española, celebrada en Evora (Portugal) enel marco de un proyecto de cooperación mutua entre ambas.Se estudiaron conjuntamente los temas de mayor actualidad y queresultan más comunes para ambos países, y a la vistade los positivos resultados de esta reunión se acordómantener una cooperación constante y fluída y mantenerestos encuentros de estudio al menos con periodicidad anual.

Por último cabe resaltar que la creación de la Oficina Checa de Protección de Datos Personales trajocomo consecuencia que las Autoridades de dicho país pusieranen marcha un Proyecto de Hermanamiento con un organismo similarde algún Estado Miembro de la UE. La Agencia de Protecciónde Datos española dado el interés de las Autoridades

checas, se presentó como candidata, resultando adjudicataria del mismo. Por ello liderará el proyecto consistente enla adecuación de la legislación de protecciónde datos de la República Checa y de la estructura y funcionesde su Autoridad de Control a las exigencias de la legislacióncomunitaria europea sobre la materia. Es una realidad que ha podidoconstatarse el pasado año, el que la legislaciónespañola en materia de protección de datos y elfuncionamiento de la APD, como Autoridad de Control, se han convertidoen punto de referencia de los países del centro y el estede Europa que aspiran a su incorporación a la UniónEuropea.

Como Director de la Agencia de Protección de Datos aspiro a que esta Memoria sea útil para quienla lea, consiga transmitir las funciones llevadas a cabo por laAgencia durante el período al que la misma se refiere yen definitiva reciba el beneplácito de los ciudadanos.En todo caso, la labor llevada a cabo por la APD ha resultadoposible gracias a la entrega de los funcionarios que en la mismatrabajan, que, a pesar de su reducido número, han sabidouna vez más multiplicar sus esfuerzos para que todos puedansentir cada día un poco mejor defendido su derecho a laprotección de datos. Madrid, junio de 2.001

Juan Manuel FernándezLópez

Director de la Agencia de Protecciónde Datos

MEMORIA DE 2000 - FUNCIONAMIENTO DE LA AGENCIA

I. CONSEJO CONSULTIVO

* El Consejo Consultivo, previsto en el artículo 38 de la LO 15/99 de Protección de Datos de Carácter Personal, y en los artículos 18 a 22 del Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia de Protección de Datos, se configura como órgano colegiado de asesoramiento del Director del Ente Público, cuyos cometidos se centran en emitir informe en todas las cuestiones que le someta el Director de la Agencia y formular propuestas en temas relacionados con las materias de competencia de ésta.
* En su composición, está integrada por los siguientes miembros:
* Presidente:
* D. Juan Manuel Fernández López, Director de la Agencia de Protección de Datos.
* Vocales:
* D. Carlos Navarrete Merino, Diputado propuesto por Congreso de los Diputados
* Dª. Rosa Vindel López, Senadora propuesta por el Senado
* D. Álvaro de la Cruz Gil, Vocal de la Administración Local propuesto por la Federación Española de Municipios y Provincias.
* D. Eloy Benito Ruano, Vocal propuesto por la Real Academia de Historia
* D. Antonio Pérez Prados, Vocal propuesto por el Consejo de Universidades.
* Dª. Alberto Perales Albert, Vocal propuesto por el Consejo de Consumidores y Usuarios.
* Dª. Elena Gómez del Pozuelo, Vocal del sector de ficheros privados propuesta por el Consejo Superior de Cámaras de Comercio, Industria y Navegación.
* Dª Rosa García Ontoso Directora de la Agencia de Protección de Datos de la Comunidad de Madrid, en representación de esta Comunidad Autónoma. Incorporada en el consejo celebrado el 19 de octubre de 2000, y nombrada por el Consejo de Ministros en su reunión de 15 de septiembre del mismo año.
* Secretario/a:
* Dª. Sofía Perea Muñoz, Secretaria General de la Agencia de Protección de Datos hasta el 6 de octubre de 2000 y D. Carlos Corbacho Pérez, Secretario General de la desde el 11 de octubre de 2000.

De la lectura de lo anterior se deduce las dos variaciones producidas en la composición del Consejo a lo largo del año 2000 que han sido la incorporación de Dª Rosa García Ontoso Directora de la Agencia de Protección de Datos de la Comunidad de Madrid, como nuevo miembro del Consejo y la del cambio experimentado en la Secretaría del Consejo a la que accede D. Carlos Corbacho Pérez, al ser nombrado Secretario General de la Agencia de Protección de Datos, tras la baja de Dª Sofía Perea Muñoz en el indicado puesto, a petición propia.

Se han convocado, como viene siendo habitual, cuatro reuniones del Consejo y entre los temas objeto de estudio y análisis durante las citadas pueden destacarse las siguientes:

* Consideración de los problemas que plantea la nueva Ley de Protección de Datos.

* Consideraciones sobre el Real Decreto 195/2000, por el que se amplía el plazo de la exigencia de las medidas de seguridad de nivel básico.

* Jornadas sobre Protección de la Privacidad, Telecomunicaciones e Internet celebradas conjuntamente con la Universidad Pública de Navarra.

* Fallo de los Premios "Protección de Datos Personales Convocatoria 2000" y primer Premio de Periodismo "Protección Datos Personales"

* Presentación al Consejo Consultivo de la Memoria de la Agencia de Protección de Datos correspondiente al ejercicio 1999.

* Incremento de la actividad de la Agencia de Protección de Datos.

* Necesidad de incremento de medios humanos y materiales de la Agencia de Protección de Datos ante las nuevas competencias atribuidas a la misma.

* Nuevos modelos de inscripción de ficheros. Notificación por Internet.

* Decisión de la Comisión de la Unión Europea sobre "Puerto Seguro" para la transmisión de datos a los Estados Unidos de América.

* Instrucción de la Agencia sobre la transmisión internacional de datos.

* Resumen de la Actividad de la Agencia de Protección de Datos durante el actual.

II SUBDIRECCIÓN GENERAL DEL REGISTRO GENERAL DE PROTECCIÓN DE DATOS.

1. INTRODUCCIÓN

El año 2000 ha supuesto un avance significativo desde el punto de vista de la demanda de inscripciones realizadas por los responsables de ficheros o tratamientos al Registro General de Protección de Datos (en adelante RGPD).

Durante el mismo se ha llevado a término el desarrollo de los programas informáticos que han posibilitado la notificación de inscripción por medios telemáticos a través de la red Internet y se ha publicado la Resolución de 30 de mayo de 2000 (B.O.E. Nº 135 de 27 de junio), de la Agencia de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el RGPD.

Se ha iniciado la tramitación de 10.512 solicitudes relativas a inscripción de ficheros, lo que ha supuesto la realización de 25.760 operaciones de inscripción a lo largo del año, de las que 17.230 han sido expedientes de alta de inscripción, 5.083 de modificaciones y 3.447 supresiones de inscripción.

Comparando la cantidad de solicitudes de inscripción recibidas y tramitadas en los primeros meses de 2000, con las correspondientes al mismo periodo del año anterior se observa que el volumen de carga de trabajo en el RGPD se incrementó en un 1400%, durante el mes de enero, consolidándose en un 500% durante todo el primer trimestre. A lo largo del resto del año,sin alcanzar tal magnitud, el número de operaciones que se realizan en el RGPD ha sido muy superior a años anteriores. Al finalizar el ejercicio este aumento pudiera estar estabilizado habiéndose multiplicado por cuatro respecto al año 1999.

Si se analiza la evolución de las solicitudes de inscripción de ficheros y las notificaciones de las correspondientes inscripciones por meses desde enero de 1997 hasta la fecha actual, se observa una tendencia prácticamente constante hasta mediados de 1999, tendencia que se ajustaba a lo que venía siendo la actividad del Registro en término medio en los años anteriores. Pero determinados factores, hacen que a partir de septiembre de 1999 comience una tendencia fuertemente creciente que eleva las solicitudes de todo tipo al RGPD.

Las causas, que han producido el incremento pueden ser debidas, por un lado, a la entrada en vigor de la nueva Ley y a la referencia especial que se hace en la misma, en su Disposición Adicional Primera, en la que se estipula un plazo formal de tres años para comunicar a la Agencia de Protección de Datos los ficheros y tratamientos de toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal. Por otro lado, los responsables de ficheros han solicitado al RGPD la inscripción de todos los cambios que ha supuesto la revisión de sus sistemas de información con el objetivo de realizar el documento de seguridad preceptivo en cumplimiento del artículo 8 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (en adelante Reglamento de Seguridad).

Las fechas de finalización del plazo para implantar las medidas de seguridad de nivel básico, que estableció el Reglamento de Seguridad, era ampliado posteriormente por el Real Decreto 195/2000, de 11 de febrero, disponiendo en su artículo 1 que *"Los sistemas de información que se encontraran en funcionamiento a la entrada en vigor del Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio, deberán implantar las medidas de seguridad de nivel básico previstas por dicho Reglamento en un plazo que finalizará el día 26 de marzo de 2000"*. Asimismo, también ha tenido repercusión, aunque menor, la finalización del plazo para adoptar las medidas de nivel medio, fijadas en el Reglamento de Seguridad el 26 de junio de 2000.

Por último, también podría haber influido en el aumento de solicitudes de inscripción, la creación de un gran número de nuevas empresas durante este período y la implantación en la sociedad de nuevas formas de empresas y negocios relacionados con las nuevas tecnologías en el ámbito de Internet (e-business) y la presentación de las mismas a través de los llamados portales de la red.

La venta a distancia, enseñanza, publicación, selección de personal, atención al cliente o al ciudadano que se realiza de una forma virtual a través de la red implica la creación de un gran número de ficheros y tratamientos incluidos en el ámbito de aplicación de la Ley.

Uno de los requisitos imprescindibles para garantizar a los ciudadanos los derechos que la Ley les reconoce, es lograr el máximo nivel de respuesta de los responsables en la notificación de la creación de sus ficheros y tratamientos para su inscripción. Con este fin se ha puesto en marcha la opción de utilizar la red de Internet, así como facilitar al responsable un programa de ayuda que le permita cumplimentar el modelo oficial, permite que los procesos de inscripción sean más eficaces y eficientes, minimiza los costes de recogida de la información, facilitando la depuración y calificación previa a la inscripción, consiguiendo el máximo control en todo el procedimiento. A su vez, facilita al responsable la cumplimentación del aspecto formal del documento dado que existe una herramienta de ayuda que le guía en la cumplimentación de los modelos de inscripción.

2. PUBLICACIÓN DEL CATÁLOGO DE FICHEROS

Como en años anteriores, la Agencia de Protección de Datos al objeto de dar cumplimiento al art. 37.j) de la Ley ha publicado el CD-ROM correspondiente al Catálogo de ficheros 2000, en el que se incluye la relación de los ficheros que figuraban inscritos en el RGPD a 30 de abril de 2000.

Este CD-ROM se publica con el fin de que cualquier persona pueda conocer, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, cumpliendo así el objetivo de dar publicidad de la existencia de los ficheros y facilitar el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, puesto que en dicho catálogo se publica asimismo la dirección a dónde pueden dirigirse los interesados.

No obstante, para cumplir con el precepto de dar publicidad a la existencia de ficheros también se viene manteniendo desde 1998 el catálogo de ficheros inscritos en la web de la Agencia, con una actualización mensual.

Por otra parte, también ha sido incluido en este CD-ROM, aprovechando su capacidad y la coincidencia de la publicación de éste con la Resolución de 30 de mayo de 2000 de la Agencia, el Programa de Ayuda a la Notificación de Ficheros, mediante el que se pueden generar las declaraciones de los mismos, posibilitando su remisión posterior a la Agencia, tanto por medio de un disquete como a través de Internet.

Como en ediciones anteriores, el CD-ROM ha sido completado con otras informaciones de interés sobre Protección de Datos, concretamente:

* Estadísticas del Registro General de Protección de Datos

* Memorias de la Agencia de Protección de Datos de 1994, 1995, 1996, 1997, 1998 y 1999.

* Publicaciones de la Agencia de Protección de Datos correspondientes a las Jornadas y Conferencias que ha venido realizando desde su creación.

* Premios de Protección de Datos correspondientes a 1997 y 1998. En este caso no se ha publicado el correspondiente a 1999 dado que su autora no ha dado su autorización.

* Legislación actualizada sobre Protección de Datos.

* Manual de Protección de Datos.

3. ENTRADA EN VIGOR DE LA LEY ORGÁNICA 15/1999 Y NUEVOS MODELOS DE NOTIFICACIÓN

3.1 DECLARACIÓN DE FICHEROS

La Ley es de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Por lo tanto, se regirá por esta Ley todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Los principios de protección deben aplicarse a todos los tratamientos de datos de carácter personal cuando se realicen en territorio español en el marco de las actividades de un establecimiento del responsable. Asimismo, se regirán por la Ley todos aquellos tratamientos de datos que utilicen medios situados en territorio español, excepto que tales medios se utilicen únicamente con fines de tránsito en la transmisión de los datos.

Estarían excluidos de los principios de protección el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como por ejemplo la correspondencia y la llevanza de un repertorio de direcciones.

También estarían excluidos del ámbito de aplicación de la Ley los ficheros y tratamientos establecidos con fines de investigación del terrorismo y formas graves de delincuencia organizada.

Los principios de protección de datos establecen, por una parte, las obligaciones que incumben a las personas, autoridades públicas, empresas, organismos, etc., que efectúen tratamientos con datos de carácter personal, obligaciones relativas a la recogida de los datos, a la calidad, la seguridad, la notificación, al principio de finalidad y todas aquellas circunstancias en las que se pueden efectuar un tratamiento de datos. Por otra parte, establecen los derechos otorgados a las personas cuyos datos sean objeto de tratamiento (afectado o interesado en terminología de la Ley), el derecho a ser informado acerca del tratamiento, de poder acceder a los datos, solicitar su rectificación o cancelación o incluso oponerse a su tratamiento en determinadas circunstancias.

El RGPD, en cumplimiento del artículo 14 de la Ley, es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal, con la finalidad de que los ciudadanos tengan la posibilidad de ejercitar los derechos de acceso, rectificación, oposición y cancelación de sus datos, pudiendo conocer a tal fin la siguiente información:

- la existencia de ficheros automatizados

- la finalidad de sus tratamientos

- la identidad del responsable del fichero

Debe recordarse que la inscripción de los ficheros en el RGPD tiene un carácter meramente declarativo, sin perjuicio de la obligación de notificar los mismos en los términos establecidos y de que la información contenida en la notificación se ajuste a la realidad.

La Ley ha desechado el establecimiento de la autorización previa a la inscripción constitutiva en un registro con la pretensión de evitar una perniciosa burocratización, por lo tanto, la inscripción en el RGPD es declarativa. Por otra parte, la consulta es pública y gratuita y serán objeto de inscripción en el mismo, tanto los ficheros de los que sean titulares las Administraciones Públicas, así como los ficheros de titularidad privada. También serán objeto de inscripción las autorizaciones de transferencias internacionales de datos a terceros países, y los códigos tipo.

Los principios de la inscripción de ficheros se pueden resumir en los siguientes puntos:

- El responsable del fichero deberá efectuar una notificación para su inscripción en el Registro, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos.

- La inscripción de un fichero de datos no prejuzga que se hayan cumplido el resto de las obligaciones derivadas de la Ley.

- La notificación de ficheros implica el compromiso por parte del responsable de que el tratamiento de datos personales declarados para su inscripción cumple con todas las exigencias legales.

- La notificación de los ficheros al Registro supone, una obligación de los responsables del tratamiento, sin coste económico alguno para ellos, y facilita que las personas afectadas puedan conocer quienes son los titulares de los ficheros ante los que deben ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición.

- Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

- En la notificación deberán figurar necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

- Deberá comunicarse a la APD cualquier cambio que se produzca con respecto a la declaración inicial y particularmente en la finalidad del fichero, en su responsable y en la dirección de su ubicación.

- El RGPD inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

- Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos.

No obstante, sería interesante hacer algunas consideraciones en relación con la entrada en vigor de la LOPD, aunque no haya supuesto cambios sustanciales a los efectos de lo previsto en los artículos que regulan la creación de ficheros y la obligación de notificarlos.

La nueva Ley regula la creación e inscripción de los ficheros de titularidad pública y privada, respectivamente, en los artículos 20, 25 y 26, estableciendo los requisitos que deberán darse para crear ficheros y los que se tendrán que incorporar en las solicitudes de inscripción en el RGPD. Asimismo, la LOPD introduce nuevas definiciones, tales como las referentes al *encargado del tratamiento y fuentes accesibles al público* y modifica, entre otros, los supuestos legales que amparan la comunicación o cesión de datos, establecidos por los artículos 11 y 21, o los relativos al movimiento internacional de datos previsto en los artículos 33 y 34.

En los artículos 20 y 26 se establece para los ficheros de titularidad pública y privada respectivamente, la información que, como mínimo, debe figurar en la notificación. Una de las novedades respecto de las previsiones que contemplaba la LORTAD, es la relativa a las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.

Respecto a los ficheros de titularidad pública, se determina que la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente, siendo las principales novedades las medidas de seguridad y las transferen-

cias de datos a países terceros.

Se establecen los términos en los que ha de publicarse esta norma habilitante del tratamiento de los datos, exigiendo que indique:

* La finalidad del fichero y los usos previstos para el mismo.

* Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

* El procedimiento de recogida de los datos de carácter personal.

* La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

* Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

* Los órganos de las Administraciones responsables del fichero.

* Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

* Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Por último, en relación con las disposiciones que se dicten para la supresión de ficheros, también se dispone que se determine el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción .

Hasta la fecha, el procedimiento de notificación e inscripción de ficheros de datos de carácter personal en el RGPD se regula fundamentalmente en el Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la Ley Orgánica 5/1992, cuyos artículos 5 y 6 habilitan a la Agencia de Protección de Datos para elaborar modelos normalizados de solicitud de inscripción para los ficheros de titularidad pública o privada, respectivamente.

La Disposición transitoria tercera de la LOPD declara expresamente la vigencia de este Real Decreto. Ello no obstante, el régimen previsto en los artículos 20 y 26, ya citados, en el que se introduce la obligación de notificar las medidas de seguridad exigibles al fichero, así como la necesaria adaptación de dichos preceptos al régimen general establecido en la Ley, han hecho necesario un nuevo modelo de notificación de ficheros, reemplazando al establecido en la Resolución de la Agencia de Protección de Datos, de 22 de junio de 1994. Los nuevos modelos se han regulado por Resolución de 30 de mayo de 2000, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el RGPD. Los citados modelos se pueden obtener a través de Internet la página Web www.agenciaprotecciondatos.org

Atendiendo al artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimientos Administrativo Común, donde se insta a las Administraciones Públicas a promover la incorporación de técnicas electrónicas, informáticas y telemáticas en el desarrollo de su actividad y el ejercicio de sus competencias, y al Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de dichas técnicas, delimitando, en el ámbito de la Administración General del Estado, las garantías, requisitos y supuestos de utilización de las técnicas electrónicas, informáticas y telemáticas, en la Resolución de 30 de mayo de 2000, se posibilita la declaración de ficheros por medios electrónicos.

La distribución de este *"Programa de Ayuda"* se realiza a petición del usuario desde la Página Web de la Agencia, cuya dirección de Internet es **https://www.agenciaprotecciondatos.org/inscinternet.htm**

El *"Programa de Ayuda"* contiene dos aplicaciones diferenciadas de generación de notificaciones para la inscripción de ficheros, una de titularidad pública y otra para titularidad privada.

Para la utilización del *"Programa de Ayuda"* es necesaria la descarga del mismo desde la página Web de la Agencia al ordenador personal donde se va a generar la notificación, permitiendo dos opciones: *"Ejecutar la aplicación desde Internet"* o "*Salvar a un fichero"*. Se descargará el programa que corresponda al tipo de fichero que se desea inscribir: *"Programa de inscripción de ficheros de titularidad pública"* en el caso de que el responsable del fichero sea un Organismo de las Administraciones Públicas, o *"Programa de inscripción de ficheros de titularidad privada"* si fuera una persona física o jurídica privada.

Para garantizar la seguridad y confidencialidad de la información contenida en las notificaciones presentadas a través de Internet, y dando cumplimiento al párrafo octavo de la Resolución de 30 de mayo de 2000, donde se establece la necesidad del cifrado de la información y del alojamiento de la misma en un servidor Web seguro, se ha procedido a la obtención del *Certificado de Servidor Seguro*, otorgada por la correspondiente *entidad de certificación*, garantizando al usuario que la información que de este modo se deposite no puede ser accedida ni manipulada por parte de un tercero.

El programa permite generar notificaciones de inscripción, dando lugar a un fichero. Este fichero se remite a la Agencia, bien directamente a través de Internet, bien mediante un disquete. En ambos casos deberá cumplimentarse y firmarse la hoja de solicitud de inscripción generada por el programa, que ha de presentarse en la Agencia de Protección de

Datos, o en cualquiera de los registros y oficinas a que se refiere el artículo 38.4 de la Ley 30/1992.

Cada remisión en soporte papel podrá incluir varias declaraciones, siempre y cuando las mismas se refieran a un mismo responsable. La Resolución establece en su punto Cuarto que cada remisión en soporte magnético o telemático podrá incluir varias declaraciones, siempre y cuando las mismas se refieran a un mismo responsable y no pudiendo exceder de 50 el número de declaraciones en una notificación o envío.

Los modelos se pueden cumplimentar indistintamente en soporte papel, magnético o telemático, gozando las declaraciones de la misma validez, siempre y cuando sea debidamente cumplimentada y firmada la hoja de solicitud de inscripción a la que se refiere la Resolución. En caso de que la declaración se efectúe a través de Internet, queda garantizada la seguridad de los datos notificados a la APD, dado que la utilización del programa supone el cifrado de aquéllos, así como que los mismos se alojarán en un servidor web seguro.

Entre las posibilidades que aporta la utilización del "*Programa de Ayuda para la notificación de inscripción de ficheros*" está la de mantener en el propio ordenador del responsable un registro de las notificaciones generadas por el mismo, permitiendo su visualización en cualquier momento.

La instrumentación de estas nuevas formas de inscripción se ha realizado atendiendo a criterios de máxima compatibilidad con el entorno tecnológico actual , de forma que sean suficientes unos medios informáticos básicos y la conexión a Internet para su utilización. Este nuevo programa de inscripción ha sido desarrollado utilizando *software* de amplia difusión, reduciéndose así los riesgos de incompatibilidad tecnológica.

Por último, a fin de facilitar la implantación y comprensión de los nuevos modelos, la Resolución estableció un periodo transitorio, que se extendió hasta el 1 de septiembre de 2000, durante el cual ha sido posible la presentación ante la APD de declaraciones cumplimentadas conforme a los modelos anteriores, sin perjuicio de que, al haber entrado en vigor la nueva Resolución, también haya sido posible la presentación en el nuevo modelo.

Todas las recepciones de soportes legibles por ordenador serán provisionales, a resultas de su proceso de comprobación. Cuando no se ajusten al diseño y demás especificaciones establecidas en la Resolución, se requerirá al declarante para que en el plazo de diez días hábiles subsane los defectos de que adolezca la misma, transcurridos los cuales y de persistir anomalías sustanciales que impidan a la APD el acceso a los datos exigidos para la notificación, se le tendrá por desistido de su petición, archivándose sin más trámite.

La solicitud de inscripción de ficheros a través de Internet entró en funcionamiento en el mes de julio de 2000 y las solicitudes notificadas desde entonces hasta el 31 de diciembre de 2000 - utilizando este medio- han supuesto un total de 2.445 operaciones de inscripción, modificación o supresión de ficheros privados y 21 de ficheros públicos, superando a las operaciones realizadas mediante el envío de soporte magnético en el caso de ficheros privados (1.995 durante todo el año).

En el modelo de notificación de ficheros de titularidad privada son de obligada cumplimentación la hoja de solicitud y los apartados: Responsable, Nombre del Fichero, Sistema de Tratamiento, Medidas de Seguridad, Estructura, Finalidad y Procedencia.

En la solicitud de inscripción de un fichero de titularidad pública es indispensable la cumplimentación de la hoja de solicitud de inscripción y los apartados de Responsable del fichero, Disposición, Nombre del fichero, Medidas de Seguridad, Estructura, Finalidad, Colectivo y Procedencia.

Los apartados que presentan variaciones respecto del modelo anterior son los correspondientes al responsable del fichero, encargado del tratamiento, medidas de seguridad, estructura básica, finalidad, procedencia y procedimiento de recogida, cesiones y transferencias.

La hoja de solicitud de inscripción es una novedad introducida en los nuevos modelos de notificación de tratamiento de datos de carácter personal aprobados por Resolución de 30 de Mayo. Ésta deberá ser presentada en papel y debidamente cumplimentada y firmada por persona habilitada a tal efecto, de acuerdo con el artículo 70.1.d) de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, independientemente de que los modelos se hayan cumplimentado en soporte papel, magnético o telemático.

A los efectos previstos en el artículo 39 de la Ley Orgánica 15/1999, no se entenderá recibida la declaración efectuada mediante su envío por medios telemáticos sino desde la fecha en que tenga entrada en la APD la hoja de solicitud de inscripción, debidamente cumplimentada y firmada.

En todo caso, carecerán de efecto alguno, las declaraciones si la hoja de solicitud de inscripción, debidamente cumplimentada y firmada, no hubiera sido presentada en la Agencia de Protección de Datos o en alguno de los registros y oficinas a los que se refiere el artículo 38.4 de la Ley 30 /1992, transcurridos 10 días desde la recepción de la declaración telemática en la página web de la Agencia.

Mediante la hoja de solicitud se cumplimentarán los datos exigidos por la Ley 30/1992 en su artículo 70.1.a). : nombre y apellidos del interesado, y en su caso, de la persona que lo represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones.

En la hoja de solicitud figura el tipo de movimiento solicitado, haciendo constar si se notifica una solicitud de creación,

de modificación o de supresión de la inscripción de un fichero.

En cuanto a la persona física que efectúa la notificación hay que hacer la consideración de que, únicamente figura como solicitante en representación del responsable del fichero a los únicos efectos de presentar la correspondiente solicitud de inscripción de creación, modificación o supresión.

Con el fin de dar cumplimiento con lo previsto en el artículo 5 de la Ley relativo al derecho de información en la recogida de datos, se ha incluido en la hoja de solicitud el siguiente texto:

En cumplimiento del artículo 5 de la Ley 15/1999, por el que se regula el derecho de información en la recogida de los datos, se advierte de los siguientes extremos: Los datos de carácter personal, que pudieran constar en esta notificación, se incluirán en el fichero de nombre "Registro General Protección de Datos", creado por Resolución del Director de la Agencia de fecha 18 de junio de 1994, (B.O.E. nº 180, 29-7-94), por la que se regulan los ficheros automatizados de datos de carácter personal existentes en la Agencia de Protección de Datos. La finalidad del fichero es velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal con el fin de hacer posible el ejercicio de los derechos de información, oposición, acceso, rectificación y cancelación de los datos. Los datos relativos a la persona física que actúa como declarante de la notificación, únicamente se utilizarán en los términos previstos en los procedimientos administrativos que sean necesarios para la tramitación de la correspondiente solicitud. Tendrán derecho a acceder a sus datos personales informatizados, rectificarlos o, en su caso, cancelarlos en la Agencia de Protección de Datos, órgano responsable del fichero.

En caso de que en la notificación deban incluirse datos de carácter personal, referentes a personas físicas distintas de la que efectúa la solicitud o del responsable del fichero, deberá, con carácter previo a su inclusión, informarles de los extremos contenidos en el párrafo anterior.

A continuación se expondrá pormenorizadamente el análisis de actividad y las dudas que se plantean en la declaración de ficheros, estructurando esta información en los diferentes apartados de los que consta la notificación de ficheros.

3.2 RESPONSABLE DEL FICHERO O TRATAMIENTO

3.2.1 Titularidad privada

Atendiendo a los cambios introducidos por la Ley y con el objetivo de corregir ciertos epígrafes del modelo anterior, se han introducido nuevas modificaciones respecto de los anteriores modelos. Uno de los cambios efectuados ha sido la adaptación de la Clasificación Nacional de Actividad Económica (C.N.A.E.), que por su gran extensión y desconocimiento daba lugar a errores en la declaración. Se ha realizado una codificación propia, denominada en el modelo Código de Actividad Principal, agrupando o desagregando los sectores de actividad, en función de las exigencias de la protección de datos, adjuntándose como relación anexa en las instrucciones publicadas con el modelo de notificación.

Se ha procedido de oficio a la conversión de estos códigos en los ficheros inscritos con anterioridad. Por otra parte, se ha introducido el subapartado de país y de dirección de correo electrónico.

El apartado de responsable ha generado confusión en la declaración de los ficheros, debido a que desde la perspectiva de los propios declarantes, han existido interpretaciones erróneas derivadas de la falta de delimitación clara en la definición utilizada en la Ley en su artículo 3.d), donde se define al *responsable del fichero o tratamiento* como la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Respecto de los ficheros de titularidad privada el artículo 25 habilita la creación de ficheros que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que la Ley establece para la protección de las personas.

El artículo 26.3 de la Ley establece la obligación de comunicar al RGPD los cambios que se produzcan en el responsable de un fichero.

La Resolución de 30 de mayo de 2000, en el apartado relativo a la modificación de la inscripción, expresa que únicamente se cumplimentará dicho apartado en caso de notificar la modificación de un fichero previamente inscrito en el RGPD. Asimismo, será necesario indicar el código de inscripción asignado por la Agencia y señalar aquellos apartados que se modifican respecto a la notificación anterior.

No se realizará la modificación de datos identificativos del responsable por cambio del titular que figure inscrito en el RGPD si no se adjunta la documentación fehaciente que lo justifique.

En relación a la modificación de este apartado, cuando se produce un cambio de titular, se ha observado que existe la tendencia, por parte de los responsables, de notificar la solicitud de una nueva inscripción cuando lo que procedería sería notificar una modificación o una supresión, dependiendo de la causa que ha originado el cambio de responsable. Esta forma de actuar produce, a veces, una duplicidad de inscripción de ficheros que posteriormente deben ser objeto de depuración, tanto de oficio como a petición del interesado en el caso que hubiera sido requerido para ello.

En el RGPD se producen situaciones singulares de solicitud de cambio de responsable que la mayoría de las veces

está justificada en operaciones de concentración o escisión de empresas, cambio de titular por sucesión, venta de activos o por cualquiera de las operaciones mercantiles previstas en la legislación vigente.

En relación con la cumplimentación de este apartado se plantean varias cuestiones, entre ellas, quién ha de ser considerado como responsable del fichero o tratamiento. En concreto, se plantean dudas en las siguientes situaciones:

- Las entidades que solicitan cambios de responsable justificados en operaciones de fusión o absorción de empresas. Cuando hay una fusión entre sociedades, puesto que se extinguen y pierden su personalidad jurídica, el nuevo responsable de los ficheros será el resultante de la misma. A los efectos de regularizar su inscripción, deberán solicitar supresiones de las inscripciones de los ficheros y tratamientos que se hayan fusionado y que tengan la misma finalidad, para que no estén duplicados. A su vez, deberán solicitar la modificación de la denominación del responsable y sus datos identificativos para hacerlos constar en el RGPD.

La escisión de empresas es un instrumento de descentralización empresarial, es un proceso similar a la fusión de sociedades, aunque de signo contrario. En el caso de que el traspaso activos sea parcial y se limite exclusivamente al traspaso del fichero se estaría ante un supuesto de cesión de datos. Por lo tanto, la otra entidad no podrá utilizar ni tratar los datos de ese fichero salvo que mantenga una relación contractual con la misma finalidad o medie el consentimiento del interesado.

La reorganización de Grupos de empresa, es otra de las circunstancias singulares que se alegan en la solicitud de cambio de responsable. Es consideración de esta Agencia que en estos casos debería existir documentación justificativa respecto del alcance y consecuencias jurídicas de la "reorganización de un Grupo de empresas".

Normalmente, una reorganización no justifica un cambio en la titularidad del responsable del fichero si no va asociado a una nueva relación contractual o al otorgamiento del consentimiento del afectado al nuevo responsable.

En efecto, los ficheros se crean y notifican por la entidad responsable de los mismos, pero no hay que olvidar que para que el responsable pueda tratar datos es necesario el consentimiento inequívoco del afectado, o que se haya producido una relación contractual o precontractual o que una Ley lo disponga.

En este sentido, debe señalarse que no se puede ignorar que el hecho de ser parte de un grupo no afecta a la personalidad jurídica de las diferentes empresas que lo integran, de modo que cada una de ellas deberá considerarse un sujeto jurídico independiente de los restantes y por lo tanto responsable de los ficheros que resulten necesarios para el logro de la actividad u objeto legítimo de esa sociedad.

En los casos de Grupo de Empresas y de Unión Temporal de Empresas, habrá que tener en cuenta que el grupo como tal carece de personalidad jurídica y que las sociedades integradas en el Grupo conservan su personalidad jurídica propia, por lo que cada una de éstas seguirá siendo responsable de sus ficheros. Las Agrupaciones de Interés Económico al tener personalidad jurídica podrán ser responsables de ficheros.

La modificación del apartado del responsable puede implicar una comunicación de datos al nuevo responsable, que constituiría conforme al artículo 3.i) de la LOPD una cesión de datos la cual deberá realizarse conforme a lo previsto en el artículo 11 de la norma. En estos casos, correspondería solicitar una modificación del apartado de cesiones notificando el nuevo destinatario de la cesión, siendo a su vez necesario, que el destinatario de la cesión del fichero proceda a notificar una nueva inscripción.

- Se plantean diversas cuestiones relacionadas con la situación en la que una empresa encarga a una asesoría laboral o gestoría la gestión de las nóminas de su personal, la llevanza de la contabilidad etc.,. En concreto, se plantea a quién corresponde notificar el fichero, lo que exige tener en consideración quién ha de ser el responsable del mismo.

Para delimitar en quién concurre en este caso la condición a la que se ha venido haciendo referencia, habrá, en consecuencia, que atender a quién decide sobre la finalidad, contenido y uso del tratamiento. En el caso que nos ocupa, las empresas, serán éstas las responsables de los ficheros estando obligadas a comunicar la declaración de los mismos, no siendo el gestor más que un mero encargado del tratamiento, figura recogida en el artículo 12 de la Ley, que trata los datos por cuenta del responsable.

En este mismo sentido, se debe indicar que una interpretación distinta impediría el tratamiento de los datos sin recabar, con carácter previo, el consentimiento de los afectados, dado que los datos de aquéllos han sido incorporados al fichero como consecuencia de la relación laboral que vincula a los mismos como empleados o como suministradores del titular de la empresa.

Debe, en este sentido, recordarse que el artículo 6.2 de la LOPD sólo exceptúa el consentimiento del interesado para el tratamiento de sus datos en un reducido número de supuestos entre los que se encuentra la existencia de un vínculo laboral o contractual con el responsable del fichero, de modo que si el responsable no fuera el empresario, se produciría un tratamiento inconsentido de los datos.

Ello no se ve afectado por el hecho de que los datos sean facilitados al gestor en soporte no automatizado, por cuanto ello no afecta al poder decisorio del responsable, limitándose la actividad del gestor, precisamente, a la incorporación de los datos a soporte informático y a la realización de determinadas actividades previamente concertadas.

En consecuencia, a tenor de lo indicado hasta este punto, se considera que la obligación de notificar el fichero corres-

ponderá al empresario, en su condición de responsable del mismo y el asesor o gestor sería un encargado del tratamiento en los términos del artículo 12 de la Ley.

- Otra de las dudas que surgen es la relativa a la determinación del responsable en los tratamientos cuya finalidad sea transmitir información utilizando el correo electrónico a través de servicios de telecomunicación.

El Considerando 47 de la Directiva 95/46/CE dispone que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje, aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión. Las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio.

Por lo tanto, se podría concluir que las personas que ofrecen los servicios serán únicamente responsables de aquellos ficheros o tratamientos necesarios para ejercer el servicio que suponga la relación contractual.

Titularidad Pública

El responsable de un fichero de titularidad pública es la persona jurídica de naturaleza pública u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento de los datos personales.

Los datos que se recogen en este apartado son los que identifican la denominación del órgano administrativo responsable del fichero y la dirección del mismo.

Dada la organización de la administración pública española, este apartado contiene un primer campo en el que se recoge una clasificación de las diferentes administraciones públicas, y a continuación un campo de texto libre donde se incluye el nombre del órgano administrativo responsable del fichero y las unidades superiores de las que depende jerárquicamente.

Respecto a la citada clasificación, se ha simplificado respecto del cuestionario anterior en el que se desglosaba de cada tipo de Administración sus organismos autónomos, quedando agrupada en la siguiente relación:

* Administración General del Estado, Seguridad Social, y organismos públicos dependientes de ellas.

* Administración Autonómica y sus organismos públicos.

* Entidades Locales

* Otras Personas Jurídico Públicas.

Se ha realizado esta agrupación debido a la dificultad que representa para el Registro mantener actualizada la identificación del responsable de ficheros de titularidad pública debido a las distintas modificaciones funcionales y de denominaciones que se producen a lo largo de una legislatura de los diferentes órganos responsables de ficheros, y que lleva a no poder ofrecer una información actualizada.

Por otra parte, aunque aparentemente no reviste complejidad la cumplimentación de este apartado se observa que no se interpretan correctamente las instrucciones, lo que produce las siguientes situaciones:

* En vez de indicar el nombre del órgano administrativo responsable del fichero se indica el nombre del puesto de trabajo que ostenta la persona titular de dicho órgano.

* El CIF, que sería la información necesaria a efectos estadísticos para diferenciar el número de Organismos que han inscrito ficheros, no es un dato fiable puesto que en algunos casos se declara el mismo para todas las unidades y órganos de un departamento o de toda una comunidad autóno otros casos varía por dependencias hasta un nivel inferior.

Normalmente, estas situaciones se subsanan de oficio cuando son detectadas si se dispone de información que acredite la situación real. Con el CIF no es posible realizar dicha normalización, al no aparecer publicado en las guías oficiales de estructuras administrativas.

Sin embargo el problema mas importante que se plantea en el RGPD con este apartado es el que se produce cuando un responsable de fichero cambia de denominación. Este es el caso de las reestructuraciones orgánicas ministeriales o de las comunidades autónomas.

La modificación de un fichero de las administraciones públicas debe estar regulada por una disposición general, tal como indica el artículo 20. A los efectos de modificación del apartado de responsable, se ha mantenido el criterio de que se pueda considerar disposición de modificación del fichero la propia Orden por la que se establece la nueva estructura orgánica, salvo que se escinda en dos o mas unidades diferentes las funciones del responsable, en cuyo caso es necesario que en uno de los nuevos organismos se proceda a publicar una nueva disposición que habilite la creación del fichero resultante de la reorganización de competencias.

En el año 2000, el Gobierno en uso de las atribuciones que le confiere la Ley 50/1997, de 27 de noviembre, del Gobierno, efectuó una amplia reestructuración ministerial mediante los Reales Decretos 557/2000, 558/2000, 574/2000 y 689/2000, entre otros, de abril y mayo de 2000, por los que se modificaron el nombre de ciertos departamentos ministeriales, se crearon algunos y se suprimieron otros.

Esta situación ha dado lugar a que la inscripción en el RGPD de los ficheros de la Administración General del Estado no ofrezca una información actualizada respecto a las denominaciones de los órganos responsables de ficheros.

Por ello, en el mes de octubre de 2000 el Director de la Agencia requirió a los responsables con competencias en esta materia de cada uno de los departamentos ministeriales, para que procedieran a revisar su inscripción y comunicasen los cambios pertinentes a efectos de su actualización en este Registro.

Al finalizar el ejercicio habían comunicado la situación actual en relación con los ficheros inscritos los Ministerios de Economía, Portavoz del Gobierno, Justicia, Defensa, Medio Ambiente, Trabajo y Asuntos Sociales, Agricultura, y Presidencia.

Asimismo, y a los efectos de que exista una correspondencia entre los ficheros inscritos en el RGPD y el encuadramiento del órgano responsable en el departamento que le corresponda según la estructura funcional del Ministerio del que dependen se ha procedido de oficio a realizar los cambios de denominaciones que se indican a continuación.

Las competencias del Ministerio de Economía y Hacienda se han desglosado en el Ministerio de Economía y el Ministerio de Hacienda, por lo que se han ido adscribiendo a cada uno de estos Ministerios los ficheros dependientes de los siguientes Centros Directivos:

Ministerio de Economía

- Cámaras Oficiales de Comercio, Industria y Navegación
- Comisión Nacional del Mercado de Valores
- Consejo Superior de Cámaras Oficiales de Comercio, Industria y Navegación de España
- Dirección General de Política de Pymes
- Dirección General de Seguros
- Dirección General del Tesoro y de Política Financiera
- Fabrica Nacional de Moneda y Timbre
- Instituto de Contabilidad y Auditoria de Cuentas
- Secretaria General Técnica
- Subdirección General de Recursos y Reclamaciones
- Subsecretaria de Economía y Hacienda

Ministerio de Hacienda

- Agencia Estatal de Administración Tributaria
- Dirección General de Análisis y Programación Presupuestaria
- Dirección General de Coordinación con las Haciendas Territoriales
- Dirección General de Costes de Personal y Pensiones Públicas
- Dirección General de Presupuestos
- Dirección General de Tributos
- Dirección General del Catastro
- Instituto de Estudios Fiscales
- Instituto Nacional de Estadística
- Intervención General de la Administración del Estado
- Organismo Nacional de Loterías y Apuestas del Estado
- Secretaria de Estado de Comercio, Turismo y Pymes
- Secretaria de Estado de Hacienda
- Secretaria de Estado de Presupuestos y Gastos
- Secretaria General Técnica
- Subsecretaria de Economía y Hacienda
- Comisión Interministerial Liquidadora Ley 19/1990
- Parque Móvil del Estado
- Tribunal Económico-Administrativo Central

Se ha procedido a subsanar de oficio la denominación de los ficheros inscritos cuyo responsable constaba Ministerio de Educación y Cultura, asignándoles su actual denominación de Ministerio de Educación, Cultura y Deporte y los del Ministerio de Industria y Energía han sido adscritos al Ministerio de Ciencia y Tecnología.

Únicamente se realiza el cambio de la denominación o adscripción de cada ministerio ya que para modificar el encuadramiento completo del responsable (Centro Directivo y Unidad Responsable) no se dispone de suficiente información.

A finales del año 2000, también se ha realizado un requerimiento a 92 Ayuntamientos de municipios con poblaciones superiores a los 4000 habitantes para los que no consta inscrito ningún fichero en el RGPD, esperando una respuesta en los primeros meses del año 2001. De no recibir la correspondiente solicitud de inscripción se dará traslado a la Inspección de Datos.

3.3 SERVICIO O UNIDAD PARA EJERCER LOS DERECHOS DE OPOSICIÓN, ACCESO, RECTIFICACIÓN Y CANCELACIÓN/ UBICACIÓN PRINCIPAL.

El apartado del servicio o unidad para ejercer los derechos de oposición, acceso, rectificación y cancelación únicamente deberá cumplimentarse en el caso de que la dirección dónde se prevea atender al ciudadano que desee ejercitar tales derechos sea diferente a la indicada en el apartado de *Responsable del fichero o tratamiento* .

El Real Decreto 1332/94, establece que las entidades que procedan a inscribir un fichero en el RGPD, deberán declarar, entre otros apartados de cumplimentación obligatoria, la ubicación del mismo. Ésta se especificará en el apartado de *Ubicación principal*, únicamente cuando el fichero se encuentre establecido en una dirección diferente a la del responsable del fichero o tratamiento.

Se cumplimentará obligatoriamente el nombre de la dependencia u oficina y la dirección completa de la entidad donde se ubiquen los ficheros. Si se trata de una base de datos o un sistema de ficheros distribuidos se indicará la dirección principal de ubicación. También se consignará el nombre del país, en caso de que el fichero no esté ubicado en territorio español. En este caso se deberá cumplimentar obligatoriamente el apartado de Transferencias Internacionales.

En muchas ocasiones, el apartado de ubicación se ha utilizado, por parte de aquellos responsables de ficheros, cuya razón social disponía de varias sedes distribuidas en lugares diferentes. Dichos responsables declaraban la ubicación de las distintas sedes dónde se producía la recogida de los datos e, incluso, parte del tratamiento. Este sería el caso de entidades con una única denominación jurídica, pero con diversos centros distribuidos en lugares diferentes (hoteles, clínicas y centros comerciales).

En otros casos, los responsables de los tratamientos, declaran como dirección de acceso, la correspondiente al lugar dónde se encuentra ubicado el fichero. En este tipo de entidades, que además de tener ubicaciones diferentes, comparten el nombre del fichero, ya que forma parte de una misma aplicación informática que se distribuye a los distintos centros, puede ser muy complejo facilitar una dirección dónde las personas interesadas puedan ejercer su derecho de oposición, acceso, rectificación y cancelación.

Al tramitar los expedientes de inscripción de los ficheros de estas entidades, se ha procedido a informar a los responsables de los mismos, de la conveniencia de identificar el nombre del fichero con la ubicación dónde se encuentra, con miras a que cualquier ciudadano que consulte el catálogo de ficheros, pueda tener una información clara de dónde ejercer los derechos que le atribuye la Ley.

Se ha utilizado también para declarar el lugar de la ubicación del ordenador que realiza las funciones de servidor en aquellos tratamientos que utilizan Internet como medio. En algunos casos, esta ubicación se sitúa fuera del territorio español, por lo que se hace necesario declarar las correspondientes transferencias internacionales de datos, según lo dispuesto en los artículos 33 y 34 de la Ley.

La mayoría de los sitios Web son visitados por usuarios que no residen en el territorio donde está establecido el responsable de la información presentada o registrada en esa Web.

Esto no quiere decir, que por el hecho de que un ciudadano (afectado) se conecte a una página Web de un responsable establecido fuera de España y registre sus datos en ella o inicie una relación precontractual o contractual con el responsable del fichero, este responsable deba notificar sus ficheros al RGPD.

La proliferación de empresas establecidas en la red Internet producen mucha confusión entre los posibles responsables en relación con la obligación de inscribir sus ficheros en el Registro español.

El país donde esté ubicada u hospedada la página Web no influye para determinar que jurisdicción de protección de datos le sería aplicable. Uno de los parámetros que el RGPD está utilizando para determinar si es competencia de este Registro la inscripción de un fichero de un responsable, es que el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable.

Por otro lado, la mayoría de las empresas "puntocom" tienen la ubicación de sus ficheros (sedes Web) en países distintos del que está establecido el responsable.

La jurisdicción de las empresas "puntocom" no es fácil de identificar en un primera calificación de la información declarada en la notificación de ficheros.

Es evidente que la normativa de protección de datos vigente en cada estado miembro debe cumplirse cuando exista un establecimiento del responsable situado en ese estado.

3.4 NOMBRE Y DESCRIPCIÓN DEL FICHERO O TRATAMIENTO DE DATOS

En este apartado se deberá indicar el nombre que identifique al fichero o tratamiento a notificar y una breve descripción del mismo.

La Ley utiliza conceptos como fichero y tratamiento de datos indistintamente en muchos de sus preceptos, pudiendo producir una confusión en el uso de los términos. Asimismo, los conceptos tecnológicos de fichero y archivo en los sistemas informáticos a veces también produce dudas entre los responsables a los efectos de la notificación.

La definición de estos términos a los efectos de la Ley, se encuentran en el artículo 3 de la misma.

Se define *Fichero* a todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Se define *Tratamiento de datos* como las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

No obstante, sería interesante hacer algunas consideraciones en relación con los conceptos de *tratamiento* y *fichero* utilizados por la nueva Ley.

Tanto en la Ley como en la Directiva existen definiciones de los dos conceptos en idénticos términos. A efectos prácticos se puede considerar que:

* La creación de un fichero exige, con carácter previo, la realización de diferentes tratamientos de datos personales: recogida, grabación, depuración, organización y estructuración, etc.

* Un tratamiento de datos supone la realización de cualquier operación o conjunto de operaciones sobre datos que deben encontrarse estructurados, ser accesibles y estar almacenados en ficheros.

Idéntica similitud de conceptos puede encontrarse en los modelos que ha publicado la Agencia en la Resolución de 30 de mayo de 2000. Así, se puede observar que la denominación del cuestionario aparece como "MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL" *Creación, Modificación y Supresión de ficheros.*

Una de las dudas planteadas con más frecuencia es la relacionada con el número de ficheros que deben declararse y si esos ficheros son equivalentes a todos lo ficheros y tablas de los sistemas informáticos.

Los distintos extremos que debe contener el modelo de notificación de ficheros será una guía que determinará la declaración de uno o más ficheros a los efectos de su inscripción en el RGPD.

En un principio, se podría considerar que la declaración de un fichero supondrá la notificación de la información que corresponda con el conjunto de datos asociados a un tratamiento o uso de los mismos, con una finalidad o finalidades compatibles y determinadas.

Cada notificación de fichero podrá englobar varias operaciones y procedimientos técnicos que permitan la recogida, grabación, conservación, elaboración, etc. de datos personales, siendo indiferente si se declara un fichero por cada "tabla" o se declara un conjunto de tablas con tratamientos comunes.

Será indiferente a los efectos de inscripción en el RGPD, los ficheros (en terminología técnica) o tablas que incluyan los diseños informáticos de los sistemas de información. Se tendrá que notificar por cada declaración de ficheros la información que corresponda con el conjunto de datos asociados a un tratamiento o uso de los mismos, con una finalidad o finalidades compatibles y determinadas. Por lo tanto, un responsable deberá notificar los ficheros de datos personales que se tratan bajo su autoridad, los cuales no tendrán que corresponder necesariamente con todas las operaciones y procedimientos técnicos ya sean de almacenamiento de datos o de tratamiento de los mismos.

Ficheros manuales

La disposición adicional primera de la Ley, relativa a *ficheros preexistentes* , en su segundo párrafo dispone:

"En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica y la obligación de inscribirlos deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados".

El Considerando 27 de la Directiva 95/46/CE especifica que:

1.- La protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual.

2.- El alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves.

3.- Que no obstante, por lo que respecta al tratamiento manual la Directiva solo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas. En particular, el contenido de un fichero debe estructurarse conforme a criterios específicos o determinados relativos a las personas, que permitan determinar los elementos de un conjunto estructurado de información relativa a las mismas y que permitan acceder fácilmente a los datos personales.

4.- Que los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro.

5.- Que las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la Directiva 95/46/CE.

La definición de *fichero* prevista en la Directiva es la siguiente: Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Como ya se citó anteriormente, la definición de *fichero* prevista en la Ley es: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Los archivos (carpetas o conjunto de carpetas) o ficheros manuales, así como sus portadas, que no estén estructurados conforme a criterios específicos y determinados relativos a las personas, en un principio, se puede interpretar que no están comprendidos en el ámbito de aplicación de la Ley.

Por lo tanto, un fichero manual estará incluido dentro del ámbito de aplicación, cuando el fichero o archivo contenga un conjunto estructurado de datos personales que sean accesibles fácilmente a los datos personales con arreglo a criterios determinados.

3.5 ENCARGADO DEL TRATAMIENTO

La derogada LORTAD, recogía en su artículo 27, los tratamientos, regulados mediante un contrato, realizados por un tercero por cuenta del responsable del fichero. La Ley adaptó al Derecho nacional la figura del encargado del tratamiento que venía contemplada en la Directiva 95/46/CE.

El artículo 3.g) de la Ley 15/1999, define al encargado del tratamiento como "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

En este sentido, en lo que se refiere a la inscripción de ficheros en el RGPD, se ha de tener en cuenta que, las entidades que realicen funciones de encargados del tratamiento, no deben notificar los ficheros para su inscripción.

No obstante, el es necesario tener presente, que según el Artículo 12 de la misma:

- "*No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.*

- *La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.*

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

- *Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*

- *En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

En algunos casos, se ha puesto de manifiesto la existencia de varios encargados de tratamiento para un mismo fichero, declarando los responsables esta circunstancia a la hora de presentar la solicitud de inscripción en el RGPD. En todos los casos, se ha procedido a dejar constancia registral de estos extremos. No obstante, para facilitar la cumplimentación de la declaración, se recomienda especificar como encargado del tratamiento a la entidad principal que realice dichas funciones.

Un error habitual que se ha producido al cumplimentar el modelo de notificación, consiste en considerar como encargado del tratamiento, al personal que trabaja por cuenta del responsable del fichero. Estos casos no se ajustan a lo considerado en los citados artículos 3.g) y 12 de la Ley. Conviene aclarar que una persona que trabaja bajo la dependencia o autoridad directa del responsable debido a una relación contractual dentro del ámbito del derecho laboral, no tiene la consideración de encargado del tratamiento a los efectos de esta Ley.

Por ello, en estos casos, no procede cumplimentar dicho apartado del modelo de solicitud de inscripción. En bastantes

ocasiones se ha requerido al responsable del fichero para que subsane su declaración y, en otros casos, cuando del contenido de la declaración se ha desprendido claramente que se trataba de un error manifiesto, se ha procedido a su subsanación de oficio, informando al responsable de la corrección realizada.

3.6 MEDIDAS DE SEGURIDAD

Según el artículo 9 de la Ley *"el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".*

"No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas".

"Asimismo, se establecerán reglamentariamente los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 relativo a datos especialmente protegidos".

No hay ningún plazo estipulado para declarar el nivel de seguridad en los ficheros inscritos en el RGPD con anterioridad a la entrada en vigor de la nueva Ley.

No obstante, la Disposición Adicional Primera de la Ley, establece, que los ficheros y tratamientos automatizados, inscritos o no en el RGPD deberán adecuarse a dicha Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

A la vista de la redacción de la citada Disposición se plantean las siguientes cuestiones:

a) En primer lugar, la determinación del ámbito de aplicación de la Disposición y, concretamente, el sentido que ha de darse a la expresión *"ficheros y tratamientos automatizados inscritos o no en el RGPD".*

b) En segundo lugar, se plantea la duda sobre si la adecuación a la Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor, (14 de enero de 2000) se refiere a la totalidad de las previsiones contenidas en la Ley Orgánica o resulta sólo aplicable al cumplimiento de las obligaciones formales de notificación para su inscripción en el RGPD.

A juicio de la Agencia de Protección de Datos, la interpretación de las previsiones contenidas se refieren al aspecto formal necesario para adecuar la inscripción de los ficheros preexistentes en un plazo de tres años. Por lo tanto, todos los ficheros que figuren inscritos en el RGPD antes del 15 de enero de 2000, tendrán tres años para completar su declaración con los niveles de seguridad.

La referencia a los ficheros no inscritos en el RGPD, únicamente debe alcanzar a aquellos ficheros o tratamientos, públicos y privados que en la LORTAD, no se encontraban sujetos a la normativa reguladora y que, en consecuencia, no estaban obligados a notificarlos para su inscripción en el RGPD, y que en la actual Ley, han sido incluidos en el ámbito de aplicación.

En las inscripciones realizadas desde la entrada en vigor de la Resolución de 30 de mayo de 2000 ya se incluye este apartado de medidas de seguridad. En dicho apartado se indicará el nivel de seguridad exigible, clasificándose en tres niveles: básico, medio y alto.

Se consignará nivel medio, si se trata de un fichero que contenga datos relativos a servicios financieros, o si se trata de un fichero para la prestación de servicios de información sobre solvencia patrimonial y crédito. En el caso de ficheros de titularidad pública se incluirán en este nivel los que contengan datos relativos a la comisión de infracciones administrativas o penales y Hacienda Pública.

Se consignará nivel alto cuando el fichero contenga datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. En titularidad pública los ficheros que contengan datos recabados con fines policiales sin consentimiento de las personas afectadas.

En cualquier caso, al menos, deben consignarse las medidas de seguridad catalogadas como de nivel básico.

Por otra parte, para los ficheros de titularidad pública, a partir de la nueva Ley, también se deberá indicar en la disposición general de creación del fichero el nivel de medidas de seguridad en el que se encuentra catalogado. Y por lo tanto, en el modelo de notificación debe señalarse el mismo nivel que se ha publicado en la norma de creación, por lo que, en caso de discrepancias entre la disposición y la declaración se solicita del responsable una aclaración al respecto.

Los principales problemas en este apartado se plantean cuando la disposición general en que se ampara la creación

del fichero se ha dictado de acuerdo con el art. 18 de la derogada LORTAD, que no exigía la declaración del nivel de seguridad.

En estos casos, cuando la fecha de la disposición general es posterior a la fecha de entrada en vigor de la nueva Ley, se devuelve al responsable para que subsane la disposición general y sea publicada de nuevo en el diario oficial correspondiente, con la información relativa al nivel de seguridad.

Por el contrario, si la fecha de la disposición fuera anterior a la fecha de entrada en vigor de la ley, únicamente se deberá consignar el nivel de medidas de seguridad que corresponda en la notificación correspondiente.

3.7 DESCRIPCIÓN DE LOS TIPOS DE DATOS. DATOS ESPECIALMENTE PROTEGIDOS.

Este apartado del modelo, en el que se declaran los tipos de datos que se incluyen en el fichero, ha experimentado algunas variaciones. Estas variaciones se resumen en las siguientes:

* Datos especialmente protegidos: Se ha incluido el tipo de dato de *afiliación sindical.*

* Datos de carácter identificativo: Se ha incluido el tipo de dato de *firma electrónica.*

* Datos de características personales: Separación de los tipos de datos de *fecha de nacimiento y edad.*

* Datos económico-financieros y de seguros: Se ha incluido el nuevo tipo de *datos de deducciones impositivas/impuestos.*

En este apartado es dónde se declara la utilización de datos de carácter personal y, por lo tanto, se determina que dicho fichero o tratamiento se incluye en el ámbito de aplicación de la Ley.

La protección deberá aplicarse a cualquier información relativa a una persona física identificada o identificable; una persona no será identificable cuando los datos fueran anónimos o no se pudiera determinar su identidad.

No obstante, se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante un número de identificación, o un conjunto de elementos que pudiera ser característico de su identidad física, fisiológica, psíquica, económica, cultural o social.

Se debe llamar la atención, sobre aquellos tratamientos que, utilizando gran cantidad de datos, aparentemente no identificables, junto con técnicas informáticas y de marketing especiales, pudieran convertir dichos datos, en principio anónimos, en información relativa a personas identificadas. Es decir, los datos de los ciudadanos, cuando se fusionan y se mezclan con más información, pueden llegar a dar un perfil concreto del individuo que permita su identificación.

Por su especial importancia, a continuación se analiza la inscripción de ficheros, cuyos responsables han declarado la utilización de datos especialmente protegidos.

Datos especialmente protegidos: Afiliación Sindical

El artículo 7.2 de la Ley, se refiere a la información relativa a la afiliación sindical, como un dato que puede ser recabado con el consentimiento expreso y por escrito del afectado. En la Ley anterior, no se citaba expresamente la afiliación como un tipo de dato especialmente protegido, pero no quedaban dudas acerca de que ese tipo de dato, se encuadraba entre los que determinaban la ideología del afectado.

Una vez que la nueva Ley entró en vigor, y antes de que se aprobasen los nuevos modelos, los responsables de los ficheros solicitaron la inscripción de los datos relativos a la afiliación sindical, cumplimentando el anterior modelo, señalando el tipo de dato de ideología. Como aclaración, comunicaban que éste, efectivamente, se refería a la afiliación sindical de los empleados. Posteriormente, como consecuencia de la aprobación de la Ley y, una vez que se aprobaron los nuevos modelos, fue posible declarar la información relativa a la afiliación sindical como una tipología diferenciada de los datos de ideología.

Como justificación del tratamiento de este tipo de datos, los responsables de los ficheros han declarado que se trataba de los datos de la cuota de afiliación sindical que, a petición expresa de los trabajadores, en lugar de abonar aquélla al sindicato al que están afiliados, han solicitado expresamente que se les deduzca su importe de la nómina haciendo la empresa, en consecuencia, efectivo el pago de la cuota al sindicato correspondiente, en virtud de lo previsto sobre dicho particular en la Ley Orgánica de Libertad Sindical.

En otros casos, han justificado que eran datos recabados con el consentimiento expreso del afectado, y era necesario para la gestión de personal y control del personal que estaba liberado por dedicación a tareas sindicales.

A 31 de diciembre de 2000, constan inscritos 154 ficheros de titularidad pública y privada, cuyos responsables han declarado explícitamente el tratamiento de datos de afiliación sindical, 113 de los cuales, se han inscrito en el RGPD durante el año 2000. Paralelamente, se ha procedido a realizar la adaptación de las inscripciones anteriores cuyos responsables habían informado del uso de datos de afiliación sindical, tipificando ideología. No obstante, gran número de inscripciones realizadas durante la etapa LORTAD siguen figurando inscritas con datos de ideología aunque éstos

se refieran a la pertenencia a sindicatos.

Por otra parte, en el mismo apartado, se recoge el supuesto previsto en el segundo inciso del artículo 7.2, que excepciona del consentimiento expreso y por escrito para tratar datos especialmente protegidos de ideología, afiliación sindical, religión y creencias. Dicho supuesto se refiere a "*los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado*". Este supuesto no se contemplaba en el modelo anterior, ya que la LORTAD, excluía del ámbito de aplicación de la ley, en su artículo 2.e "*a los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieren a sus asociados o miembros y ex-miembros ...* ".

Durante el año 2000, únicamente se ha recibido la solicitud de inscripción de un fichero cuyo responsable es una central sindical, que se amparaba en el supuesto de que "*es un fichero mantenido por partidos políticos, sindicatos, ...".* Dicho responsable declaró que ha recabado el consentimiento expreso y por escrito del afectado para tratar los datos especialmente protegidos de afiliación sindical. No obstante, se recuerda que los ficheros que anteriormente estaban exceptuados del ámbito de aplicación de la LORTAD, la Ley los ha incluido en su ámbito y sus responsables tienen un plazo transitorio hasta el 14 de enero de 2003 para declararlos.

Datos especialmente protegidos: Salud

Durante el año 2000, se ha producido un incremento del 388%, en lo referente a la inscripción de ficheros de titularidad privada que declaran datos especialmente protegidos de salud, en relación con la declaración del mismo tipo de ficheros en 1999. En total, durante el año 2000, se han inscrito 767 ficheros cuyos responsables han declarado la utilización de datos de salud. En la mayor parte de estas inscripciones, los responsables han declarado que tratan datos con el consentimiento expreso de los afectados.

De las inscripciones realizadas durante este año en las que se han declarado datos de salud, un 20% de ellos, corresponden a responsables cuyo sector de actividad se enmarca dentro de las actividades sanitarias. En menor medida se incluirían en el sector de seguros (11%) y en la industria química y farmacéutica (3%). El resto, es decir, más de un 60% de los ficheros inscritos durante el año 2000, que utilizan este tipo de datos, se refiere, fundamentalmente a tratamientos cuyas finalidades principales están relacionadas con la gestión de personal, nóminas y recursos humanos. Este gran número de ficheros se justifica claramente en la aplicación de los tratamientos amparados en la Ley de Seguridad e Higiene en el Trabajo y Prevención de Riesgos Laborales y en la legislación del IRPF.

Tratamientos amparados en la Ley 31/1995 de 8 de noviembre de Seguridad e Higiene en el Trabajo y Prevención de Riesgos Laborales:

Como consecuencia de la plena aplicación de la Ley de Seguridad e Higiene en el Trabajo y Prevención de Riesgos Laborales, ha tenido lugar un gran incremento de notificaciones que han declarado la utilización de datos de salud amparados en dicha ley y, cuya finalidad era la prevención de riesgos laborales. Cabe señalar que en el nuevo modelo normalizado, se ha incluido una finalidad tipificada dentro del epígrafe de recursos humanos, denominada *Prevención de Riesgos Laborales* , para contemplar este tratamiento de datos.

Del total de los ficheros anteriormente señalados, cuyos responsables declaran datos de salud, 43 de estos tratamientos han declarado que el uso de datos de salud se ampara únicamente en la Ley de Prevención de Riesgos Laborales, no constando en su declaración que han recabado el consentimiento expreso de los afectados. No obstante, es preciso señalar que este tipo de tratamientos solo se podrá amparar en la Ley de Seguridad e Higiene en el Trabajo y Prevención de Riesgos Laborales, cuando el acceso a los datos relativos a la salud se limite a los servicios médicos de empresa.

El artículo 22.1 de la Ley de Prevención de Riesgos Laborales como regla general establece que la vigilancia periódica del estado de salud de los trabajadores exige el consentimiento expreso de éstos, al señalar que: *"El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo.*

Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

En todo caso se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo".

Adicionalmente, el artículo 22.4 de la Ley 31/1995 limita el acceso a la información médica y reitera la exigencia de consentimiento cuando señala que: *"Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador.*

El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias

que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador".

No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva.

Por lo tanto, el empleador podrá tratar únicamente el dato de que el empleado es apto o no apto, para el desempeño de su trabajo. No obstante, este dato se considera como dato de salud, toda vez que el apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa viene a definir la noción de datos de carácter personal relativos a la salud, considerando que su concepto abarca *"las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo, pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido".* Añade el citado apartado 45 que *"debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas".*

Tratamientos amparados en la legislación del IRPF.

El Real Decreto 214/1999, de 5 de febrero, por el que se aprueba el Reglamento del Impuesto sobre la Renta de las Personas Físicas, establece la comunicación de determinados datos de los perceptores de rentas del trabajo a su pagador, en los siguientes términos: "*Los contribuyentes deberán comunicar al pagador la situación personal y familiar que influye en el importe excepcionado de retener, en la determinación del tipo de retención o en las regularizaciones de éste, quedando obligado, asimismo, el pagador a conservar la comunicación debidamente firmada.*

El contenido de las comunicaciones se ajustará al modelo que se apruebe por Resolución del Departamento de Gestión Tributaria de la Agencia Estatal de Administración Tributaria ."

En dichos modelos, de comunicación de la situación personal y familiar del perceptor de rentas del trabajo, o de su variación, ante el pagador, aprobados mediante Resolución de 28 de diciembre de 1999, del Departamento de Gestión Tributaria de la Agencia Tributaria, se determina la forma en que debe efectuarse dicha comunicación, estableciendo que se deben declarar como circunstancias personales, el grado de discapacidad propia y/o de los hijos o descendientes.

De todo ello se desprende que, el dato relativo al porcentaje de minusvalía en relación con la retención a cuenta del I.R.P.F. se considera dato de salud. Este hecho ha propiciado un notable incremento, durante el año 2000, en la inscripción de ficheros de titularidad privada, cuyos responsables han declarado que recababan datos especialmente protegidos de salud.

Por último, debido al impacto que desde el punto de vista de las medidas de seguridad tiene la recogida de este tipo de datos, muchos responsables de ficheros notifican el tratamiento de datos especialmente protegidos de salud, únicamente cuando alguno de sus empleados ha declarado esta circunstancia.

Datos especialmente protegidos: Vida sexual

Durante el año 2000, se ha producido un aumento en las notificaciones de ficheros de titularidad privada que declaraban la utilización de datos especialmente protegidos referentes a la vida sexual de los afectados. Dicho incremento, aunque porcentualmente es muy elevado (725%), queda matizado por los datos absolutos, ya que en total se han inscrito 33 ficheros cuyos responsables han declarado este tipo de datos especialmente protegidos, frente a los 4 ficheros que se inscribieron en 1999.

Cabe señalar que los sectores de actividad mayoritarios a los que pertenecen dichos responsables, son los que se refieren a las actividades sanitarias. También se han declarado este tipo de datos como necesarios para la puesta en marcha de concursos de TV en los que los participantes deben convivir durante cierto tiempo. La justificación que han aportado los responsables se refiere a que dichos datos son recabados con el consentimiento expreso de los interesados, y su necesidad viene justificada por la estrecha relación que se establece entre los concursantes y las extremas condiciones en las que las personas seleccionadas para el concurso deben pasar durante un largo período de tiempo, que exige conocer a priori esta información, para realizar la selección.

Por otra parte, se han tramitado solicitudes de inscripción de las que, de la información aportada por los responsables, se podría desprender el tratamiento de datos especialmente protegidos, aunque no fueron declarados en su momento. Una vez requeridos los responsables para que aclarasen la posible utilización de este tipo de datos, han comunicado que no se realizan tratamientos de esta naturaleza.

Dentro de este tipo de problemática, se pueden incluir las solicitudes de inscripción de páginas web, en las que no se declaraba el tratamiento de datos especialmente protegidos de vida sexual, pero, del contenido y colectivo al que va dirigido, se podría desprender su utilización. De estas solicitudes, se podría desprender que por el sólo hecho de registrarse en la página web, se estuviera revelando información relativa a la vida sexual de los usuarios.

3.8 FINALIDAD DEL FICHERO Y USOS PREVISTOS

La experiencia obtenida a lo largo de los años de funcionamiento del RGPD, ha puesto de manifiesto la necesidad de modificar el diseño de este apartado, con el fin de facilitar la cumplimentación del mismo a los responsables de ficheros.

En el formulario anterior aparecía un espacio para la cumplimentación de un texto libre para describir la finalidad del fichero, y a continuación la lista de tipificaciones de finalidad, sin ninguna agrupación, por lo que no era fácil encontrar aquellos epígrafes que se ajustaran a la finalidad declarada en el texto libre.

Por ello, en el nuevo formato del formulario se ha mantenido el espacio para la descripción en texto libre de la finalidad, pero se han agrupado las tipificaciones de finalidad por grandes apartados comunes:

TITULARIDAD PRIVADA	TITULARIDAD PÚBLICA
Gestión contable, fiscal y administrativa **Recursos humanos** **Servicios económico-financieros y seguros** **Publicidad y prospección comercial** **Servicios de telecomunicaciones** **Actividades asociativas, culturales, recreativas, deportivas y sociales** **Educación** **Sanidad** **Seguridad** **Finalidades varias:** Fidelización de clientes Reservas y emisión de billetes Fines históricos, científicos o estadísticos Otras finalidades	**Recursos humanos** **Hacienda y gestión económico-financiera** **Justicia** **Seguridad pública y defensa** **Trabajo y bienestar social** **Sanidad** **Educación y cultura** **Estadística** **Finalidades varias:** Procedimientos administrativos Registro de entrada y salida de documentos Otros registros administrativos Atención al ciudadano Concesión y gestión de permisos, licencias y autorizaciones Seguridad y control de acceso a edificios Publicaciones Fines científicos, históricos o estadísticos Gestión sancionadora Gestión de estadísticas internas Prestación de servicios de certificación Otras finalidades

Por otro lado, del análisis de la información declarada en el texto libre que describe detalladamente la finalidad y usos previstos del fichero o tratamiento, se ha visto la necesidad de cambiar la denominación de alguna de éstas tipificaciones de finalidad y añadir tipologías nuevas.

Así, se ha modificado la descripción de la tipificación añadiendo alguna palabra que aclare el concepto, o se han subdividido o unificado, las siguientes tipificaciones de finalidad:

Titularidad Privada

DENOMINACIÓNANTERIOR	DENOMINACIÓNACTUAL
Gestión Contable, Fiscal y Administrativa	- Gestión Económica y Contable - Gestión Fiscal - Gestión Administrativa
Auditorías, Asesorías y Servicios Relacionados	Consultorías, Auditorías, Asesorías y Servicios relacionados
Formación Profesional	Formación de personal
Información sobre la Solvencia Patrimonial y Crédito	Prestación de Servicios de Solvencia Patrimonial y Crédito
Publicidad Propia Publicidad para Terceros	Publicidad
Prospecciones de Mercado	Prospección Comercial
Servicios de Telecomunicación	Prestación de Servicios de Telecomunicaciones
Gestión Administrativa de los Integrantes de Clubes y Asociaciones Deportivas, Culturales, Profesionales y Similares.	Gestión de Clubes o Asociaciones Deportivas, Culturales, Profesionales y Similares
Medios de Comunicación Social	Gestión de Medios de Comunicación Social
Educación Infantil Primaria	Enseñanza Infantil Primaria
Educación Secundaria	Enseñanza Secundaria
Educación Universitaria	Enseñanza Universitaria
Investigaciones Científicas y Médicas	Investigación Epidemiológica y Actividades Análogas
Seguridad y Control Interno	Seguridad y Control de Acceso a Edificios
Seguridad	Otras Actividades de Seguridad
Obtención de Estadísticas Diversas	Fines Históricos, Científicos y Estadísticos
Otros	Otras Finalidades

Titularidad Pública

DENOMINACIÓNANTERIOR	DENOMINACIÓNACTUAL
Control de Patrimonio de Altos Cargos Públicos	Control de Patrimonio de Altos Cargos
Gestión Económica con Terceros	Gestión Económica y Contable
Indultos	Tramitación de Indultos
Actuaciones Policiales	Actuaciones de Fuerzas y Cuerpos de Seguridad con Fines Policiales
Servicio Militar	Tramitación del Servicio Militar
Formación Profesional	Formación Profesional Ocupacional
Acción a favor de Migrantes	Acción a Favor de Inmigrantes
Promoción y Servicios a la Juventud	Promoción Social a la Juventud
Promoción y Servicios a la Mujer	Promoción Social a la Mujer
Investigaciones Científicas o Médicas y Actividades Análogas	Investigación Epidemiológica y Actividades Análogas
Enseñanza Universitaria	Enseñanza Superior
Formación Profesional y Escuela Oficial de Idiomas	Enseñanzas Artísticas e Idiomas
Otras Enseñanzas, Becas y Ayudas a Estudiantes	Becas y Ayudas a Estudiantes
Padrón	Padrón de Habitantes
Concesión de Licencias y Autorizaciones	Concesión y Gestión de Permisos, Licencias y Autorizaciones
Otros	Otras Finalidades

En cuanto a los ficheros de titularidad privada, los principales factores que han determinado la ampliación de nuevas tipificaciones de finalidad son los siguientes:

- El análisis de la descripción de la finalidad declarada por los responsables de ficheros.
- Las nuevas formas de contratación de trabajadores en el mercado laboral.
- La generalización de tratamientos, tales como los análisis de perfiles, los sistemas de ayuda a la toma de decisione - segmentación de mercados.
- El uso cada vez más extendido de Internet, en el comercio electrónico, la prestación de servicios de telecomunica - ciones y los servicios de certificación para garantizar la seguridad de las comunicaciones.
- Prevención de Riesgos Laborales.
- La entrada en vigor de la nueva Ley 15/99 de Protección de Datos que amplía el ámbito de aplicación a los ficheros y tratamientos para la gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comu - nidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, que antes quedaban fuera del ámbito de aplicación de la LORTAD.

NUEVAS FINALIDADES
Gestión Contable, Fiscal y Administrativa
Gestión de Facturación
Gestión de Proveedores
Administración de Fincas

Recursos Humanos
Gestión de Nóminas
Gestión de Trabajo Temporal
Promoción y Gestión de Empleo
Prevención de Riesgos Laborales
Control Horario

Servicios Económico-Financieros y Seguros
Cumplimiento/Incumplimiento de Obligaciones Dinerarias

Publicidad y Prospección Comercial
Venta a Distancia
Análisis de Perfiles
Segmentación de Mercados
Sistemas de Ayuda a la toma de Decisiones
Recopilación de Direcciones

Servicios de Telecomunicaciones
Guías/Repertorios de Servicios de Telecomunicaciones
Comercio Electrónico
Asociación de Servicios de Certificación
Actividades Asociativas, Culturales, Recreativas, Deportivas y Sociales
Gestión de Actividades Culturales
Gestión de Asociados o Miembros de Partidos Políticos, Sindicatos, Iglesias, Confesiones o Comunidades Religiosas y Asociaciones,Fundaciones y Otras entidades sin ánimo de Lucro
Actividades Asociativas Diversas
Asistencia Social
Finalidades Varias
Fidelización de Clientes

En cuanto a la creación de nuevos tipos de finalidades, los principales factores que han influido, para los ficheros de titularidad pública, son:

- El análisis de la descripción de la finalidad declarada por los responsables de ficheros.

- La nueva Ley de Prevención de Riesgos Laborales.

- El control de la inmigración.

- La gestión de la tarjeta sanitaria implantada en las Comunidades Autónomas.

- La creación del Censo Promocional como nueva fuente de datos accesibles al público, según lo dispuesto en los artículos 3.j) y 31 de la Ley.

- Los servicios de certificación para garantizar la seguridad en las comunicaciones con las nuevas tecnologías.

DESCRIPCIÓN FINALIDAD
Recursos Humanos
Gestión de Nómina
Promoción y Selección de Personal, Oposiciones y Concursos
Prevención de Riesgos Laborales
Control Horario

Hacienda y Gestión Económico Financiera
Gestión de Facturación
Gestión Fiscal

Justicia
Registros vinculados con la Fe Pública (incluye a la antNacionalidad)

Seguridad Pública y Defensa
Solicitudes de Visado/Residencia

Trabajo y Bienestar Social
Acción a favor de Toxicómanos
Gestión de Tarjeta Sanitaria

Estadística
Gestión del Censo Promocional
Finalidades Varias
Registro de Entrada y Salida de Documentos
Otros Registros Administrativos
Atención al Ciudadano
Fines Científicos, Históricos o Estadísticos
Prestación de Servicios de Certificación

3.9 PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA

Las entidades que procedan a solicitar la inscripción de un fichero, deberán declarar, entre otros apartados de cumplimentación obligatoria, el *Origen o procedencia de los datos.*

En este apartado se estructuran los posibles tipos de procedencia de los datos, en los siguientes:

- El propio interesado o su representante legal
- Otras personas físicas distintas del afectado o su representante
- Fuentes accesibles al público
- Registros públicos
- Entidad privada
- Administraciones públicas

La tramitación de los expedientes de inscripción de ficheros o tratamientos ha puesto de manifiesto las dudas que se producen, por parte de los responsables de los ficheros, en la interpretación de estos conceptos, en relación con los preceptos legales que los regulan. En la mayor parte de los casos, estas dudas se han producido en el responsable cuando se le han solicitado las aclaraciones oportunas, antes de inscribir el fichero, de las distintas situaciones que se producían, en relación con la información consignada en este apartado.

Registros Públicos

La mayor parte de las veces, se justifica que se trataba de un error y han procedido a subsanar los datos consignados en su declaración. En muchos casos, habían declarado la procedencia de *Administraciones Públicas* y/o *Registros Públicos*, junto con la del *propio interesado o su representante legal*. En buena parte de estos casos, se trataba de responsables de ficheros que realizaban el tratamiento por cuenta de los propios clientes que contrataban sus servicios: gestores, administradores de la propiedad, consultores, asesores, etc. Como parte de dicha gestión tenían que acudir a determinados Registros Públicos, como el de la Propiedad, para contrastar los datos del propio interesado o solicitar las correspondientes certificaciones.

De acuerdo a la documentación aportada por el responsable, se deduce que el origen de los datos es ® el propio interesado o su representante legal ¯ y, por lo tanto, no procedía cumplimentar que los datos proceden de Registros Públicos.

A modo de ejemplo, se transcribe la justificación de un responsable cuya actividad es el asesoramiento de empresas: " La única vía, en cuanto a la procedencia de los datos, es la del propio interesado. Ahora bien, a partir de que la persona en cuestión solicita nuestros servicios y es cliente de nuestra empresa, es posible que necesitemos completar y/o ampliar los datos que el cliente nos remite (mercantiles, tributarios, laborales, etc.). Es por ello, que a partir de que una persona es cliente y actuando en **representación** de nuestro cliente y bajo su autorización, accedemos a las diversas fuentes existentes en el mercado para recabar dicha información".

En el caso a que se refiere este responsable, se deberá cumplimentar como origen de los datos, únicamente, *el propio interesado o su representante legal.* El resto de la información, se puede declarar como *procedimiento de recogida*, indicando en el texto de formato libre cualquier aclaración.

Desde el punto de vista de la protección de datos, en general, y desde el punto de vista de la tramitación de expedientes de solicitud de inscripción, en particular, son importantes estas aclaraciones, puesto que muchas de las personas que proceden a crear ficheros con datos de carácter personal, confunden el hecho de que la información inscrita en los Registros Públicos sea pública en los términos previstos para cada uno de ellos, con la posibilidad de que se pueda tratar esa información con finalidades incompatibles con la previsión de publicidad formal.

La mayoría de los responsables argumentan que dichos datos estaban accesibles al público con carácter general y concluyen que, por lo tanto, son de libre disposición y uso. Sin embargo, no tienen en cuenta que las únicas fuentes accesibles son las previstas en el artículo 3 ni tampoco los principios que se establecen en la Ley, que impide el tratamiento posterior de estos datos por terceros para finalidades no compatibles con la finalidades legítimas para las que se crean cada uno de los Registros Públicos.

No obstante, es oportuno aclarar, en relación con este apartado, que la Ley permite la recogida de datos desde los Registros Públicos, para realizar tratamientos cuya finalidad sea la prestación de servicios de información sobre solvencia patrimonial y crédito, según lo previsto en su artículo 29.1

Administraciones Públicas

Otra situación que también produce dudas es cuando se declaran datos cuyo origen o fuente son las Administraciones Públicas.

Cuando del contenido de la declaración, existen dudas razonables de que el origen de los datos fuesen las *Administraciones Públicas*, se ha procedido a solicitar aclaración al respecto. A veces, los responsables han contestado que habían cometido un error en la consignación de este apartado. En otros casos, han alegado que dicha procedencia era pertinente como fuente de datos, ya que por la actividad desarrollada por esa sociedad, los datos provenían de colaboraciones con las Administraciones Públicas. En este sentido, informaban de que la propia Administración les facilitaba información de las personas que ocupan responsabilidades públicas para la organización de diversos actos o certámenes o, que eran las propias Administraciones las que promovían los actos públicos.

En este caso normalmente, lo que se estaría produciendo, es un acceso a los datos de terceros por ser necesarios para la prestación de un servicio al responsable del fichero, en los términos del artículo 12 de la Ley. Por ello, habría que considerar que los datos facilitados por las Administraciones Públicas a terceros, no tendrían la consideración de cesión.

Fuentes accesibles al público

Otro de los casos en los que se pone de manifiesto cierta confusión al cumplimentar el modelo de solicitud de inscripción, se produce cuando se declara el censo promocional como origen de los datos del fichero o tratamiento.

En el citado modelo normalizado, se han tipificado las fuentes accesibles al público que la Ley cita en su artículo 3.j):

- Censo promocional
- Guías de servicios de telecomunicaciones
- Listas de personas pertenecientes a grupos profesionales
- Diarios y Boletines oficiales
- Medios de comunicación

Toda vez que el censo promocional, no se encuentra disponible para su uso, se procede a requerir a los responsables de ficheros que, declaraban que la procedencia de los datos era el censo promocional, advirtiéndoles de la necesidad de subsanar dicho error, ya que a fecha de cierre de esta memoria, no se ha producido el desarrollo reglamentario del censo promocional.

Conjuntamente con este requerimiento, se informa al responsable, en relación con las previsiones establecidas en el artículo 31 y la falta de desarrollo prevista en la Disposición Transitoria Segunda, que respectivamente señalan: "*Quienes puedan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral*", concluyendo en la Disposición Transitoria Segunda de la citada Ley que *"reglamentariamente se desarrollarán los procedimientos de formación del Censo Promocional* .

También ha sido muy común, por parte de los responsables, declarar que la procedencia de los datos obtenidos de Internet, podría ser considerada como fuente accesible al público, toda vez que los mismos figuraban en páginas web de acceso disponible para cualquier persona. Estos problemas se abordarán con mayor detalle en el apartado correspondiente a la declaración de tratamientos en Internet, ya que ha tenido una especial incidencia en la inscripción de ficheros relacionados con este medio.

3.10 CESIÓN O COMUNICACIÓN DE DATOS.

En el año 2000 se han inscrito 306 ficheros de titularidad pública (34,81% del total de ficheros inscritos) y 3.300 de titularidad privada (20,36% del total de ficheros inscritos) que declaran este apartado.

Los ficheros inscritos durante este año de titularidad pública han declarado ampararse en los distintos supuestos legales según los datos siguientes:

Supuestos	Nº ficheros	%
Con consentimiento de los afectados(art. 11.1)	177	57,84%
Existencia de una relación jurídica que implica necesariamente la conexión del fichero con ficheros de terceros (art. 11.1.c)	53	17,32%
Existencia de una norma reguladora que los autoriza (art.11.2a)	259	84,64%
datos recogidos de fuentes accesibles al público (art. 11.2.b)	26	8,50%
Competencias mismas materias (art. 21.1)	139	45,42%
Datos obtenidos o elaborados con destino a otra administración pública (art. 21.2)	124	40,52%
Tratamiento posterior de los datos con fines históricos, estadísticos o científicos (art. 11.2.e)	19	6,21%

Los ficheros de titularidad privada han declarado ampararse en los siguientes supuestos legales:

Supuestos	Nº ficheros	%
Con consentimiento de los afectados (art.11.1)	2.433	73,73%
Existencia de una relación jurídica que implica la conexión del fichero con ficheros de terceros (art.11.1.c)	1.595	48,33%
Existencia de una norma reguladora que los autoriza (11.2.a)	1.467	44,45%
Datos recogidos de fuentes accesibles al público (11.2.b)	212	6,42%

El total de ficheros inscritos con cesiones no corresponde a la suma de los datos que figuran en cada supuesto ya que un mismo fichero puede estar amparado en varios.

El nuevo modelo de notificación de ficheros prevé un nuevo supuesto legal para la cesión de un fichero de titularidad

pública, que es aquel en el que la comunicación de los datos tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos en los términos previstos del artículo 11.2.e).

Las incidencias que se plantean en este apartado no están relacionadas con la cumplimentación del mismo sino con las cuestiones de fondo que suponen las cesiones de datos.

Así, se declara la cesión de datos a terceros, en gran parte, empresas privadas, cuando en realidad se está llevando a cabo la prestación de un servicio mediante un encargado del tratamiento, en cuyo caso debería cumplimentarse el apartado de encargado del tratamiento en vez del de cesiones, además de haber cumplido el resto de las previsiones contempladas en el art. 12.

En este apartado y en relación con los ficheros de titularidad pública, el epígrafe en el que se consigna que la cesión se ampara en que está autorizada en una Ley según previsión del art. 11.2.a), se está consignando la norma de disposición general de creación del fichero como norma habilitante para la cesión, utilizando los términos previstos en el segundo inciso del art. 21.1 "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso".

Esta interpretación, a partir de la sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional no será posible dado que se ha dictado la inconstitucionalidad y nulidad del citado inciso.

No obstante, analizando la información declarada en los ficheros en los que se produce esta situación, se puede concluir que en la mayoría de los casos los órganos administrativos destinatarios de las cesiones son órganos de otras Administraciones Públicas con las mismas competencias que el responsable cesionario, por lo que, o están amparados en el primer inciso del art. 21.1. *"Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas"*, o en las previsiones generales de la cesión prevista en su art. 11.2.a) *"cuando la cesión este autorizada en una Ley".*

Otros casos, se producen cuando la cesión se realiza a otros órganos del mismo Ministerio o de otros Departamentos en previsión del cumplimiento de las funciones que encomienda el ordenamiento jurídico, por competencias y materias similares que estarían amparadas en el primer inciso del citado art. 21.1. Como ejemplo, se puede citar por su interés y porque se repite en muchas de las cesiones de datos realizadas al Instituto Nacional de Estadística a los efectos de cumplir las funciones previstas en la Ley 12/89 de Función Estadística Pública. Aunque las cesiones se hayan declarado amparadas en la disposición de creación del fichero ha sido debido a un error formal, toda vez que estas cesiones están habilitadas por la Ley de Función Estadística Pública. Asimismo, desde la entrada en vigor de la Ley también estaría amparada esta cesión en el artículo 11.2.e) anteriormente citado, cuando los destinatarios de las cesiones fueran organismos con competencia en materias relacionadas con fines históricos, estadísticos o científicos.

Esta circunstancia también se ha producido cuando se declaran cesiones a la Agencia Estatal de Administración Tributaria o al Instituto Nacional de Seguridad Social, que se encuentran reguladas en la Ley General Tributaria, 25/1995, y en la Ley General de la Seguridad Social, 1/1994, respectivamente.

Ante estas conclusiones obtenidas del estudio de los datos declarados e inscritos en el RGPD, se podría afirmar que la sentencia 292/2000 no va a corregir situaciones de fondo importantes, toda vez que las Administraciones Públicas estaban realizando las cesiones a otras administraciones amparándose en la Ley o en competencias idénticas cuando son otros órganos los que las ejecutan.

Es previsión de este Registro informar a los responsables que hubieran declarado las cesiones de esta forma para que procedan a revisar la inscripción, con este objetivo se van a remitir en el próximo año, a cada responsable una relación de estos ficheros para que procedan a subsanar los defectos y, en el caso que proceda, realicen únicamente la cesión amparándose en la previsión legal correspondiente.

Asimismo, se comunicará a las Administraciones Públicas las exigencias derivadas de la STC292/2000 con el fin de que se realicen la regularizaciones que en su caso procedan.

3.11 DISPOSICIÓN GENERAL DE CREACIÓN, MODIFICACIÓN O SUPRESIÓN DEL FICHERO (SÓLO TITULARIDAD PÚBLICA)

Como ya se ha indicado en esta memoria la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

El modelo de titularidad pública para notificar ficheros contiene un apartado en el que hay que consignar la referencia a esta disposición general.

Como requisito adicional, la notificación de un fichero de titularidad pública debe llegar al RGPD acompañada de una copia de esta publicación.

A continuación se relacionan las disposiciones generales que han sido publicadas en el BOE durante 2000, por responsables de la Administración General del Estado.

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

- RESOLUCIÓN de 1 de diciembre de 2000, del Consejo Superior de Deportes, por la que se acuerda la incorporación a la relación de ficheros de tratamiento automatizado de carácter personal: "Deportistas del programa de detección de talentos", "Personal administrativo, servicios profesionales y deportistas que reciben retribuciones, por parte de cualquiera de las federaciones deportivas nacionales", de conformidad con el artículo 20 de la Ley Orgánica 15/1999 (BOE nº 312, 29/12/2000)

- RESOLUCIÓN de 31 de agosto de 2000, del Consejo Superior de Deportes, por la que se crean los ficheros de tratamiento automatizado de datos de carácter personal del profesorado de los cursos de formación de Entrenadores Deportivos y de los diplomas y certificados que se expidan (BOE nº 260, 30/10/2000)

- RESOLUCIÓN de 6 de marzo de 2000, del Consejo Superior de Deportes, por la que se crean ficheros de tratamiento automatizado de datos de carácter personal de deportistas universitarios y entrenadores delegados (BOE nº 82, 05/04/2000)

MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES

- ORDEN de 15 de noviembre de 2000 por la que se crean, modifican y suprimen ficheros automatizados de datos de carácter personal gestionados por el Ministerio de Trabajo y Asuntos Sociales (BOE nº 291, 05/12/2000)

- ORDEN de 4 de enero de 2000 por la que se crean, modifican y suprimen ficheros automatizados de datos de carácter personal gestionados por el Ministerio de Trabajo y Asuntos Sociales (BOE nº 11, 13/01/2000)

MINISTERIO DE LA PRESIDENCIA

- ORDEN de 30 de septiembre de 2000 por la que se crean ficheros automatizados de datos de carácter personal (BOE nº 263, 02/11/2000)

MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACIÓN

- ORDEN de 19 de octubre de 2000 por la que se crea el fichero de agricultores asegurables para la gestión de los seguros de rendimientos incluidos en los Planes Anuales de Seguros Agrarios Combinados (BOE nº 258, 27/10/2000)

MINISTERIO DEL INTERIOR

- ORDEN de 21 de septiembre de 2000 por la que se regulan los ficheros automatizados para la identificación genética, ADN-Humanitas, restos humanos, y ADN-Veritas, vestigios biológicos, y muestras para cotejo, en la Dirección General de la Policía (BOE nº 233/2000, 28/09/2000)

MINISTERIO DE HACIENDA

- CORRECCIÓN de errores de la Orden de 21 de diciembre de 1999 por la que se aprueba la relación de ficheros automatizados de datos de carácter personal de la Agencia Estatal de Administración Tributaria (BOE nº 58, 08/03/2000)

- ORDEN de 21 de diciembre de 1999 por la que se aprueba la relación de ficheros automatizados de datos de carácter personal de la Agencia Estatal de Administración Tributaria (BOE nº 18, 21/01/2000)

MINISTERIO DE ADMINISTRACIONES PÚBLICAS

- CORRECCIÓN de errores de la Orden de 19 de mayo de 2000 por la que se modifica la de 22 de julio de 1994, reguladora de los ficheros de tratamiento automatizado de datos de carácter personal del Ministerio de Administraciones Públicas y sus entidades (BOE nº 151, 24/06/2000)

- ORDEN de 19 de mayo de 2000 por la que se modifica la Orden de 22 de julio de 1994, reguladora de los ficheros de tratamiento automatizado de datos de carácter personal del Ministerio de Administraciones Públicas y sus entidades (BOE nº 131, 01/06/2000)

MINISTERIO DE SANIDAD Y CONSUMO

- ORDEN de 25 de mayo de 2000 por la que se crean y regulan dos ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo, referidos al censo provisional y censo definitivo de personas con hemofilia u otras coagulopatías congénitas, que hayan desarrollado la hepatitis C, como consecuencia de haber recibido tratamiento o con concentrados de factores de coagulación en el ámbito del sistema sanitario público (BOE nº 131, 01/06/2000)

MINISTERIO DE DEFENSA

- ORDEN 86/2000, de 24 de marzo, por la que se modifica la Orden 75/1994, de 26 de julio, por la que se regulan los

ficheros de tratamiento automatizado de datos de carácter personal existentes en el Ministerio de Defensa (BOE nº 82, 05/04/2000)

MINISTERIO DE JUSTICIA

- ORDEN de 20 de marzo de 2000 por la que se modifica el anexo de la Orden de 26 de julio de 1994 por la que se regulan las ficheros con datos, de carácter personal, gestionados por el Ministerio de Justicia e Interior (BOE nº 80, 03/04/2000)

MINISTERIO DE FOMENTO

- RESOLUCIÓN de 1 de marzo de 2000, de la Comisión del Mercado de las Telecomunicaciones, por la que se crean el fichero automatizado del Registro de asignaciones y reservas de recursos públicos de numeración y el fichero de protocolo de la Comisión del Mercado de las Telecomunicaciones (BOE nº 71, 23/03/2000)

MINISTERIO DEL INTERIOR

- ORDEN de 7 de marzo de 2000 por la que se regula el fichero automatizado de identificación genética de vestigios biológicos (ADNIC), en la Dirección General de la Guardia Civil (BOE nº 71, 23/03/2000)

MINISTERIO DE MEDIO AMBIENTE

- ORDEN de 14 de diciembre de 1999 que modifica la de 9 de julio de 1998 por la que se crean los ficheros automatizados de datos de carácter personal del Ministerio de Medio Ambiente (BOE nº 17, 20/01/2000)

MINISTERIO DE SANIDAD Y CONSUMO

- ORDEN de 14 de diciembre de 1999 por la que se crean y se regulan ficheros automatizados con datos de carácter personal, gestionados por el Ministerio de Sanidad y Consumo (BOE nº 17, 20/01/2000)

MINISTERIO DE ECONOMIA

- RESOLUCIÓN de 11 de noviembre de 1999, de la Comisión Nacional de Energía, por la que se crean ficheros automatizados de datos de carácter personal en este organismo (BOE nº 15, 18/01/2000) Esta disposición fue publicada por el extinguido Ministerio de Industria y Energía del que dependía este organismo.

- RESOLUCIÓN de 4 de abril de 2000, de la Comisión Nacional del Sistema Eléctrico, por la que se suprimen ficheros automatizados de datos de carácter personal de este organismo (BOE nº 102, 28/04/2000) Esta disposición fue publicada por el extinguido Ministerio de Industria y Energía del que dependía este organismo.

En relación con las administraciones de Comunidades Autónomas, a continuación se relacionan las referencias de publicación en los diarios oficiales correspondientes de las disposiciones generales que han sido publicadas a los efectos de creación, modificación o supresión de ficheros de datos personales:

COMUNIDAD AUTÓNOMA DE ANDALUCÍA

- Resolución de 7/11/00 del Instituto de Fomento BOJA 136 de 25/11/00

COMUNIDAD AUTÓNOMA DE ILLES BALEARS

- Decreto 2/2000 de la Consejería de Interior BOCAIB 9 de 20/01/00

COMUNIDAD AUTÓNOMA DE CANARIAS

- Orden de 18/05/00 de la Consjería de Presidencia BOC 65 de 25/05/00

COMUNIDAD AUTÓNOMA DE CASTILLA LA MANCHA

- Ordenes de 27 de abril, 22 y 23 de mayo de la Consejería de Sanidad DOCM 48 y 56 de 19/05/00 y 9/06/00

COMUNIDAD AUTÓNOMA DE CASTILLA LEÓN

- Ordenes de 10 de mayo y 14 de julio de la Consejería de Industria, Comercio y Turismo BOC y L 102, 113, 130 y 153 de 29/05/00, 13/06/00, 10/05/00 y 08/08/00

COMUNIDAD AUTÓNOMA DE CATALUÑA

- Decreto 166/00 de 2 de mayo de la Consejería de Sanidad y Seguridad Social DOGC 3139 de 15/05/00

COMUNIDAD AUTONOMA DE EXTREMADURA

- Orden de 2 de junio de la Consejería de Educación DOE 69 de 15/06/00

COMUNIDAD AUTONOMA DE MADRID

- Decretos 339/99, 15/00, 4/00, 50/00, 93/00, 48/00 y 240/00, de 23/12/99, 3/02/00, 16/03/00, 30/03/00, 25/05/00, 23/03/00 y 02/11/00, respectivamente de la Consejería de Economía y Empleo. BOCM 13, 59, 79, 87,132, 219 y 278, de 17/01/00, 10/03/00, 3/04/00, 12/04/00, 5/06/00, 14/09/00, 22/11/00

- Decretos 17/00, 78/00, 110/00, 190/00, 233/00, 236/00 y 248/00, de 2/02, 4/05, 1/06, 31/07, 19/10, 26/10 y 16/11, respectivamente, de la Consejería de Sanidad BOCM 39 de 16/02/00, 118 de 19/05/00, 140 de 14/06/00, 187 de 8/08/00, 258 de 30/10/00, 283 de 28/11/00, 270 de 13/11/00

- Decretos 18/00, 19/00, 28/00 y 90/00, de 10/02, 24/02 y 25/05 de la Consejería de Hacienda. BOCM 40 de 17/02/00, 53 de 3/03/00 y 127 de 30/05/00.

- Decreto 96/00, de 26/05 de la Consejería de Presidencia. BOCM 126 de 29/05/00

- Decretos 133/00, 187/00, 188/00, 208/00 y 235/00, de 8/06 y 31/07, 14/09 y 26/10 de la Consejería de Educación. BOCM 142 de 16/06/00, 186 de 7/08/00, 186 de 7/08/00, 229 de 26/09/00, 262 de 3/11/00

- Decreto 217/00 de 21 de septiembre de la Consejería de Servicios Sociales. BOCM 280 de 24/11/00

- Decreto 221/00 de 28 de septiembre de la Consejería de Justicia, Función Pública y Administración Local. BOCM 238 de 6/10/00

- Decretos 223/00 y 236/00 de 28/09 y 26/10 de la Consejería de Medio Ambiente. BOCM 240 de 9/10/00 y 270 de 13/11/00

- Decreto 229/00 de 19/10 de la Consejería de Obras Públicas, Urbanismo y Transporte. BOCM 55 de 26/10/00

COMUNIDAD AUTÓNOMA DE MURCIA

- Orden de 20/06/00 de la Consejería de Economía y Hacienda. BORM 150 de 30/06/00

COMUNIDAD AUTÓNOMA DE NAVARRA

- Orden Foral 31/00, de 13 de marzo, de la Consejería de Presidencia, Justicia e Interior BON 42 de 05/04/00.

- Orden Foral 96/00, de 22 de junio, de la Consejería de Industria, Comercio, Turismo y Trabajo. BON 80 de 03/07/00

COMUNIDAD AUTÓNOMA DEL PAÍS VASCO

- Orden de 22 de febrero del Departamento de Hacienda y Administración Pública BOPV 51 de 14/03/00

COMUNIDAD AUTÓNOMA DE LA RIOJA

- Salud y Servicios Sociales BOLR 55 de 29/04/00 (Orden 9/2000 de 20/04)

- Turismo y medio ambiente BOLR /2000 (Orden 14/2000 de 28/05)

- Turismo y medio ambiente BOLR 63 de 18/05/2000 (Corr. de errores Orden 14/2000 de 28/05)

- Agricultura, Ganaderia y Desarrollo rural BOLR 128 de 14/10/00 (Orden 39/00 de 06/10)

- Salud y Servicios Sociales BOLR 152 de 07/12/00 (Corr. de errores Orden 9/2000 de 24/04)

COMUNIDAD AUTÓNOMA DE VALENCIA

- Justicia y Administraciones Publ. DOGV 3700 de 02/03/00 (Orden de 10/02/00)

- Justicia y Administraciones Publ. DOGV 3722 de 03/04/00 (Orden de 08/03/00)

- Sanidad DOGV 3815 de 16/08/00 (Orden de 31/05/00)

- Cultura y Educación DOGV 3807 de 03/08/00 (Orden de 28/07/00)

- Justicia y Admones. Públicas DOGV 3846 de 28/09/00 (Orden de 22/09/00)

- Presidencia DOGV 3894 de 11/12/00 (Orden de 15/11/00)

4. INSCRIPCIONES SECTORIALES

4.1 DECLARACIÓN DE TRATAMIENTOS INTERNET: COMERCIO ELECTRÓNICO, PORTALES, PÁGINAS WEB

Por su especial incidencia en la privacidad de las personas y el aumento que se ha producido en el uso de este medio, se ha procedido a incluir un apartado específico sobre los problemas relacionados con la red de Internet y sus consecuencias en la inscripción de ficheros en el RGPD.

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre comercio electrónico), reitera en su considerando 14 la aplicación de la norma de protección de datos personales en los tratamientos que se realizan en Internet o utilizan Internet como medio: "*La protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personal circulación de los datos y la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa a los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que son enteramente aplicables a los servicios de la sociedad de la información. Dichas Directivas establecen ya un marco jurídico comunitario en materia de datos personales y, por tanto, no es necesario abordar este aspecto en la presente Directiva para garantizar el correcto funcionamiento del mercado interior, en particular la libre circulación de los datos personales entre Estados miembros. La aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios* ...".

Durante el año 2000, ha continuado incrementándose el número de solicitudes de inscripción de ficheros en el RGPD, cuyos responsables declaraban que el tratamiento objeto de notificación, tenía alguna relación con Internet, ya fuese como origen de los datos o como medio de tratamiento.

Para declarar que se utiliza Internet como origen de los datos, se puede cumplimentar el apartado de *Procedencia y procedimiento de recogida de los datos* del modelo normalizado. Este apartado consta de tres epígrafes*: Procedencia de los datos*, *Procedimiento de recogida* y *Soporte utilizado para la obtención*. Dentro del procedimiento de recogida, se incluye la *Transmisión electrónica de datos/Internet*, y como soporte utilizado, aparece *Vía telemática*. Además, el responsable dispone de campos de texto libre para indicar cualquier aclaración que estime oportuna acerca del origen de los datos.

Igualmente, para declarar que se utiliza Internet como medio de tratamiento, los responsables de ficheros pueden utilizar el apartado de *Sistema de tratamiento*. Se ha incluido en este apartado la posibilidad de indicar la dirección de la página web. En este mismo sentido, se han incluido en el citado modelo, nuevas finalidades normalizadas que están relacionadas con este tipo de tratamientos, entre otras, la de comercio electrónico.

Actividades que utilizan Internet como medio de recogida o tratamiento de datos personales:

Los responsables de tratamientos han notificado en sus declaraciones de inscripción que utilizan Internet para alguna de las siguientes actividades:

- Comercio electrónico: Se incluyen tratamientos entre empresas y particulares, así como entre empresas y empresas.

- Portales de contenidos diversos: Incluyen datos personales de los usuarios del portal, de los usuarios que crean páginas web dentro de dichos portales, datos personales de participantes en concursos que se desarrollan dentro del portal, etc.

- Prestadores de servicios: Se incluyen empresas cuyo sector de actividad es el de las telecomunicaciones, que además de declarar los ficheros necesarios para su gestión, declaran tratamientos que se refieren a servicios de comercio electrónico.

- Recopilación de direcciones: Se incorporan listas de direcciones de personas pertenecientes a grupos, profesiones, gustos, envío de felicitaciones, venta de datos para publicidad directa, etc.

- Gestión de anuncios en portales y páginas web.

- Páginas web de temas diversos: entretenimiento, concursos, salud, contactos, inserción del curriculum en la red

- Empresas convencionales que han instalado algún tipo de servicio en la red: (p.e. Banca electrónica).

- Gestión de moneda virtual

La recogida de datos en Internet:

Durante la tramitación de inscripción de ficheros relativos a alguna de las actividades descritas anteriormente, se ha puesto de manifiesto que los tipos de datos de carácter personal que se recogen para el tratamiento, se refieren en su mayor parte a:

- Datos de carácter identificativo: nombre, apellidos dirección de correo electrónico

- Datos de características personales: fecha de nacimiento, sexo, nacionalidad

- Datos académicos y profesionales: formación, titulaciones

- Datos de circunstancias sociales: aficiones y estilo de vida

- Datos de detalles de empleo: profesión, datos no económicos de nómina, historial del trabajador

- Datos económico-financieros: tarjeta de crédito, datos bancarios

- Datos de transacciones: bienes y servicios recibidos por el afectado.

En muy pocos casos se han declarado la utilización de datos especialmente protegidos en tratamientos relacionados con Internet. La actividad de los responsables que declaran este tipo de datos, se enmarca en diversos sectores. Cabe señalar los que se refieren a actividades sanitarias, gabinetes médicos y psicológicos, con la finalidad de mantener el historial clínico *on-line* y sitios web, cuya finalidad es la de facilitar los encuentros personales, en los que los interesados cumplimentan datos relacionados con sus creencias religiosas o, sus preferencias sexuales, con el fin de facilitar intercambios personales.

En algunas declaraciones de inscripción de ficheros, se ha observado que el único dato de carácter personal que trataban era la dirección de correo electrónico. Normalmente dichas solicitudes de inscripción, han sido acompañadas de consultas en las que se solicitaba información acerca de si la dirección de correo electrónico se consideraba un dato de carácter personal desde la perspectiva de la LOPD.

La norma general de interpretación, se podría desprender de las conclusiones recogidas en el documento de trabajo: *Tratamiento de datos personales en Internet*, aprobado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 23 de febrero de 1999, y que comparte la opinión de la Conferencia Europea de Comisarios sobre Protección de Datos, que establece que "*El tratamiento de datos personales en Internet debe respetar los principios de protección de datos al igual que el mundo normal (off-line)...La Directiva 95/46/CE, de carácter general sobre protección de datos hace referencia a cualquier tipo de tratamiento de datos personales dentro de su campo de acción, con independencia de los medios técnicos utilizados. Por consiguiente, el tratamiento de datos personales en Internet debe considerarse a la luz de la Directiva* ".

Por lo tanto, se puede concluir que, con carácter general, el dato del correo electrónico de una persona física, sería un dato de carácter personal y, por consiguiente el fichero o tratamiento que utilizara este dato, estaría incluido en el ámbito de la LOPD. No obstante, este criterio no impide que deba analizarse cualquier otra situación, que tenga una problemática más particular.

Sobre la procedencia de los datos en este medio, la mayor parte de los responsables han declarado que los datos proceden del propio interesado, recogidos en el momento de la identificación en la página web, normalmente mediante formularios que tiene que cumplimentar antes de obtener determinado servicio o, registrando sus datos para acceder al resto de la información.

En otros casos, se han solicitado inscripciones de ficheros cuyos responsables declaraban que los datos de carácter personal se obtenían de fuentes accesibles al público, señalando que dicha fuente era Internet.

Según lo establecido en el artículo 30 de la Ley "*quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en* **fuentes accesibles al público** o cuando hayan sido **facilitados por los propios interesados** u obtenidos con su consentimiento".

Solamente tendrán la consideración de fuentes accesibles al público las expresadas en el artículo 3.j) de la citada Ley y son: el censo promocional; los repertorios telefónicos en los términos previstos por su normativa específica; las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo; los Diarios y Boletines Oficiales y los medios de comunicación.

Se puede establecer, como conclusión, que no se considera que la procedencia de los datos recogidos en Internet sea la de fuente accesible al público, siendo necesario, por lo tanto, la obtención del consentimiento inequívoco, específico e informado del afectado para realizar tratamientos con sus datos personales publicados en Internet, aunque éstos se hayan publicado de forma que cualquier internauta pueda acceder a los mismos. Consideración aparte, merecería la circunstancia en la que con el consentimiento inequívoco, específico e informado del interesado, se publicaran sus datos para poder ser tratados en los términos y finalidades consentidas por el propio interesado.

Otro procedimiento de recogida de datos de carácter personal en Internet, serían los denominados tratamientos invisibles, denominación utilizada también por el Grupo Operativo de Internet en la Recomendación 1/99 del grupo de trabajo sobre el tratamiento invisible y automático de datos personales en Internet efectuados por software y hardware.

Según este documento son ejemplos típicos de "tratamiento invisible": "*el chatering en el nivel HTTP, los hipervínculos automáticos a terceros, el contenido activo (como Java, ActiveX u otras tecnologías que ejecutan scripts en el cliente) y el mecanismo cookies en su aplicación actual en los navegadores usuales".*

Cuando al proceder a tramitar estas solicitudes de inscripción, ha sido necesario solicitar aportación de documentación adicional, por ejemplo, para justificar el consentimiento del afectado para la realización de transferencias internacionales a algún país que no proporciona un nivel de protección equiparable, estos responsables de tratamientos han aportado como documentación la política de privacidad incluida en su página web.

En dicha documentación se ha puesto de manifiesto, la realización de tratamientos invisibles por medio de "*cookies*" que no se declaraba en el momento de solicitar la inscripción en el RGPD. En estos casos, se ha requerido al responsable del fichero para que subsane la solicitud de inscripción, incluyendo el uso de este tipo de datos en su declaración en el apartado de *Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero,* señalando alguna de las tipologías de datos que se incluyen en dicho apartado o, indicándolo en cualquiera de los espacios de texto libre.

También se ha puesto de manifiesto la utilización de estos mismos tratamientos invisibles por medio de "*cookies*", como consecuencia del Plan de Inspección sobre comercio electrónico que la Inspección de Datos ha llevado a cabo (citado en detalle en el apartado correspondiente de esta memoria). Únicamente será lícito el tratamiento de estos datos con la finalidad de personalizar los futuros accesos a la página web, cuando así lo haya manifestado o solicitado el afectado. Igualmente, se ha requerido al responsable del fichero para que incluya este tipo de datos en el apartado correspondiente, en los mismos términos que lo señalado anteriormente.

Sin embargo, no se podrá almacenar la información suministrada por las "*cookies*", con la finalidad de obtener una evaluación de la personalidad, si no es con el consentimiento inequívoco del afectado, lo que supondrá que su manifestación de voluntad sea libre, específica e informada.

Existen otros tipos de procesos paralelos a los "tratamientos invisibles", cuyo fin es obtener una segmentación y una elaboración de perfiles, a partir del análisis de un gran número de datos concernientes a las personas. Aunque estos tratamientos de análisis de perfiles no son exclusivos de los tratamientos realizados a través de Internet, han experimentado un gran aumento debido a la cantidad de datos personales que pueden ser recabados en la red. Este fenómeno ha sido destacado por María de los Reyes Corripio, "*la aparición de las técnicas de geomarketing que añaden valor informativo a una dirección, alienta a los operadores de mercado a recoger el mayor número posible de direcciones* ". Además de ésto, dicha información se registra en el almacén de datos (*Datawarehouse)* o el *datamart* de marketing, para posteriores tratamientos con datos de los suscriptores o procedentes de datos demográficos relacionados con el código postal y datos de fuentes accesibles al público , con lo que se puede obtener una visión muy completa del comportamiento de las personas.

En cualquier caso, para que estos tipos de tratamientos se realicen de una manera lícita desde el punto de vista de la protección de datos, es necesario contar con el consentimiento del afectado. Para ello se le tiene que informar tanto de la realización de dichos tratamientos, como de la finalidad de los mismos. También debe ser informado de las consecuencias, si las hubiera, de la falta de aceptación de estos tratamientos.

El principio de calidad de los datos:

Según lo dispuesto en el artículo 4 de la LOPD, en su apartado primero, "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido* ".

Es de reseñar la progresiva toma de conciencia de los responsables que operan en este medio sobre la necesidad de incluir políticas de privacidad transparentes en lugares visibles de su página web. En este sentido, es de señalar la influencia que ha tenido la difusión del Código Ético de Protección de Datos Personales en Internet, adoptado por la Federación Española de Comercio Electrónico y Marketing Directo, inscrito en el RGPD desde el año 1998.

Una política de privacidad transparente deberá facilitar, al usuario, al menos la siguiente información:

1. Identificación de la razón social del responsable del fichero.

2. La finalidad o finalidades a que se destinan los datos de carácter personal.

3. La identificación de los destinatarios cuando se tenga previsto la realización de cesiones o comunicaciones de datos, especificando la información a ceder así como la finalidad de dicha comunicación de datos.

4. La identificación clara del país y de la razón social de los destinatarios cuando se tenga previsto la realización de transferencias internacionales de datos especificando la información a ceder así como la finalidad de dicha transferencia internacional de datos.

5. La solicitud clara de consentimiento cuando los datos son recogidos del propio interesado.

6. La existencia de derechos de oposición, acceso, rectificación y cancelación de los datos, especificando una dirección del correo electrónico, así como una dirección postal para poder ejercerlos.

7. Información referente al uso de tratamientos invisibles, bien sea para, informar de que no utiliza este tipo de tratamientos o, en el en los utilizara, una indicación de la finalidad de los mismos y una solicitud del consentimiento. Algunos responsables incluyen información acerca de las opciones que incluyen los navegadores con relación a las "*cookies*", para que los usuarios puedan aceptar o no el envío de las mismas.

8. Las medidas de seguridad adoptadas en relación con el tratamiento de sus datos personales.

9. Información acerca de la seguridad en la transmisión de los datos, especificando si la comunicación se establece a través de un canal seguro, si los datos se transmiten cifrados o no, etc.

10. Política del responsable del tratamiento acerca del envío de comunicaciones no solicitadas.

Problemas específicos en relación con la inscripción de ficheros.

Durante la tramitación de los expedientes de inscripción, se han constatado las dudas existentes a la hora de determinar quién es el responsable del tratamiento, quién el encargado del mismo y su relación con el dominio de Internet dónde se producía la recogida o el tratamiento de los datos personales.

Esta situación, además, se hace más compleja con la determinación de dónde se ubica el equipo informático que hace de servidor del sitio web para estos tratamientos de datos personales, ya que el responsable del fichero está obligado a declarar la ubicación física del fichero en la solicitud de la inscripción. En este mismo sentido hay que advertir de que, si el equipo servidor estuviera ubicado en otro país, se estaría produciendo una transferencia internacional de datos, según lo previsto en el artículo 33 de la Ley, que es preceptivo declarar en el correspondiente apartado de *Transferencias internacionales* .

Datos de tráfico y facturación en las telecomunicaciones

La legislación sobre los datos de tráfico se establece en la Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, transpuesta a nuestro derecho interno por la Ley General de Telecomunicaciones y el Real Decreto 1736/1998 que la desarrolla. Así en el artículo 6 de esta Directiva se establece que "... *los datos sobre tráfico relacionados con los usuarios y abonados tratados para establecer comunicaciones y almacenados por el proveedor de una red o servicio público de telecomunicación deberán destruirse o hacerse anónimos en cuanto termine la comunicación*". No obstante, en los apartados 2 y 3 del citado artículo se especifica que el proveedor de un servicio público de telecomunicaciones podrá tratar los datos a los efectos de facturación de los usuarios y de los pagos de interconexiones hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. Para que el proveedor de un servicio público de telecomunicaciones pueda tratar este tipo de datos para la promoción comercial de sus propios servicios de telecomunicación, deberá contar con el consentimiento del abonado .

Por lo tanto, cualquier fichero o tratamiento que almacene y trate este tipo de datos, necesarios para mantener la relación contractual entre usuarios y prestadores de servicios, están dentro del ámbito de aplicación de la Ley y, por lo tanto será necesario su notificación al RGPD para su inscripción.

Asimismo, en este tipo de tratamiento, únicamente se podrán utilizar los datos a los efectos de suministrar el servicio correspondiente y sería incompatible el tratamiento de datos para cualquier finalidad relacionada con la forma de comportamiento del cliente a través de sus datos de navegación o facturación.

La propuesta de revisión de la Directiva 97/66/CE, hace una definición sobre datos de tráfico como *"cualquier dato tratado en el curso de o a efectos de la transmisión de una comunicación a través de una red de comunicaciones electrónicas"*.

Conviene hacer una referencia al Dictamen 7/2000 emitido por el Grupo de Trabajo en relación con la definición prevista en la propuesta de modificación de la Directiva 97/66/CE, que opina que la citada definición *"implica que todos los datos sobre tráfico generados durante una comunicación, deben destruirse una vez finalizada la misma. La definición incluye asimismo los datos de navegación (como URL o localizadores unificados de recursos), que pueden revelar intereses personales de los particulares (por ejemplo, sitios web que pueden ofrecer indicaciones sobre las creencias religiosas, las ideas políticas, la salud o la vida sexual de quienes los frecuentan). Al indicar exactamente las páginas de un sitio web que han sido visitas, revelan el contenido exacto al que ha podido acceder el particular.*

Puesto que los datos sobre tráfico pueden incluir este tipo de información personal, deberían estar revestidos de la confidencialidad prevista para las comunicaciones".

4.2 DECLARACIÓN DE FICHEROS CON FINES DE INVESTIGACIÓN EN LA INDUSTRIA QUÍMICA Y FARMACÉUTICA

Durante el año 2000, se ha incrementado el número de notificaciones de ficheros de entidades pertenecientes a la industria química y farmacéutica. Las declaraciones de inscripción de estos ficheros incluyen como finalidad los estudios que los laboratorios y entidades del sector farmacéutico vienen desarrollando sobre ensayos clínicos, estudios epidemiológicos y farmacovigilancia.

A lo largo del ejercicio, se han inscrito en el RGPD, 428 ficheros que declaran la finalidad de gestión y control sanitario, 184 con la finalidad de investigación epidemiológica y actividades análogas y 4.080 con fines históricos, científicos o estadísticos. De este total de ficheros declarados, 552 corresponden a 175 entidades de este sector de actividad.

Entre la información contenida en este tipo de ficheros se encuentran datos especialmente protegidos, de origen racial o étnico, salud y/o vida sexual. Como norma general y sin perjuicio de los requisitos adicionales que exige la normativa sanitaria para recabar, tratar y ceder este tipo de datos es necesario el consentimiento informado del afectado o su representante. Sin embargo, las posibles cesiones, a la Administración del Estado y a las Comunidades Autónomas que ostenten competencias de ejecución en materia de productos farmacéuticos, de datos relativos a las reacciones adversas de los medicamentos, se realizan en base a la obligación recogida en la Ley del Medicamento y en la Ley General de Sanidad.

Existen ciertas dudas en la interpretación por parte del responsable para determinar si sus ficheros estarían dentro del ámbito de la Ley Orgánica, cuando en los mismos solo se recogen, como datos de carácter identificativo, las iniciales de los afectados, de acuerdo a los protocolos del proyecto.

La cuestión que se plantea es si los datos se pueden considerar suficientemente disociados, o por el contrario se pueden considerar como razonablemente identificables.

En este sentido el artículo 3.f) de la Ley considera procedimiento de disociación a *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable".*

Por otra parte, el art. 3.a) considera como dato de carácter personal *"cualquier información concerniente a personas físicas identificadas o identificables".* Por lo tanto la inclusión de otro tipo de datos en el fichero será el determinante para apreciar si la persona es identificada o identificable. En este último caso también deberán ser notificados para su inscripción.

En los ficheros de ensayos clínicos y estudios epidemiológicos, normalmente la información relativa al origen racial o étnico, a la salud y a la vida sexual que es sometida a tratamiento automatizado no contiene la identificación directa de los afectados ya que en los Cuadernos de Recogida de Notas (formularios sujetos al Protocolo de cada ensayo clínico y autorizados por las autoridades sanitarias) sólo constan las iniciales del paciente y algún otro dato como fecha y lugar de nacimiento, datos de situación familiar, etc. Los encargados de cumplimentar y facilitar a los responsables de los ficheros dichos Cuadernos son los centros sanitarios que participan en los ensayos clínicos. La existencia de un número de Código en estos Cuadernos de Recogida de datos podría suponer un nexo de unión con la historia clínica del paciente, lo que le hace identificable y por lo tanto que el fichero esté incluido en ámbito de aplicación de la Ley.

En este sector es frecuente la notificación de transferencias internacionales de datos en sus ficheros, siempre amparadas en el consentimiento informado, expreso y por escrito. Esto es debido a que muchas de estas empresas son parte de un Grupo multinacional, cuyo empresa matriz está ubicada en el extranjero y a que normalmente estos proyectos se realizan de forma compartida con otros centros de investigación.

4.3 DECLARACIÓN DE FICHEROS DE UNIVERSIDADES

Durante este año se han inscrito en el RGPD los ficheros correspondientes a la Universidad Católica Santa Teresa de Jesús de Avila, de titularidad privada, y un nuevo fichero de la Universidad Miguel Hernández, de titularidad pública.

Las Universidades Pablo de Olavide de Sevilla y la Universidad Rey Juan Carlos, que al cerrar la memoria anterior habían comunicado que se encontraban en el periodo de puesta en marcha de sus sistemas informáticos han elaborado las disposiciones generales de creación de sus ficheros que fueron remitidas al BOE para su publicación habiendo sido devueltas por este Organismo, rechazando la publicación, argumentando que debían ser publicadas en el diario oficial de la Comunidad Autónoma correspondiente, porque en opinión de este organismo las Universidades son administraciones integradas en las Comunidades Autónomas.

Al cierre de esta memoria, quedan inscritos los ficheros de ambas Universidades, en base a las Resoluciones de 3 de abril de 2000, de la Universidad Pablo de Olavide (BOJA nº 121, de 21-10-2000) y de 26 de mayo de 2000 de la Universidad Rey Juan Carlos (BOCAM nº 164, de 12-7-2000).

5. TRANSFERENCIAS INTERNACIONALES DE DATOS

La Ley 15/1999 ha establecido en el título V artículos 33 y 34 el régimen al que han de someterse los movimientos internacionales de datos.

Artículo 33. Norma general

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Para realizar transferencias de datos de carácter personal a algún país que no proporciona un nivel de protección equiparable al que presta la LOPD, además de haberse observado lo dispuesto en la Ley, se deberá obtener autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

Con carácter general, habrá de estarse a lo dispuesto en el artículo 33 de la Ley. No obstante, el artículo 34 excepciona de la norma general, los siguientes supuestos:

a) *Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.*

b) *Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.*

c) *Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.*

d) *Cuando se refiera a transferencias dinerarias conforme a su legislación específica.*

e) *Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.*

f) *Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.*

g) *Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.*

h) *Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.*

i) *Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.*

j) *Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.*

k) *Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.*

Si la transferencia internacional de datos no se encuentra amparada en ninguno de los supuestos citados en el artículo 33, se deberá solicitar la preceptiva autorización de transferencia internacional.

En caso contrario, se deberá aportar la documentación que acredite cualquiera de los supuestos del artículo 34 de la Ley en el que se ampare la transferencia sin previa autorización.

En todo caso, siempre será necesario especificar tanto el país destinatario de la transferencia internacional como la razón social completa de la empresa destinataria.

Aunque en la LORTAD ya existía la previsión legal de autorizar las transferencias internacionales cuando los países de destino no tuvieran un nivel de protección equiparable al nuestro, la Agencia de Protección de Datos venía resolviendo las preceptivas autorizaciones de transferencias internacionales cuando se aportaban garantías suficientes.

El movimiento internacional de datos de carácter personal ha sido una de las cuestiones que ha suscitado mayores dudas a los responsables de los ficheros y a la sociedad en general.

La actuación de la APD ha generado una abundante casuística relacionada con las transferencias internacionales de datos de carácter personal que no venía recogida sistemáticamente en ningún texto.

Por todo ello, en uso de la competencia del Director de la Agencia de Protección de Datos para "*dictar instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley*", se dicta la Instrucción 1/2000, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos, publicada en el Boletín Oficial del Estado el día 16 de diciembre.

La Instrucción 1/2000 tiene por objeto señalar los criterios orientativos seguidos por la Agencia de Protección de Datos en relación con aquellos tratamientos que supongan una transferencia internacional de datos, poniendo de manifiesto el procedimiento que se sigue cada caso concreto. La finalidad de esta Instrucción es aclarar y facilitar a todos los interesados en un único texto, el procedimiento seguido para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos.

En este sentido, deben tenerse en cuenta las recientes Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE y 2000/520/CE, de 26 de julio, (publicadas en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000), que consideraron adecuado el nivel de protección de datos personales en Suiza, Hungría, así como "el conferido por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos".

La Decisión 2000/520/CE ha considerado que los principios de puerto seguro, aplicados de conformidad con la orientación que proporcionen las preguntas más frecuentes (en lo sucesivo "FAQ") publicadas por el Departamento de Comercio de Estados Unidos de América, que figuran en el anexo II de la citada Decisión, garantizan un nivel adecuado de protección de los datos transferidos desde la Comunidad a entidades establecidas en Estados Unidos.

En relación con cada transferencia de datos se deberán cumplir entre otras condiciones, las siguientes:

- La entidad receptora de los datos deberá haber manifestado de forma inequívoca y pública su compromiso de cumplir los principios aplicados de conformidad con las FAQ.

- Se considerará que la entidad cumple las condiciones a partir de la fecha en que notifique al Departamento de Comercio de los Estados Unidos el compromiso de cumplir los principios de puerto seguro.

- Para ello la entidad deberá autocertificar su adhesión y notificarlo al Departamento de Comercio de Estados Unidos de América.

- La entidad deberá estar sujeta a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el anexo VII de la Decisión.

Por lo tanto, para considerar que una entidad en Estados Unidos proporciona un nivel de protección equiparable, será necesario que la entidad destinataria de los datos, cumpla las garantías previstas en la Decisión de la Comisión.

Análisis del apartado de Transferencias Internacionales a efectos de inscripción de ficheros

El total de ficheros inscritos en el RGPD que declaran transferencias internacionales a 31 de diciembre de 2000 es de 1.352 de los cuales 51 corresponden a inscripciones de titularidad pública y 1.301 de titularidad privada.

Los ficheros inscritos en 2000 que contienen en su declaración transferencias internacionales de datos han sido 272.

A tenor de las excepciones contempladas en el artículo 34 de la Ley, las transferencias internacionales de datos en 2000 se han declarado amparándose en los siguientes supuestos:

SUPUESTOS LEGALES	TIT. PUBLICA	TIT.PRIVADA
Se efectúa con destino a algún país de los citados en el reglamento con nivel de protección equiparable	2	221
Se ampara en tratado o convenio del que España forma parte	0	7
Se realiza a efectos de prestar auxilio judicial internacional	0	1
Es necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios	1	1
Se refiere a transferencias dinerarias, conforme a su legislación específica	0	11
El afectado ha dado su consentimiento	1	88
Es necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a peticiónde l afectado	0	33
Es necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.	0	9
Es necesaria o legalmente exigida para la salvaguarda de un interés público	0	1
Se efectúa, a petición de persona con interés legítimo, desde un registro público y es acorde con la finalidad del mismo	0	1

La inclusión en la nueva Ley del consentimiento del afectado como excepción a la preceptiva autorización necesaria en la LORTAD, ha supuesto un cambio importante en la resolución de este tipo de expedientes.

Desde la entrada en vigor de la LOPD no ha sido necesario autorizar aquellas transferencias internacionales amparadas en las excepciones previstas en el artículo 34 cuando el país destinatario era de distinto nivel de protección. No obstante, ha sido práctica habitual en el RGPD exigir documentación y garantías que avalasen las circunstancias en las que se amparaba el declarante.

Se han inscrito, durante el año 2000, un número de 69 ficheros que declaran la transferencia internacional de datos a países con distinto nivel de protección, amparándose en el consentimiento dado por el afectado. Todo lo anterior justifica que únicamente se hayan tramitado 2 expedientes de autorización de transferencias internacional, dado que eran los únicos casos en los que no existía uno de los supuestos previstos en el artículo 34 que los justificara. Por su interés estos casos se detallan en el apartado de expedientes de autorización de transferencias internacionales.

De los 88 ficheros inscritos en el año 2000 que declaran la transferencia internacional de datos amparándose en el consentimiento dado por el afectado hay 69 que declaran transferencias a países que no tienen un nivel de protección equiparable al que presta la Ley. Conforme a lo establecido en el artículo 3.h) de la Ley consentimiento es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. Por lo tanto, para que la transferencia pueda estar amparada en el artículo 34. e), se exige que en el consentimiento coste la circunstancia de la transferencia internacional, la finalidad y el destino de la misma. Por lo general, este consentimiento se realiza mediante una cláusula escrita, que contiene como mínimo información sobre la finalidad del fichero, derechos de oposición, acceso, rectificación o cancelación, y países destinatarios.

Los fines más usuales de los ficheros que se transfieren son, como en el año anterior, todos aquellos relacionados con la Selección de Recursos Humanos, Servicios económico-financieros y Seguros, Publicidad y Prospección Comercial, Servicios de Telecomunicaciones, y Sanidad.

Las cláusulas de consentimiento varían su contenido dependiendo de la finalidad concreta de cada fichero.

Normalmente, las transferencias realizadas en determinados sectores como el del crédito, seguros, la intermediación financiera y bursátil, encuentran su justificación legal en las excepciones previstas en el artículo 34.e) cuando el afectado haya dado su consentimiento inequívoco, 34.f) cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontratuales adoptadas a petición del afectado y 34.g) cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

A continuación por su especial interés, expondremos algunas de las justificaciones presentadas por las entidades pertenecientes a estos sectores:

- *En el sector de intermediación financiera y bursátil*, los contratos suscritos en el marco del proceso de ampliación de los mercados de valores que vienen desarrollándose en España, son celebrados para llevar a cabo las transferencias de valores con los datos de identificación de sus correspondientes titulares entre los sistemas de registro y custodia de

los sistemas de depósitos centralizados de los países.

Estos contratos deben ser calificados como contratos celebrados "en interés del afectado", como inversor que es en el Mercado y en las Bolsas, y en consecuencia, debe considerarse en el supuesto previsto en el antes mencionado artículo 34.g).

Asimismo, ha de tenerse en cuenta que en la suscripción de los correspondientes contratos entre los inversores y las entidades para sus operaciones en mercados extranjeros, a pesar de constar formalmente como partes de la relación jurídica entablada las referidas entidades, éstas actúan en la práctica como "comisionistas de los clientes".

Y por último, hay que tener en cuenta que el inversor conoce, por resultar inherente a la propia operativa del sistema, que la propia suscripción del correspondiente contrato para la realización de operaciones sobre dichos valores conlleva el consentimiento libre e informado del inversor.

- *En el sector de seguros*, hay que mencionar por su singularidad las circunstancias en las que se produce una transferencia internacional, amparándose, entre otros, en el artículo 34.b): "se realizan a efectos de prestar auxilio judicial internacional".

La intervención de entidades en el auxilio judicial, nacional o internacional, se circunscribe exclusivamente al apoyo que precise el órgano de justicia correspondiente, nacional o extranjero, para conocer algún dato relativo al aseguramiento de un determinado vehículo.

Otro de los supuestos en los que se ampara es el previsto en el artículo 34.c): "es necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios". En este supuesto, los datos se transfieren sólo en la medida en que son determinantes de una situación personal evolutiva o definitiva de lesiones o secuelas de daños físicos.

Por último en previsión del artículo 34.j): "se efectúa, a petición de persona con interés legítimo, desde un registro público y es acorde con la finalidad del mismo". Los datos son suministrados con la exclusiva finalidad de proveer a las víctimas de accidentes de la circulación internacional de vehículos a motor de las indemnizaciones previstas por la respectiva Ley de Seguro Obligatorio del país donde un siniestro haya ocurrido. La transmisión de datos opera entre Oficinas Nacionales y/o sus miembros por razón de la liquidación a las víctimas de sus daños o perjuicios. En la medida en que todas las Oficinas tienen una actividad normada en la legislación de sus respectivos países, deben considerarse como Registros Públicos a los que sólo acceden personas que justifiquen poseer un interés legítimo (víctimas y perjudicados por accidentes de circulación).

Otro caso relevante se refiere a la inscripción de un fichero de titularidad pública que declara la realización de transferencias internacionales de datos. Se trata de un fichero de personas interesadas en la solicitud de adopción de menores en el ámbito de una Comunidad Autónoma, que tiene transferidas competencias en materia de infancia y asuntos sociales.

El Convenio para la Protección del niño y cooperación en materia de adopción internacional, de 29 de mayo de 1993, ratificado por instrumento de 30 de junio de 1995, tiene como objeto instaurar un sistema de cooperación entre los Estados contratantes que asegure el respeto en esta materia y el reconocimiento en los Estados contratantes de las adopciones realizadas de acuerdo con el Convenio. En su artículo 7.1 establece que las Autoridades competentes (en este caso de la Comunidad Autónoma) deberán cooperar entre ellas y promover una colaboración entre las Autoridades competentes de sus respectivos Estados para asegurar la protección de los niños y alcanzar los demás objetivos del Convenio, añadiendo en el artículo 9 que las Autoridades recabarán información, entre otra, relativa a los futuros padres adoptivos en la medida necesaria para la adopción. Por último, en los artículos 15 y 16, que será necesaria la elaboración por el Estado de recepción de un informe referente a los padres adoptivos que deberá conocer el Estado de origen del niño.

La finalidad de este fichero es la de recoger solicitudes de adopción y realizar estudios psicosociales de los solicitantes, y los datos recogidos en el fichero se transfieren a los países de origen de los niños en adopción, por lo que la transferencia se podría realizar a países de nivel de protección no equiparable al español, siempre a través de la Asociación de Ayuda a la Infancia del Mundo (AAIM), única asociación habilitada en esa Comunidad Autónoma, englobada dentro de las Entidades Colaboradoras de Adopción Internacional. Esta transferencia se encuentra justificada en el artículo 34. e) de la Ley, al haber dado los afectados su consentimiento.

Por otra parte, la transferencia internacional a la que nos estamos refiriendo también se encontraría amparada en el Convenio mencionado, si bien éste debe estar ratificado por aquellos países a los que se vaya a realizar la comunicación de los datos.

Expedientes de Autorización de Transferencias Internacionales

Anteriormente se ha expuesto el motivo por el que durante el año 2000 se han tramitado únicamente 2 expedientes de autorización de transferencias internacionales.

La petición de autorización de transferencias internacionales de datos efectuada al amparo del artículo 33 de la Ley exige una serie de garantías que deben ser prestadas por la entidad que realiza la transferencia, establecida legalmente en nuestro país. Dicha entidad, como responsable de los ficheros, deberá garantizar el cumplimiento de todas

las obligaciones y derechos establecidos en la Ley, así como que se continuará facilitando desde España el ejercicio de los derechos de oposición, acceso, rectificación y cancelación de los datos almacenados en terceros países. El Director de la Agencia de conformidad con lo dispuesto en el artículo 33 viene exigiendo garantías que se traducen en cláusulas contractuales apropiadas.

Para poder autorizar la transferencia internacional de datos se deberá aportar un contrato que incorpore los siguientes puntos:

- Determinación de cómo se van a ofrecer a los interesados apoyo y asistencia para garantizar el ejercicio de sus derechos con rapidez y eficacia y en los plazos que determina la Ley, y especial descripción de forma detallada de cómo se facilitarán los derechos de oposición, acceso, rectificación y cancelación desde la sede del responsable en España.

- Compromiso directo del receptor de los datos con la Agencia de Protección de Datos a autorizar el acceso al establecimiento donde se esté tratando la información de un representante de la Agencia para realizar auditorías. Asimismo se garantizará a la Agencia de Protección de Datos la facultad de realizar inspecciones en las instalaciones, según lo dispuesto en el artículo 40 de la Ley 15/1999.

- Atribución al remitente de los datos de la responsabilidad del tratamiento y de los daños causados por los incumplimientos de las garantías legales por cualquiera de las partes contratantes.

- El responsable del fichero hará constar expresamente que asume el poder de decisión sobre el tratamiento. El encargado del tratamiento, es quien presta el servicio del tratamiento automatizado de datos de carácter penal y solo actuará siguiendo instrucciones del responsable del fichero. Se hará constar expresamente que el encargado del tratamiento asume lo dispuesto en el articulo 43 de la Ley 15/1999 "*Los responsables de los ficheros y los encargados de los tratamientos están sujetos al régimen sancionador establecido en la presente Ley".*

- Que la titularidad del fichero corresponde a una entidad domiciliada en territorio español y que dicha entidad, como responsable del fichero, garantiza todos los derechos y obligaciones dispuestos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, así como que se continuará facilitando desde España los derechos de acceso, rectificación y cancelación.

- Se hará constar en las Estipulaciones del Contrato, que si alguna persona externa a la entidad, física o jurídica, entra en conocimiento de los datos además de la autorización expresa de la entidad a la que se autoriza la transferencia internacional, se requerirá una nueva autorización del Director de la Agencia de Protección de Datos.

- También se deberá consignar que el encargado del tratamiento garantizará el reconocimientos de las resoluciones de la Agencia de Protección de Datos en materia de obligaciones de protección de datos.

Los expedientes de autorización de transferencia tramitados y resueltos durante el año 2000 tenían como destino Estados Unidos de América y Marruecos. Con destino a EE.UU. se realiza la transferencia internacional a la empresa matriz del grupo de la que es filial la empresa española, que desarrolla su actividad dentro del sector de fabricación y comercialización de juguetes y productos análogos. La finalidad es la prestación de servicio de tratamiento de datos, concretándose en la gestión informática de ficheros de bases de datos titularidad de la empresa española, junto con la custodia y seguridad de los mismos. Los datos objeto de la transferencia son de carácter identificativo, de características personales, de información comercial, económicos-financieros y de transacciones.

La transferencia con destino a Marruecos se realiza por una sociedad de nacionalidad española que está desarrollando su actividad dentro del sector de telecomunicaciones a una compañía de nacionalidad marroquí, en la que la mayoría de las acciones que componen su capital social están suscritas por una persona jurídica constituida conforme al derecho español y sede social en España. La finalidad de la transferencia es la prestación de servicios de teleoperación, y los datos objeto de la misma son de carácter identificativo. La ubicación del fichero está en España y la empresa destinataria de la transferencia únicamente puede acceder a la información de una persona por cada consulta on-line realizada.

No obstante, la autorización de la transferencia, podría en algunos casos, quedar condicionada a la aportación de documentación fehaciente debidamente autentificada, en el idioma español, de otorgamiento de poder bastante a favor de las personas firmantes por cada una de las sociedades contratantes, con acreditación suficiente de sus firmas.

Por último, habiéndose presentado poderes suficientes de los respectivos intervinientes, debidamente legitimados, quedaría autorizada la transferencia internacional y se daría traslado al Ministro de Justicia, a fin de que se dé cumplimiento al artículo 26 de la Directiva 95/46/CE, en el que se dispone que los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2 de dicho artículo, por lo que las dos autorizaciones han sido comunicadas al Ministerio de Justicia.

6. EL REGISTRO EN CIFRAS

A continuación se detalla la situación y características principales de los ficheros inscritos en el Registro General de Protección de Datos. Como en años anteriores, se ha tratado de establecer la comparación entre los ficheros según la titularidad del responsable, público o privado, así como el estudio de sus principales características.

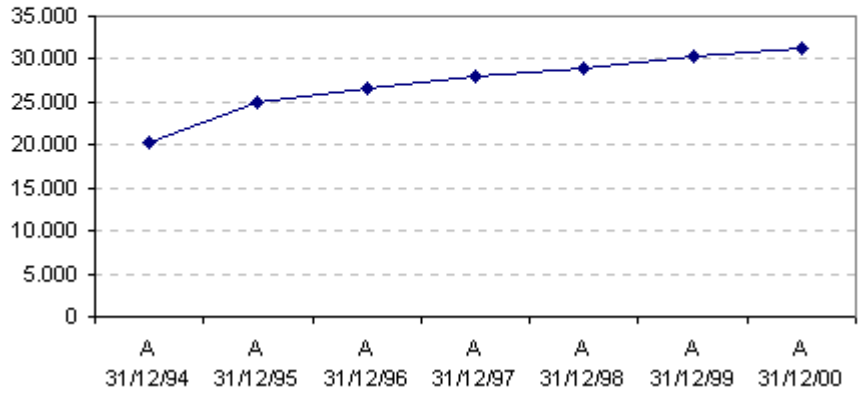
No obstante, con motivo de los cambios introducidos en el formato de los formularios de notificación de ficheros, se encontrarán diferencias con los datos referidos a años anteriores, detallándose las modificaciones en cada uno de los apartados que se relacionan a continuación.

A fecha 31 de Diciembre de 2000, el número de ficheros inscritos en el Registro General de Protección de Datos era de 249.209, de los cuales 31.155 correspondían a inscripciones de titularidad pública y 218.054 a inscripciones de titularidad privada.

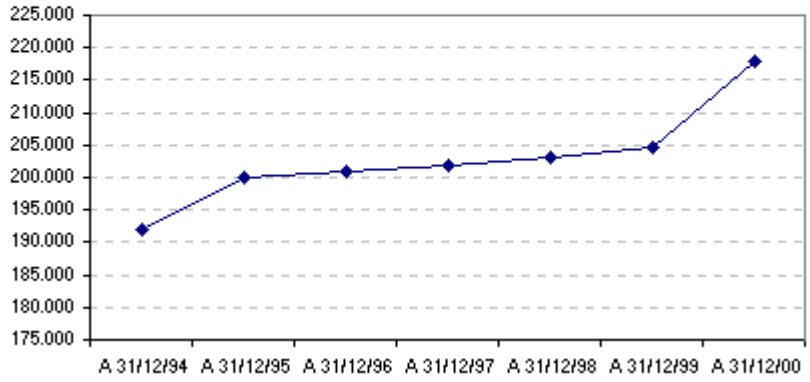
RESUMEN DETALLADO DE LOS FICHEROS INSCRITOS EN EL RGPD, SEGÚN LA TITULARIDAD

Se recoge en esta tabla el número de ficheros inscritos en el Registro General de Protección de Datos a 31 de Diciembre de cada año, de acuerdo con los datos que aparecen en las memorias anuales de la Agencia, según la titularidad de los mismos.

EVOLUCION DE LA INSCRIPCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA
Gráfico Registro General nº 1



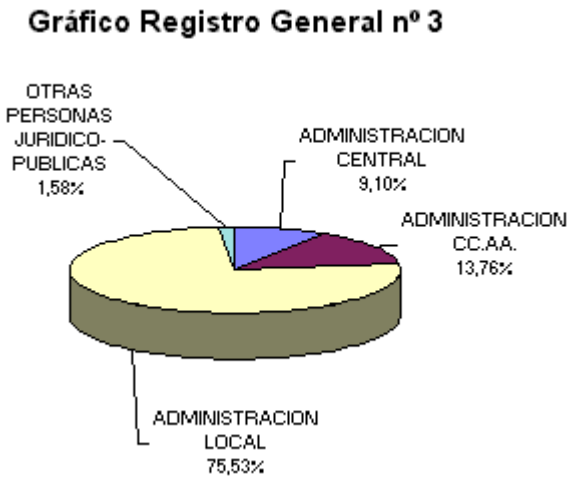
EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS DE TITULARIDAD PRIVADA
Gráfico Registro General nº 2



DISTRIBUCION DE FICHEROS DE TITULARIDAD PUBLICA INSCRITOS EN EL RGPD, SEGÚN EL TIPO DE ADMINISTRACIÓN AL QUE PERTENECEN

En el nuevo formulario de notificación de ficheros se han eliminado los subgrupos de cada uno de los tipos de administración, manteniendo diferenciados únicamente los cuatro tipos de administración principales:

	2000	TOTAL
ADMINISTRACION CENTRAL	101	2.837
ADMINISTRACION CC.AA.	482	4.290
ADMINISTRACION LOCAL	288	23.533
OTRAS PERSONAS JURIDICO-PUBLICAS	8	495
TOTAL	879	31.155



DISTRIBUCION DE FICHEROS DE TITULARIDAD PUBLICA DE LA ADMINISTRACIÓN CENTRAL INSCRITOS EN EL RGPD

Los datos que aparecen a continuación recogen la reestructuración ministerial llevada a cabo en los Reales Decretos 557/2000, 558/2000 y 689/2000, entre otros, de abril y mayo de 2000, en la que se modificaron los nombres de algunos Departamentos Ministeriales, se crearon nuevos y se suprimieron otros.

	2000	TOTAL
MINISTERIO DE ADMINISTRACIONES PUBLICAS	11	191
MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACIO	0	40
MINISTERIO DE ASUNTOS EXTERIORES	0	522
MINISTERIO DE CIENCIA Y TECNOLOGIA	6	47
MINISTERIO DE DEFENSA	0	35
MINISTERIO DE ECONOMIA	0	93
MINISTERIO DE EDUCACION, CULTURA Y DEPORTE	6	133
MINISTERIO DE FOMENTO	16	210
MINISTERIO DE HACIENDA	0	128
MINISTERIO DE JUSTICIA	3	22
MINISTERIO DE LA PRESIDENCIA	0	39
MINISTERIO DE MEDIO AMBIENTE	24	170
MINISTERIO DE SANIDAD Y CONSUMO	4	647
MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES	24	278
MINISTERIO DEL INTERIOR	7	275
MINISTERIO PORTAVOZ DEL GOBIERNO	0	3
PRESIDENCIA DEL GOBIERNO	0	4
TOTAL	101	2.837

DISTRIBUCION DE FICHEROS DE TITULARIDAD PUBLICA DE LA ADMINISTRACIÓN DE LAS CC.AA. INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

COMUNIDAD AUTONOMA	2000	TOTAL
ANDALUCIA	53	494
ARAGON	0	175
CANARIAS	3	261
CANTABRIA	0	21
CASTILLA - LA MANCHA	7	95
CASTILLA Y LEON	0	221
CATALUÑA	14	495
CEUTA	0	23
COMUNIDAD VALENCIANA	131	341
EXTREMADURA	1	63
GALICIA	0	191
ISLAS BALEARES	6	31
LA RIOJA	104	129
MADRID	157	996
MELILLA	0	62
NAVARRA	2	94
PAIS VASCO	1	306
PRINCIPADO DE ASTURIAS	0	143
REGION DE MURCIA	3	149
TOTAL	482	4.290

DISTRIBUCION DE FICHEROS DE TITULARIDAD PUBLICA DE LA ADMINISTRACIÓN LOCAL INSCRITOS EN EL RGPD

En esta tabla aparecen, diferenciados por Provincias y Comunidades Autónomas, los ficheros de la Administración Local.

	ENTIDADES LOCALE		FICHEROS	
	2000	TOTAL	2000	TOTAL
ANDALUCIA	**12**	**679**	**25**	**5.457**
ALMERIA	1	104	1	951
CADIZ	3	48	3	332
CORDOBA	4	61	15	258
GRANADA	0	168	0	1.183
HUELVA	0	85	0	1.150
JAEN	0	82	0	468
MALAGA	1	39	2	381
SEVILLA	3	92	4	734
ARAGON	**0**	**434**	**0**	**1.967**
HUESCA	0	156	0	536
TERUEL	0	45	0	152
ZARAGOZA	0	233	0	1.279
ASTURIAS	**0**	**46**	**0**	**277**
ILLES BALEARS	**1**	**67**	**1**	**650**
CANARIAS	**3**	**68**	**8**	**415**
PALMAS, LAS	3	27	8	195
SANTA CRUZ DE TENERIFE	0	41	0	220
CANTABRIA	**0**	**43**	**0**	**192**
CASTILLA-LA MANCHA	**0**	**342**	**0**	**1.850**
ALBACETE	0	74	0	356
CIUDAD REAL	0	107	0	557
CUENCA	0	82	0	556
GUADALAJARA	0	11	0	59
TOLEDO	0	68	0	322
CASTILLA Y LEON	**1**	**499**	**1**	**2.200**
AVILA	1	7	1	20
BURGOS	0	91	0	318
LEON	0	163	0	801
PALENCIA	0	18	0	76
SALAMANCA	0	80	0	338
SEGOVIA	0	14	0	104
SORIA	0	9	0	31
VALLADOLID	0	82	0	355
ZAMORA	0	35	0	157
CATALUÑA	**19**	**548**	**38**	**2.545**
BARCELONA	18	303	33	1.377
GIRONA	0	55	0	347
LLEIDA	0	106	0	398
TARRAGONA	1	84	5	423
COMUNIDAD VALENCIANA	**5**	**312**	**59**	**2.238**
ALICANTE	2	136	50	1.243
CASTELLON DE LA PLANA	0	35	0	225
VALENCIA	3	141	9	770
EXTREMADURA	**2**	**189**	**2**	**1.561**
BADAJOZ	1	156	1	1.391
CACERES	1	33	1	170

DISTRIBUCION DE FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD

En esta tabla aparecen, diferenciados por Comunidades Autónomas y Provincias, los ficheros inscritos por responsables de titularidad privada.

	EMPRESAS		FICHEROS	
	2.000	TOTAL	2.000	TOTAL
ANDALUCIA	**380**	**9.375**	**1.316**	**18.187**
ALMERIA	9	421	34	832
CADIZ	105	1.741	203	2.759
CORDOBA	55	1.131	229	2.496
GRANADA	31	760	132	1.525
HUELVA	20	636	43	1.030
JAEN	15	838	52	1.775
MALAGA	89	2.081	291	3.727
SEVILLA	57	1.775	332	4.043
ARAGON	**205**	**8.124**	**455**	**13.365**
HUESCA	18	1.810	47	2.521
TERUEL	23	591	38	933
ZARAGOZA	164	5.728	370	9.911
ASTURIAS	**67**	**1.990**	**135**	**3.706**
ILLES BALEARS	**79**	**1.279**	**325**	**3.123**
CANARIAS	**107**	**1.324**	**239**	**2.480**
PALMAS, LAS	70	769	147	1.433
SANTA CRUZ DE TENERIFE	37	559	92	1.047
CANTABRIA	**28**	**587**	**74**	**1.281**
CASTILLA-LA MANCHA	**73**	**3.017**	**243**	**5.317**
ALBACETE	14	921	80	1.452
CIUDAD REAL	18	627	59	1.149
CUENCA	6	527	8	846
GUADALAJARA	10	226	36	535
TOLEDO	25	716	60	1.335
CASTILLA Y LEON	**143**	**4.630**	**293**	**8.470**
AVILA	11	204	41	390
BURGOS	18	1.278	31	2.045
LEON	24	663	44	1.249
PALENCIA	7	239	9	465
SALAMANCA	24	547	50	1.233
SEGOVIA	9	291	21	512
SORIA	3	242	9	387
VALLADOLID	39	927	78	1.630
ZAMORA	8	245	10	559
	EMPRESAS		FICHEROS	
	2.000	TOTAL	2.000	TOTAL
CATALUÑA	**3.187**	**32.927**	**6.451**	**61.871**
BARCELONA	2.390	24.917	5.001	47.845
GIRONA	306	3.061	507	5.397
LLEIDA	92	2.890	332	4.909
TARRAGONA	401	2.084	611	3.720

FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD POR RESPONSABLES CON SEDE EN LA UNION EUROPEA

La Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en su artículo 2.1 fija su ámbito de aplicación a cualquier tratamiento de datos de carácter personal efectuado en el territorio español, se encuentre el establecimiento del responsable en España, en territorio de la Unión Europea o fuera de ésta.

No obstante, con anterioridad a la entrada en vigor de la nueva Ley ya existían dos responsables de ficheros inscritos en Francia e Italia.

	EMPRESAS		FICHEROS	
	2.000	TOTAL	2.000	TOTAL
RESPONSABLES EN LA UNION EUROPE	**3**	**5**	**6**	**8**
FRANCIA	2	3	5	6
ITALIA	0	1	0	1
REINO UNIDO	1	1	1	1

DISTRIBUCIÓN DE FICHEROS SEGÚN LA TIPOLOGÍA DE DATOS QUE CONTIENEN

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	2000	TOTAL	2000	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	3	63	168	507
OTROS DATOS ESPECIALMENTE PROTEGIDOS	96	2.116	769	4.240
DATOS RELATIVOS A INFRACCIONES	31	1.256	---	---
DATOS DE CARACTER IDENTIFICATIVO	879	31.155	16.233	218.054
DATOS DE CARACTERISTICAS PERSONALES	381	16.057	7.811	89.379
DATOS DE CIRCUNSTANCIAS SOCIALES	125	8.044	2.244	23.146
DATOS ACADEMICOS Y PROFESIONALES	252	10.156	3.307	29.303
DETALLES DE EMPLEO Y CARRERA ADMINISTRATIVA	219	6.985	6.326	70.550
DATOS DE INFORMACION COMERCIAL	87	6.439	2.486	40.652
DATOS ECONOMICO-FINANCIEROS	220	13.847	8.598	112.178
DATOS DE TRANSACCIONES	46	5.753	3.698	55.321

---- No aplicable a esta titularidad

DISTRIBUCIÓN DE FICHEROS INSCRITOS CON DATOS SENSIBLES

La Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en su artículo 7 cita como datos especialmente protegidos los de Ideología, Creencias, Religión y Afiliación Sindical, añadiendo estos últimos a los que ya citaba la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.

Con anterioridad a la publicación de la Resolución de 30 de mayo de 2000, por la que se aprueban los nuevos modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos (BOE de 27 de junio), ya existían ficheros que declaraban la posesión de datos de afiliación sindical, si bien ante la imposibilidad de grabar esta tipología por no disponer de ella en los formularios, se estaban grabando como datos de Ideología, dejando constancia de estas circunstancia en las observaciones asociadas al fichero.

Esta información ha sido utilizada para convertir los datos de los ficheros declarados con anterioridad al nuevo formato de formulario, por lo que en la tabla que aparece a continuación ya figuran 2 ficheros de titularidad pública y 39 de titularidad privada inscritos antes del año 2000 con datos de Afiliación Sindical.

	TITULARIDAD PUBLIC/		TITULARIDAD PRIVAD/	
	2000	TOTAL	2000	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	**3**	**63**	**168**	**507**
Ideología	0	36	26	142
Creencias	0	18	3	41
Religión	0	12	31	202
Afiliación Sindical	3	5	110	149
OTROS DATOS ESPECIALMENTE PROTEGIDO	**96**	**2.116**	**769**	**4.240**
Origen Racial	5	85	8	61
Salud	96	1.901	767	4.215
Vida Sexual	14	362	33	130
DATOS RELATIVOS A INFRACCIONES	**31**	**1.256**	---	---
Infracciones Penales	10	736	---	---
Infracciones Administrativas	30	868	---	---

--- No aplicable a esta titularidad

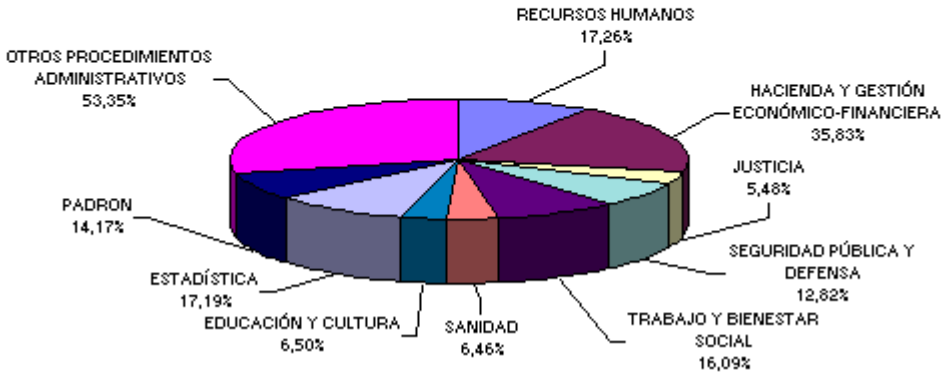
DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA INSCRITOS EN EL RGPD, SEGÚN SU FINALIDAD

Como ya se ha expuesto anteriormente, en el apartado de Finalidad del Fichero y Usos Previstos del nuevo modelo se ha realizado una agrupación de finalidades en categorías, cambiando la denominación de alguna de las tipificaciones existentes y añadiendo tipologías nuevas.

En las relaciones que se indican a continuación, aparece la distribución de ficheros inscritos por cada una de las finalidades tipificadas en el nuevo modelo. Puede llamar la atención que para alguna de ellas exista un número muy bajo de ficheros inscritos, ello se debe a que estas finalidades sólo han podido ser declaradas desde la entrada en vigor del nuevo modelo de notificación. Estas finalidades aparecen sombreadas en la tabla que se muestra a continuación.

	2000	TOTAL
RECURSOS HUMANOS		
GESTIÓN DE PERSONAL	120	4.502
GESTIÓN DE NÓMINA	4	4
FORMACIÓN DE PERSONAL	39	1.428
ACCIÓN SOCIAL A FAVOR DEL PERSONAL DE LAS ADMONES. PÚBLICAS	16	803
PROMOCIÓN Y SELECCIÓN DE PERSONAL, OPOSICIONES Y CONCURSOS	4	4
PREVENCIÓN DE RIESGOS LABORALES	0	0
CONTROL HORARIO	2	2
CONTROL DE INCOMPATIBILIDADES	16	624
CONTROL DE PATRIMONIO DE ALTOS CARGOS PÚBLICOS	1	220
HACIENDA Y GESTIÓN ECONÓMICO-FINANCIERA		
GESTIÓN TRIBUTARIA Y DE RECAUDACIÓN	68	6.716
GESTIÓN ECONÓMICA Y CONTABLE	61	5.989
GESTIÓN DE FACTURACIÓN	1	1
GESTIÓN FISCAL	2	3
GESTIÓN DEUDA PÚBLICA Y TESORERÍA	7	2.459
GESTIÓN DE CATASTROS INMOBILIARIOS RÚSTICOS Y URBANOS	13	1.848
RELACIONES COMERCIALES CON EL EXTERIOR	13	422
REGULACIÓN DE MERCADOS FINANCIEROS	0	29
DEFENSA DE LA COMPETENCIA	0	25
JUSTICIA		
PROCEDIMIENTOS JUDICIALES	13	880
REGISTROS VINCULADOS CON LA FE PÚBLICA	0	17
PRESTACIÓN SOCIAL SUSTITUTORIA	6	843
TRAMITACIÓN DE INDULTOS	0	262
SEGURIDAD PÚBLICA Y DEFENSA		
PROTECCIÓN CIVIL	11	1.654
SEGURIDAD VIAL	8	1326
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD CON FINES POLICIALES	6	2.063
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD CON FINES ADMINISTRATIVO	3	1.817
GESTIÓN Y CONTROL DE CENTROS E INSTITUCIONES PENITENCIARIAS	1	326
TRAMITACION SERVICIO MILITAR	6	2131
SOLICITUDES DE VISADO/RESIDENCIA	0	0
TRABAJO Y BIENESTAR SOCIAL		
PROMOCIÓN Y GESTIÓN DE EMPLEO	39	837
RELACIONES LABORALES Y CONDICIONES DE TRABAJO	14	1372
INSPECCIÓN Y CONTROL DE SEGURIDAD Y PROTECCIÓN SOCIAL	3	692
FORMACIÓN PROFESIONAL OCUPACIONAL	16	1.096
PRESTACIONES A DESEMPLEADOS	13	971
PRESTACIONES DE GARANTÍA SALARIAL	7	268
PRESTACIONES DE ASISTENCIA SOCIAL	30	1.608
PENSIONES, SUBSIDIOS Y OTRAS PRESTACIONES ECONÓMICAS	33	1.939
ACCIÓN A FAVOR DE INMIGRANTES	10	418
SERVICIOS SOCIALES A MINUSVÁLIDOS	22	799
SERVICIOS SOCIALES A LA TERCERA EDAD	17	1082
PROMOCIÓN SOCIAL A LA MUJER	18	629
PROMOCIÓN SOCIAL A LA JUVENTUD	13	678
PROTECCIÓN DEL MENOR	16	663
ACCIÓN A FAVOR DE TOXICÓMANOS	1	1
AYUDAS ACCESO A VIVIENDA	8	1.051
OTROS SERVICIOS SOCIALES	35	1.177
SANIDAD		

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA INSCRITOS EN EL RGPD, SEGÚN SU FINALIDAD
Gráfico Registro General nº 4

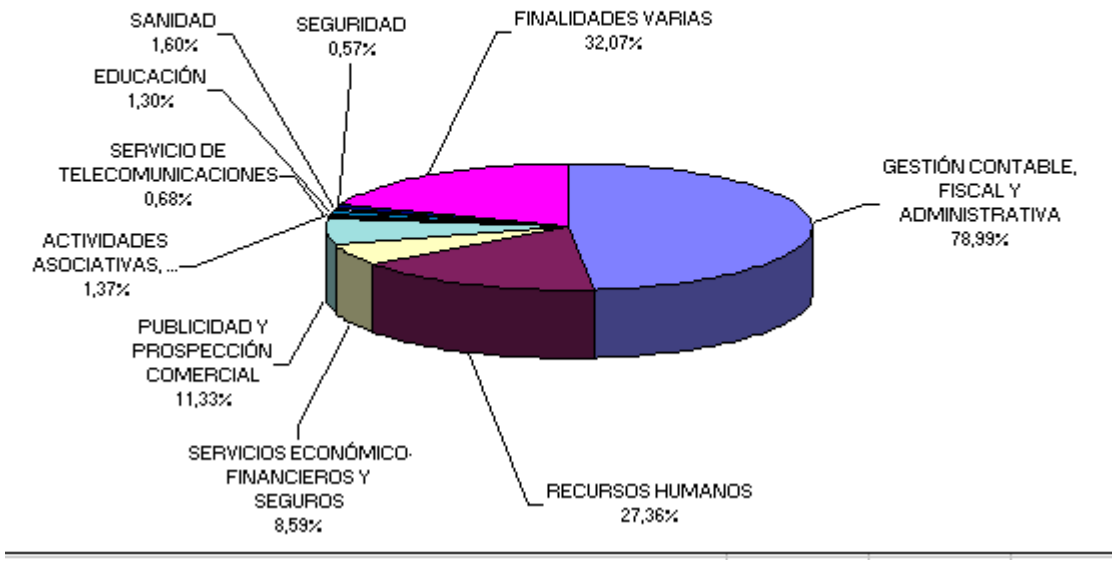


DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS, SEGÚN SU FINALIDAD

Igual que en el cuadro anterior, los cambios introducidos en este apartado del formulario implican la aparición de nuevas finalidades, que aparecen sombreadas en la tabla que se muestra a continuación

	2000	TOTAL
GESTIÓN CONTABLE, FISCAL Y ADMINISTRATIVA		
GESTIÓN ECONÓMICA Y CONTABLE	8.175	140.734
GESTIÓN FISCAL	7.598	140.151
GESTIÓN ADMINISTRATIVA	7.814	140.372
GESTIÓN DE FACTURACIÓN	1.174	1.213
GESTIÓN DE CLIENTES	5.377	69.023
GESTIÓN DE PROVEEDORES	864	891
GESTIÓN DE COBROS Y PAGOS	6.622	93.991
ADMINISTRACIÓN DE FINCAS	22	22
CONSULTORÍAS, AUDITORÍAS, ASESORÍAS Y SERVICIOS RELACIONADOS	853	14.054
HISTÓRICOS DE RELACIONES COMERCIALES	2.959	34.673
RECURSOS HUMANOS		
GESTIÓN DE PERSONAL	4.236	57.211
GESTIÓN DE NÓMINAS	820	853
FORMACIÓN DE PERSONAL	465	2.003
PRESTACIONES SOCIALES	632	14.206
SELECCIÓN DE PERSONAL	1005	4.676
GESTIÓN DE TRABAJO TEMPORAL	36	50
PROMOCIÓN Y GESTIÓN DE EMPLEO	92	112
PREVENCIÓN RIESGOS LABORALES	114	120
CONTROL HORARIO	150	158
SERVICIOS ECONÓMICO-FINANCIEROS Y SEGUROS		
CUENTA DE CRÉDITO	419	4.459
CUENTA DE DEPÓSITO	311	2.473
GESTIÓN DE PATRIMONIOS	283	2.264
GESTIÓN DE FONDOS DE PENSIONES Y SIMILARES	268	2.252
GESTIÓN DE TARJETAS DE CRÉDITO Y SIMILARES	254	1.641
REGISTRO DE ACCIONES Y OBLIGACIONES	328	2.258
OTROS SERVICIOS FINANCIEROS	515	4.104
CUMPLIMIENTO/INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS	44	55
PRESTACIÓN DE SERVICIOS DE SOLVENCIA PATRIMONIAL Y CRÉDITO	373	3.480
SEGUROS DE VIDA Y SALUD	796	6.041
OTRO TIPO DE SEGUROS	585	5.929
PUBLICIDAD Y PROSPECCIÓN COMERCIAL		
PUBLICIDAD PROPIA	2339	21.755
VENTA A DISTANCIA	350	3.004
ENCUESTAS DE OPINIÓN	644	3.607
ANÁLISIS DE PERFILES	91	98
PROSPECCIÓN COMERCIAL	1093	7.978
SEGMENTACIÓN DE MERCADOS	114	122
SISTEMAS DE AYUDA A LA TOMA DE DECISIONES	89	96
RECOPILACIÓN DE DIRECCIONES	112	118
SERVICIO DE TELECOMUNICACIONES		
PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES	267	1.430
GUÍAS/REPERTORIOS DE SERVICIOS DE TELECOMUNICACIONES	21	21
COMERCIO ELECTRÓNICO	85	89
PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN	3	4
ACTIVIDADES ASOCIATIVAS, CULTURALES, RECREATIVAS, DEPORTIVAS Y SOCIALES		
GESTIÓN DE ACTIVIDADES CULTURALES	31	33
GESTIÓN DE CLUBES O ASOCIACIONES DEPORTIVAS, CULTURALES, PROFESINALES Y SIMILARES	329	2.404
GESTIÓN DE ASOCIADOS O MIEMBROS DE PARTIDOS POLÍTICOS, SINDICATOS, IGLESIAS, CONFESIONES O COMUNIDADES RELIGIOSAS Y ASOCIACIONES, FUNDACIONES Y OTRAS	49	50

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD, SEGUN SU FINALIDAD
Gráfico Registro General nº 5



DISTRIBUCION DE FICHEROS INSCRITOS EN EL RGPD, SEGÚN LA PROCEDENCIA DE LOS DATOS Y EL PROCEDIMIENTO DE RECOGIDA

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, en su artículo 3.j) enumera explícitamente las procedencias de los datos que pueden ser consideradas Fuentes Accesibles al Público, por lo que una de las modificaciones introducidas en el formato del formulario ha sido la enumeración de éstas.

En el nuevo modelo se ha considerado a los Registros Públicos como una Procedencia de Datos, y no como un Procedimiento de Recogida, como se venía considerando en los modelos en vigor con la LORTAD.

Estas dos modificaciones han hecho necesaria la conversión de los datos ya existentes, lo cual hace que:

Para aquellos ficheros que hubieran declarado con anterioridad la procedencia de los datos de fuentes accesibles al público no constan diferenciados los tipos indicados en la nueva Ley, apareciendo estos tipos diferenciados en la tabla únicamente para los ficheros inscritos con posterioridad a Julio del 2000, o aquellos anteriores que han sufrido modificaciones después de esta fecha.

Todos aquellos ficheros que indicaban como procedimiento de recogida la de Registros Públicos, ahora constan en el apartado de procedencia de los datos.

	ENTIDADES LOCALES		FICHEROS	
	2000	TOTAL	2000	TOTAL
ANDALUCIA	**12**	**679**	**25**	**5.457**
ALMERIA	1	104	1	951
CADIZ	3	48	3	332
CORDOBA	4	61	15	258
GRANADA	0	168	0	1.183
HUELVA	0	85	0	1.150
JAEN	0	82	0	468
MALAGA	1	39	2	381
SEVILLA	3	92	4	734
ARAGON	**0**	**434**	**0**	**1.967**
HUESCA	0	156	0	536
TERUEL	0	45	0	152
ZARAGOZA	0	233	0	1.279
ASTURIAS	**0**	**46**	**0**	**277**
ILLES BALEARS	**1**	**67**	**1**	**650**
CANARIAS	**3**	**68**	**8**	**415**
PALMAS, LAS	3	27	8	195
SANTA CRUZ DE TENERIFE	0	41	0	220
CANTABRIA	**0**	**43**	**0**	**192**
CASTILLA-LA MANCHA	**0**	**342**	**0**	**1.850**
ALBACETE	0	74	0	356
CIUDAD REAL	0	107	0	557
CUENCA	0	82	0	556
GUADALAJARA	0	11	0	59
TOLEDO	0	68	0	322
CASTILLA Y LEON	**1**	**499**	**1**	**2.200**
AVILA	1	7	1	20
BURGOS	0	91	0	318
LEON	0	163	0	801
PALENCIA	0	18	0	76
SALAMANCA	0	80	0	338
SEGOVIA	0	14	0	104
SORIA	0	9	0	31
VALLADOLID	0	82	0	355
ZAMORA	0	35	0	157
CATALUÑA	**19**	**548**	**38**	**2.545**
BARCELONA	18	303	33	1.377
GIRONA	0	55	0	347
LLEIDA	0	106	0	398
TARRAGONA	1	84	5	423

DISTRIBUCION DE FICHEROS INSCRITOS EN EL RGPD QUE DECLARAN LA REALIZACIÓN DE CESIONES DE DATOS

	FICHEROS INSCRITOS AÑO 200			FICHEROS TOTALES		
	CON CESIONES	TOTAL	%	CON CESIONES	TOTAL	%
TITULARIDAD PÚBLICA	306	879	34,81	17.743	31.155	56,95
TITULARIDAD PRIVADA	3.300	16.233	20,33	37.961	218.054	17,41
TOTAL	3.606	17.112	21,07	55.704	249.209	22,35
	CON CESIONES	TOTAL				
TITULARIDAD PUBLICA	56,95	44,05				
TITULARIDAD PRIVADA	17,41	82,59				

	EMPRESAS		FICHEROS	
	2.000	TOTAL	2.000	TOTAL
ANDALUCIA	380	9.375	1.316	18.187
ALMERIA	9	421	34	832
CADIZ	105	1.741	203	2.759
CORDOBA	55	1.131	229	2.496
GRANADA	31	760	132	1.525
HUELVA	20	636	43	1.030
JAEN	15	838	52	1.775
MALAGA	89	2.081	291	3.727
SEVILLA	57	1.775	332	4.043
ARAGON	205	8.124	455	13.365
HUESCA	18	1.810	47	2.521
TERUEL	23	591	38	933
ZARAGOZA	164	5.728	370	9.911
ASTURIAS	67	1.990	135	3.706
ILLES BALEARS	79	1.279	325	3.123
CANARIAS	107	1.324	239	2.480
PALMAS, LAS	70	769	147	1.433
SANTA CRUZ DE TENERIFE	37	559	92	1.047
CANTABRIA	28	587	74	1.281
CASTILLA-LA MANCHA	73	3.017	243	5.317
ALBACETE	14	921	80	1.452
CIUDAD REAL	18	627	59	1.149
CUENCA	6	527	8	846
GUADALAJARA	10	226	36	535
TOLEDO	25	716	60	1.335
CASTILLA Y LEON	143	4.630	293	8.470
AVILA	11	204	41	390
BURGOS	18	1.278	31	2.045
LEON	24	663	44	1.249
PALENCIA	7	239	9	465
SALAMANCA	24	547	50	1.233
SEGOVIA	9	291	21	512
SORIA	3	242	9	387
VALLADOLID	39	927	78	1.630
ZAMORA	8	245	10	559
	EMPRESAS		FICHEROS	
	2.000	TOTAL	2.000	TOTAL
CATALUÑA	3.187	32.927	6.451	61.871
BARCELONA	2.390	24.917	5.001	47.845
GIRONA	306	3.061	507	5.397
LLEIDA	92	2.890	332	4.909
TARRAGONA	401	2.084	611	3.720
COMUNIDAD VALENCIANA	262	14.489	779	24.237
ALICANTE	64	5.705	189	9.194
CASTELLON DE LA PLANA	51	2.340	176	4.127
VALENCIA	147	6.452	414	10.916
EXTREMADURA	147	2.259	180	3.687
BADAJOZ	121	1.786	154	2.710

	EMPRESAS		FICHEROS	
	2.000	TOTAL	2.000	TOTAL
RESPONSABLES EN LA UNION EUROPEA	3	5	6	8
FRANCIA	2	3	5	6
ITALIA	0	1	0	1
REINO UNIDO	1	1	1	1

SUPUESTOS LEGALES EN LOS QUE SE AMPARAN LAS CESIONES DE DATOS INSCRITAS EN EL RGPD

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	2000	TOTAL	2000	TOTAL
EXISTE CONSENTIMIENTO DE LOS AFECTADOS	177	6.838	2.433	20.081
EXISTE UNA RELACION JURIDICA CUYO DESARROLLO, CONTROL Y CUMPLIMIENTO IMPLICA NECESARIAMENTE LA CONEXION DEL FICHERO CON FICHEROS DE TERCEROS	53	3.890	1.595	14.144
EXISTE UNA NORMA REGULADORA QUE LAS AUTORIZA	259	10.880	1.467	20.852
SE TRATA DE DATOS RECOGIDOS DE FUENTES ACCESIBLES AL PUBLICO	26	4.765	212	2.529
CORRESPONDEN A COMPETENCIAS IDENTICAS O QUE VERSAN SOBRE LAS MISMAS MATERIAS, EJERCIDAS POR OTRAS ADMINISTRACIONES PUBLICAS	139	10.481	---	---
SON DATOS OBTENIDOS O ELABORADOS CON DESTINO A OTRA ADMINISTRACION PUBLICA	124	9.270	---	---
LA COMUNICACIÓN TIENE POR OBJETO EL TRATAMIENTO POSTERIOR DE LOS DATOS CON FINES HISTORICOS, ESTADISTICOS O CIENTIFICOS	19	21	---	---
TOTAL FICHEROS INSCRITOS CON CESIONES	**306**	**17.743**	**3.300**	**37.961**

El total de ficheros inscritos con cesiones reflejados en el apartado anterior, no corresponde a la suma de los datos que figuran en cada subapartado, ya que un mismo fichero puede estar amparado en varios supuestos.

DISTRIBUCION DE FICHEROS INSCRITOS EN EL RGPD QUE DECLARAN LA REALIZACIÓN DE TRANSFERENCIAS INTERNACIONALES DE DATOS

	FICHEROS INSCRITOS AÑO 2000			FICHEROS TOTALES		
	CON TRANSFERENCIA	TOTAL	%	CON TRANSFERENCIA	TOTAL	%
TITULARIDAD PÚBLICA	3	879	0,34	51	31.155	0,16
TITULARIDAD PRIVADA	269	16.233	1,66	1.301	218.054	0,60
TOTAL	272	17.112	1,59	1.352	249.209	0,54

SUPUESTOS LEGALES EN LOS QUE SE AMPARAN LAS TRANSFERENCIAS INTERNACIONALES DE DATOS INSCRITAS EN EL RGPD

La Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en su artículo 34, amplía el número de supuestos legales por los que se pueden realizar transferencias internacionales de datos sin necesitar la Autorización del Director de la Agencia.

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	2000	TOTAL	2000	TOTAL
SE EFECTÚ;A CON DESTINO A PAÍSES QUE PROPORCIONAN UN NIVEL DE PROTECCIÓN EQUIPARABLE	2	47	221	1147
RESULTA DE LA APLICACIÓN DE TRATADOS O CONVENIOS EN LOS QUE SEA PARTE ESPAÑA	0	37	7	8
SE REALIZA A EFECTOS DE PRESTAR AUXILIO JUDICIAL INTERNACIONAL	0	9	1	1
ES NECESARIA PARA LA PREVENCIÓN O PARA EL DIAGNÓSTICO MÉDICOS, LA PRESTACIÓN DE ASISTENCIA SANITARIA O TRATAMIENTO MÉDICOS O LA GESTIÓN DE SERVICIOS SANITARIOS	1	6	1	24
SE REFIERE A TRANSFERENCIAS DINERARIAS, CONFORME A SU LEGISLACIÓN ESPECÍFICA	0	15	11	65
EL AFECTADO HA DADO SU CONSENTIMIENTO	1	1	88	96
ES NECESARIA PARA LA EJECUCIÓN DE UN CONTRATO ENTRE EL AFECTADO Y EL RESPONSABLE DEL FICHERO O PARA LA ADOPCIÓN DE MEDIDAS PRECONTRACTUALES ADOPTADAS A PETICIÓN DEL AFECTADO	0	0	33	35
ES NECESARIA PARA LA CELEBRACIÓN O EJECUCIÓN DE UN CONTRATO CELEBRADO O POR CELEBRAR, EN INTERÉS DEL AFECTADO, POR EL RESPONSABLE DEL FICHERO Y UN TERCERO	0	0	9	11
ES NECESARIA O LEGALMENTE EXIGIDA PARA LA SALVAGUARDA DE UN INTERÉS PÚBLICO	0	0	1	1
ES PRECISA PARA EL RECONOCIMIENTO, EJERCICIO O DEFENSA DE UN DERECHO EN UN PROCESO JUDICIAL	0	0	0	0
SE EFECTÚA , A PETICIÓN DE PERSONA CON INTERÉS LEGÍTIMO, DESDE UN REGISTRO PÚBLICO Y ES ACORDE CON LA FINALIDAD DEL MISMO	0	0	1	1
AUTORIZADA POR EL DIRECTOR DE LA AGENCIA	0	0	2	182
TOTAL FICHEROS CON TRANSFERENCIAS INTERNACIONAL	**3**	**51**	**269**	**1.301**

El total de ficheros inscritos con transferencias internacionales reflejados en el apartado anterior, no corresponde a la suma de los datos que figuran en cada subapartado, ya que un mismo fichero puede estar amparado en varios supuestos.

DISTRIBUCION DE DOCUMENTOS DE ENTRADA/SALIDA RELACIONADOS CON EL RGPD DURANTE EL AÑO 2000

RESUMEN DE OPERACIONES DE INSCRIPCIÓN REALIZADAS EN EL RGPD DURANTE EL AÑO 2000

III. SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS

1. INTRODUCCIÓN: ACTIVIDAD DE LA INSPECCIÓN DE DATOS.

La Subdirección General de Inspección de Datos es el órgano de la Agencia de Protección de Datos (APD) al que, bajo la dirección y superior autoridad del Director, le corresponde desempeñar dos de las más importantes funciones para el efectivo cumplimiento de la LOPD: la función inspectora o investigadora y la función instructora de los expedientes

sancionadores y procedimientos de tutela de derechos.

1.1. FUNCIÓN INSPECTORA

La Inspección de Datos no está contemplada por la LOPD desde la vertiente orgánica, sino sólo desde la funcional, siendo el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la APD, el que prevé que las funciones inherentes al ejercicio de la potestad de inspección que el art. 40 de la LOPD atribuye a la Agencia, se ejerzan por un órgano específico y separado de los demás al frente del cual se sitúa a un funcionario con categoría de Subdirector General.

No añade el Estatuto nuevas precisiones sobre el estatuto personal de quienes se encuadran en este órgano a las ya contenidas en la LOPD, la cual dispone que los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus cometidos (art. 40), de donde resulta que la inspección deberá ser desempeñada por funcionarios de carrera. El carácter de "autoridad pública" que el art. 40.2 LOPD atribuye a los Inspectores de Datos significa que las personas responsables de los ficheros y/o tratamientos que ofrezcan resistencia o cometan atentado contra dichos funcionarios/inspectores, podrían incurrir en su caso en responsabilidad penal, exigible conforme a la legislación penal, y en todo caso incurrirían en la responsabilidad administrativa prevista en el art. 44.3.j) de la LOPD, calificada como obstrucción al ejercicio de la función inspectora.

El Estatuto desarrolla el contenido de la potestad de inspección atribuida a la Agencia en el ya citado art. 40 de la LOPD, precisando la facultad de la Inspección de Datos para efectuar inspecciones de oficio, aunque pudieran tener su origen en una denuncia de las personas afectadas, y detallando el alcance concreto de su capacidad para requerir y obtener información, así como examinar *in situ* los ficheros y sistemas informáticos en los que se traten datos de carácter personal. En conjunto, se trata de una serie de facultades cuya finalidad es la de obtener información y, en su caso, pruebas sobre posibles incumplimientos de la LOPD, que permitan posteriormente al órgano decisorio incoar procedimientos sancionadores y adoptar, en su caso, las medidas pertinentes dirigidas a la cesación de actividades ilícitas en los términos previstos en los arts. 37.f) y 49 de dicha Ley.

Como lógico correlato de esta función inspectora, se impone a los funcionarios que la ejercen el deber de guardar secreto sobre las informaciones que conozcan en el ejercicio de tal función, incluso después de haber cesado en la misma (art. 40.2 in fine); deber cuyo incumplimiento generaría la oportuna responsabilidad disciplinaria mientras se conserve la relación de servicio con la APD, y que se reputaría infracción administrativa grave, una vez extinguida dicha relación, al amparo del art. 44.3 g) de la LOPD.

1.2. FUNCIÓN INSTRUCTORA

A la Subdirección General de Inspección de Datos le corresponde también la función instructora en los expedientes sancionadores, esto es, el ejercicio de los actos de instrucción relativos a los expedientes sancionadores (art. 29 del Estatuto).

El ejercicio de esta función instructora no es más que la consecuencia obligada de la existencia de la potestad sancionadora atribuida en exclusiva al Director de la Agencia (art. 37.g de la LOPD) y la necesaria garantía del procedimiento sancionador, cuyo ejercicio exige la separación entre la fase instructora y la sancionadora, encomendándolas o órganos distintos (art. 134 Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común).

El procedimiento sancionador, de conformidad con lo previsto en el art. 48.1 de la LOPD, está regulado en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, que detalla el cauce a seguir para la determinación de las infracciones y la imposición de sanciones, estructurándose como cualquier otro procedimiento sancionador en las tres clásicas fases de Iniciación, Instrucción y Resolución, correspondiendo al funcionario instructor el desarrollo completo de la fase de Instrucción u Ordenación del procedimiento y al Director de la Agencia las otras dos, es decir, el acuerdo de inicio del procedimiento sancionador y la Resolución del mismo.

Por otra parte, la función instructora se concreta en la incoación de tres clases de procedimientos: el **procedimiento sancionador** incoado contra los responsables de ficheros de titularidad privada por infracción de los principios y reglas contenidos en la LOPD; el **procedimiento por infracciones de las Administraciones Públicas** (art. 46) cuando es una Administración de esta clase la que vulnera los preceptos de la Ley; y el **procedimiento de tutela de derechos** previsto en el art. 18 de la Ley, que se actúa cuando son vulnerados los derechos de oposición, acceso, rectificación o cancelación de los afectados (arts. 15 a 17).

El procedimiento de **tutela de derechos** supone la existencia de un posible incumplimiento de la Ley que no se dirige inicialmente a la declaración de una infracción sino a garantizar el ejercicio de los derechos de oposición, acceso, rectificación y cancelación, lo que justifica referirse a esta potestad arbitral de tutela al margen de la potestad sancionadora de la APD. La nueva LOPD ha venido a reproducir el mismo esquema que regía bajo la vigencia de la derogada LORTAD, si bien ha introducido dos novedades en el procedimiento de tutela de derechos al ampliar el plazo máximo para dictar resolución a seis meses (art. 18.3), siguiendo la pauta general que para los procedimientos administrativos establece el art. 42.2 la Ley 30/1992, de 26 de noviembre, y dar entrada en la regulación de estos procedimientos a un nuevo derecho que se desconocía en la anterior legislación: el derecho de oposición, que consiste en esencia en que

en aquellos casos en los que no es necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal (art. 6.4).

1.3. EXPEDIENTES RELACIONADOS CON LA FUNCIÓN INSPECTORA

En el ejercicio de la función inspectora realizada por la APD durante el año 2000 se iniciaron **319** actuaciones de investigación o inspección, en su mayor parte promovidas por denuncias presentadas por los ciudadanos ante la APD, con el objeto de comprobar posibles vulneraciones de la LOPD.

De estas **319** actuaciones de inspección iniciadas durante 2000, **153** han finalizado en dicho ejercicio, estando el resto: **166** , pendientes de concluir. A las **153** actuaciones de inspección iniciadas y finalizadas en 2000 hay que añadir aquellas otras, en concreto **97**, que iniciadas el año anterior finalizaron en el presente año, lo que hace un total de **250** actuaciones de inspección terminadas en 2000.

Así mismo, y al margen de lo anterior, se han realizado durante el mismo año **28** actuaciones de información previa con el fin de determinar con carácter preliminar si concurrían circunstancias que justificaran la iniciación de una actuación de inspección y, en su caso, posterior incoación del correspondiente procedimiento. Tales actuaciones previas no dieron lugar a nuevas actuaciones debido, en su mayor parte, a que de los hechos denunciados no se deducían indicios de infracción de la LOPD, aunque podrían suponer infracciones de otro tipo, ajenas a la competencia de la APD.

El fundamento de todas estas actuaciones se encuentra en el art. 69.2 de la Ley 30/1992, de 26 de noviembre, desarrollado por el art. 12 del Real Decreto 1298/1993, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el ejercicio de la Potestad Sancionadora, que permiten realizar actuaciones previas con anterioridad a la iniciación de un concreto procedimiento. Añade el citado precepto reglamentario que las actuaciones previas serán realizadas por los órganos que tengan atribuidas funciones de investigación, averiguación e inspección en la materia; en nuestro caso, los Inspectores de Datos conforme a lo previsto en el art 40.2 LOPD.

1.4. EXPEDIENTES RELACIONADOS CON LA FUNCIÓN INSTRUCTORA

De las tres clases de procedimientos incoados en 2000 por lo órganos instructores de la Inspección de Datos, **146** corresponden a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad privada; **31** a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad pública (procedimientos por infracciones de las Administraciones Públicas); y **193** se corresponden a los iniciados por procedimientos de tutela de derechos.

De los **146** procedimientos sancionadores iniciados durante el año 2000, han finalizado en dicho ejercicio **83** , estando el resto: **63** , pendientes de concluir. A los **83** procedimientos sancionadores iniciados y finalizados en el 2000 hay que añadir aquellos otros, en concreto **54** , que iniciados el año anterior finalizaron en el presente, lo que suma un total de **137** procedimientos sancionadores terminados en 2000.

De los **31** procedimientos por infracciones de las Administraciones Públicas iniciados en el 2000, gran parte de ellos, en concreto **22** , han finalizado en dicho año, estando los **9** restantes pendientes de conclusión. Así mismo, se han terminado durante el presente ejercicio **5** procedimientos de esta clase provenientes del anterior, lo que supone la conclusión de **27** procedimientos por infracciones de las Administraciones Públicas en 2000.

A los anteriores procedimientos deben añadirse **181** Resoluciones de Archivo, que debidamente motivadas se dictan tras la correspondiente investigación previa de los hechos denunciados, después de comprobar que no constituyen infracción de la legislación en materia de protección de datos o bien que no entran en el ámbito de aplicación de la misma.

Así mismo, se han dictado **7** Resoluciones a raíz de diversas peticiones de colaboración realizadas por el Presidente de la Comisión Nationale de L'Informatique et des Libertes (CNIL), autoridad competente en materia de protección de datos en Francia, al amparo del art. 114.2 del Convenio Schengen, en relación con peticiones de acceso y cancelación de los ficheros del Sistema de Información Schengen.

Finalmente, de los **193** procedimientos de tutela de derechos iniciados en 2000, **137** han finalizado en el mismo ejercicio, quedando **56** pendientes de concluir. A los **137** antes citados hay que añadir los procedimientos de esta clase iniciados el año anterior, en concreto **20** , y terminados en el presente, lo que hace un total de **157** procedimientos de tutela de derechos concluidos en el 2000.

A todos los procedimientos anteriores deben añadirse la resolución de **113** recursos de reposición resueltos durante el mismo año 2000. La Ley 4/1999, de 13 de enero, de Modificación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, vino a reestablecer el recurso de reposición contra los actos que ponen fin a la vía administrativa, con carácter potestativo (art. 116 Ley 30/1992), lo que ha supuesto si no duplicar, sí aumentar notablemente la carga de trabajo, no sólo de la actividad de instrucción sino también de la Secretaría General de la Agencia en cuanto que es este órgano el que califica la pertinencia de las

garantías presentadas por el recurrente con objeto de obtener la suspensión de la ejecución del acto impugnado.

Por ello, dada la novedad introducida por la citada Ley 4/1999 y toda vez que los actos resolutorios del Director de la Agencia en los procedimientos sancionadores ponen fin a la vía administrativa (art. 48.2 LOPD), de la misma manera que igualmente agotan la vía administrativa en los procedimientos de tutela de derechos (art. 18.4 LOPD), se ha producido un aumento muy considerable de recursos de reposición presentados contra las Resoluciones del Director de la APD.

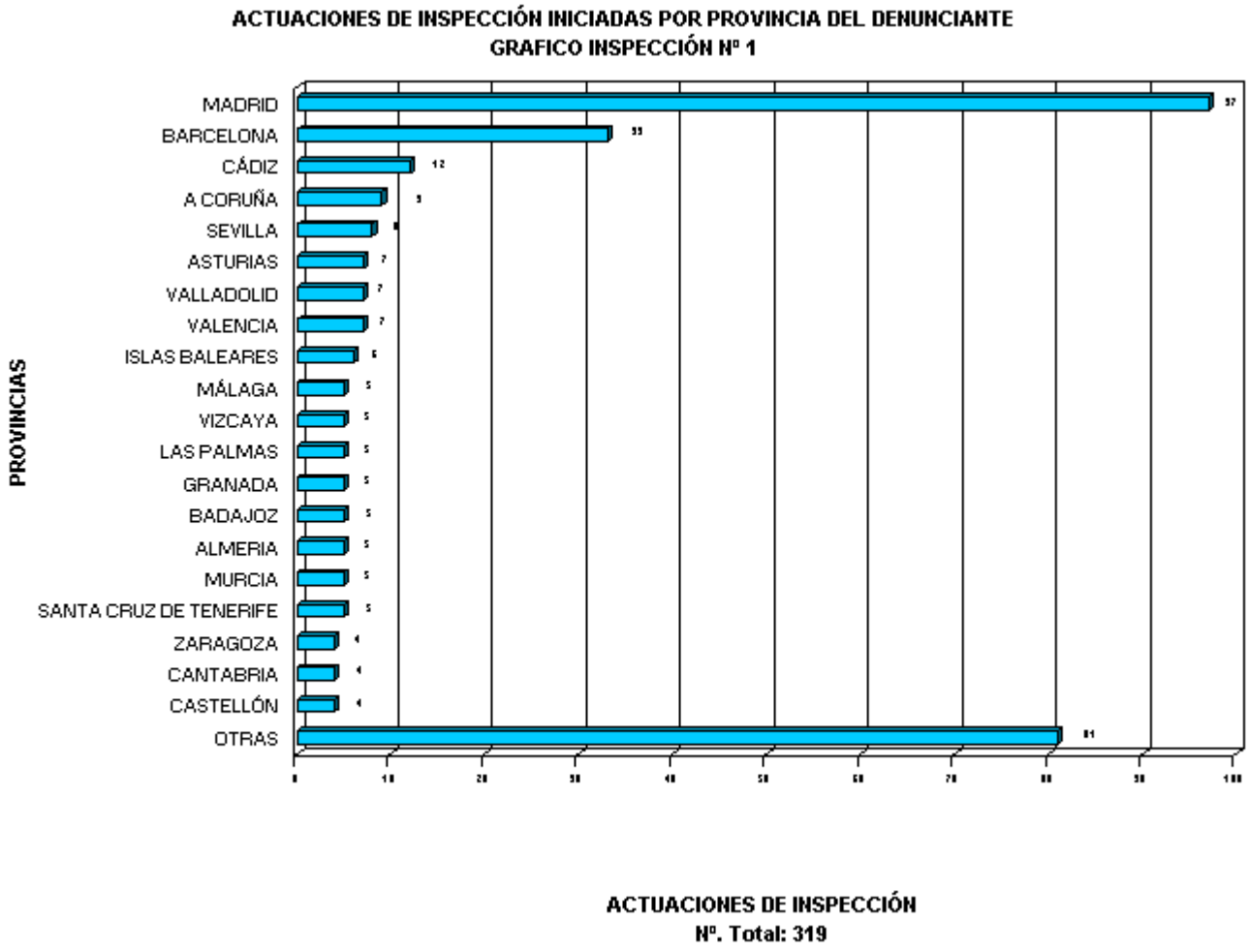
De los **113** recursos de esta clase presentados, **2** han sido estimados al reconocerse por la Agencia error en la calificación de la infracción o apreciación indebida de los hechos, **1** estimado parcialmente, **7** inadmitidos por extemporáneos o falta de legitimación y **103** desestimados por falta de fundamento de las pretensiones formuladas. No obstante, aun en estos últimos, su formulación ha facilitado la petición de suspensión de la ejecución de la Resolución sancionadora, lo que ha sido concedido por la Agencia en todos los casos en que se han considerado cumplidos los requisitos exigidos por la Ley 30/1992, de 26 de noviembre.

Como conclusión ha de señalarse que durante el ejercicio 2000 se han emitido un total de **622** Resoluciones, que comprende la suma de los procedimientos sancionadores, resoluciones de archivo, actuaciones de colaboración con la CNIL, procedimientos de tutela de derechos y recursos de reposición.

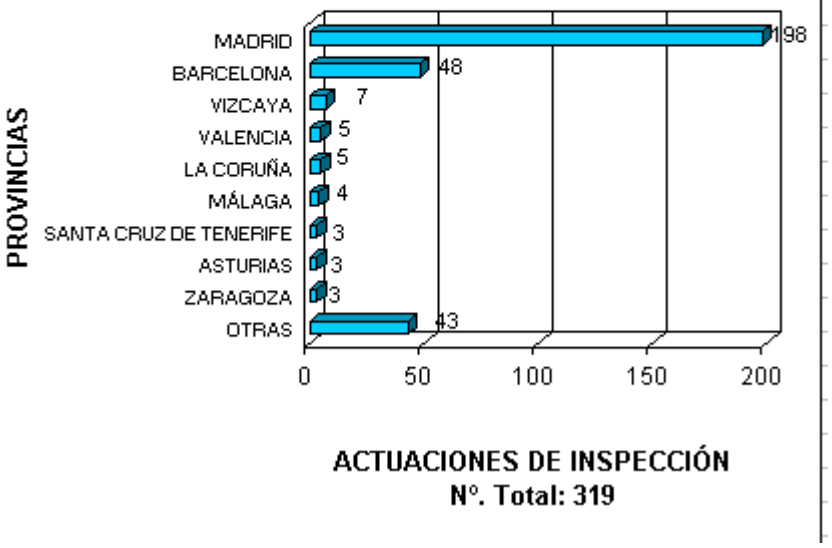
1.5. ESTADÍSTICAS MEDIANTE GRÁFICOS DE LOS EXPEDIENTES REFERIDOS.

1.5.1. Gráficos correspondientes a la función inspectora.

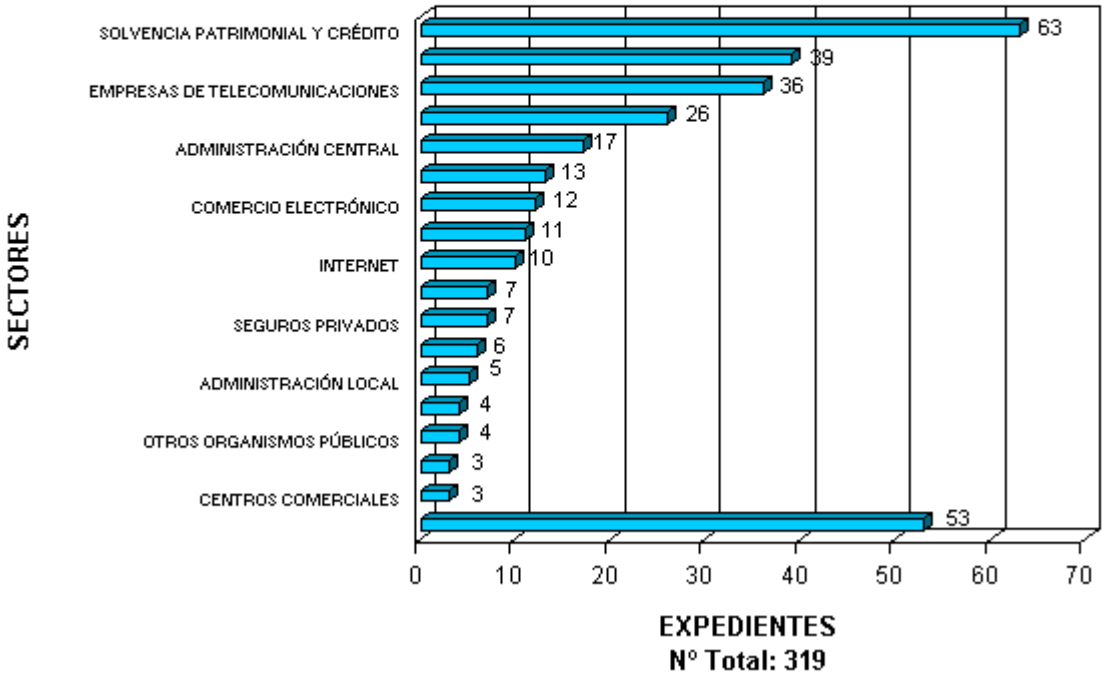
A continuación, se puede observar en los gráficos I, II, y III la distribución geográfica de las actuaciones de investigación o inspección correspondientes al año 2000, referida anteriormente en el apartado 1.3, y separadas por provincia del denunciante, provincia del denunciado y sectores de actividad inspeccionados.



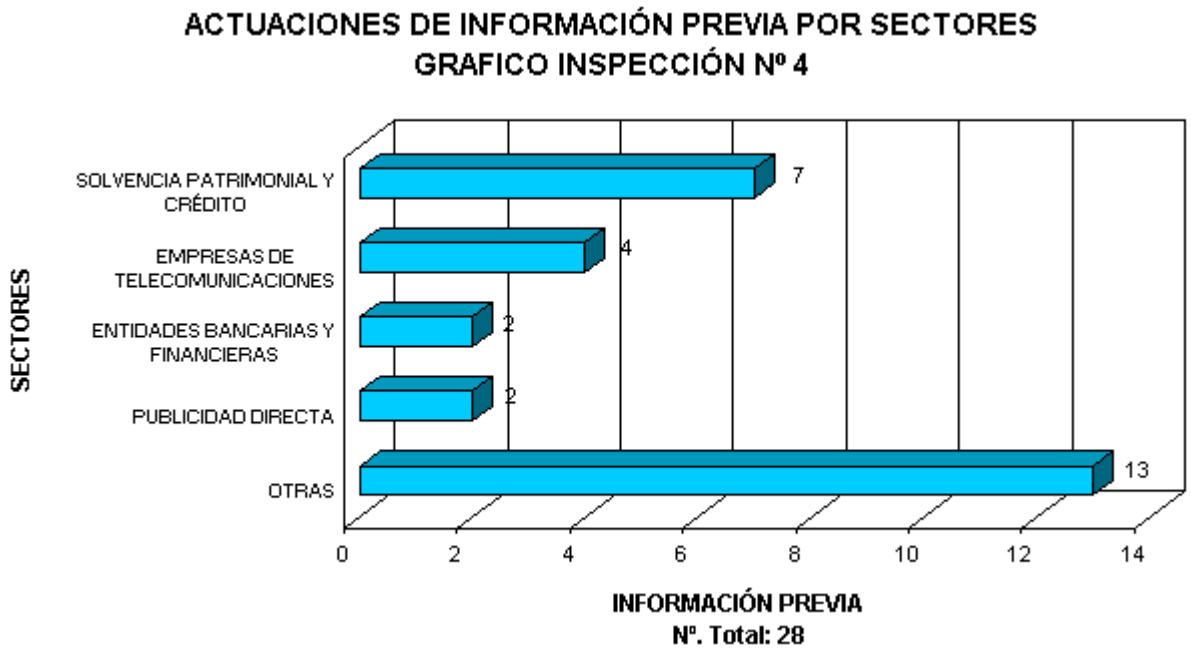
ACTUACIONES DE INSPECCIÓN INICIADAS POR PROVINCIA DEL DENUNCIADO
GRAFICO INSPECCIÓN Nº 2



ACTUACIONES DE INSPECCIÓN INICIADAS POR SECTORES DE ACTIVIDAD
GRAFICO INSPECCIÓN Nº 3



A continuación, en el gráfico IV, se puede apreciar detalladamente la distribución por sectores de actividad de las actuaciones de información previa realizadas en 2000 a las que alude el anterior apartado 1.3.

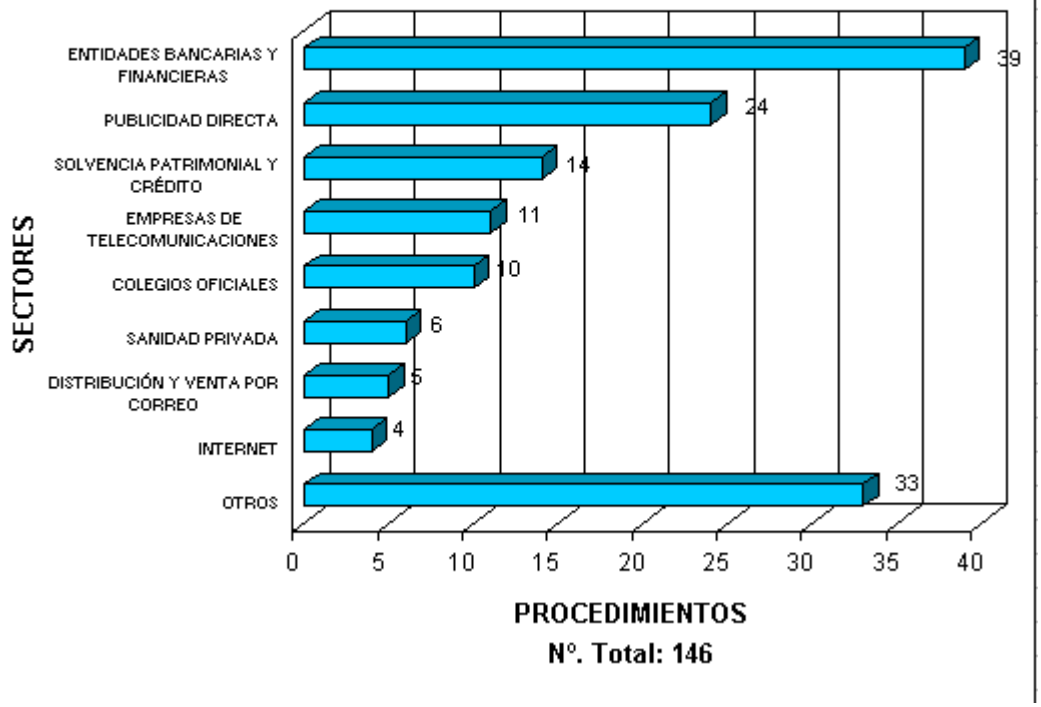


1.5.2. Gráficos correspondientes a la función instructora

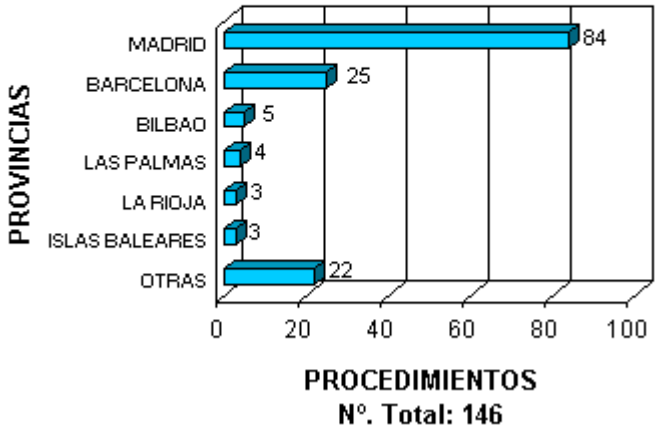
Seguidamente, en los gráficos V y V bis, VI y VI bis y VII, se puede apreciar de forma detallada la evolución del número de expedientes tramitados durante 2000 y que afectan a la función instructora a la que alude el anterior apartado 1.4., esto es, procedimientos sancionadores incoados frente a responsables de ficheros de titularidad privada, procedimien - tos sancionadores por infracciones de las Administraciones Públicas y procedimientos de tutela de derechos.

Así mismo, y dentro de la función instructora se destaca en el gráfico VIII la evolución que presenta la novedad de los recursos de reposición.

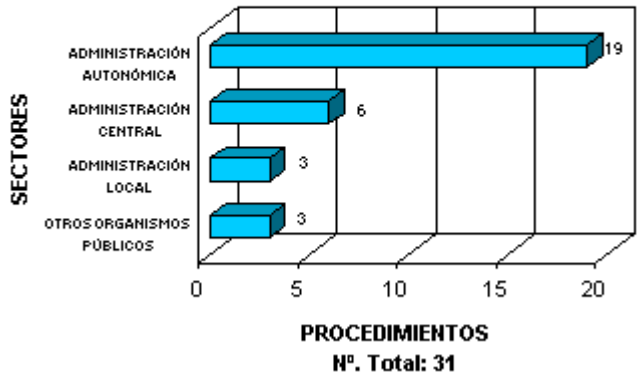
PROCEDIMIENTOS SANCIONADORES INICIADOS POR SECTORES
GRAFICO INSPECCIÓN Nº 5



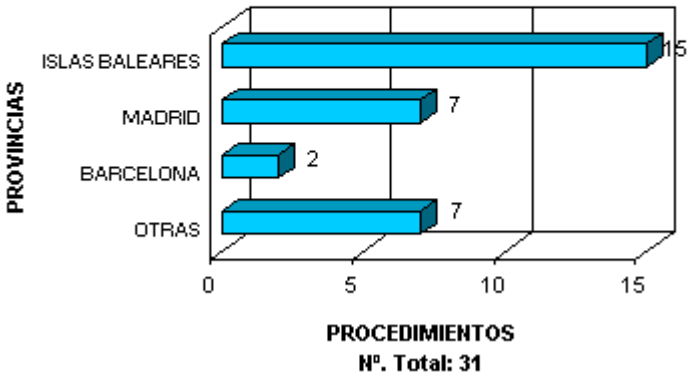
PROCEDIMIENTOS SANCIONADORES INICIADOS POR PROVINCIAS
GRAFICO INSPECCIÓN Nº 5 BIS



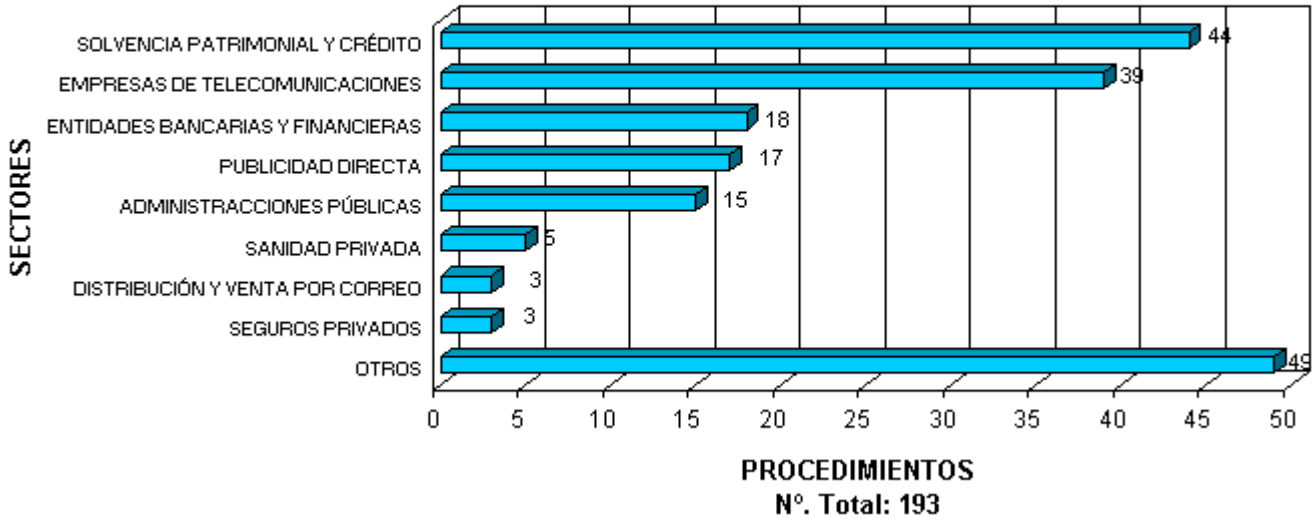
PROCEDIMIENTOS DE LAS AAPP
INICIADOS POR SECTORES
GRAFICO INSPECCIÓN Nº 6



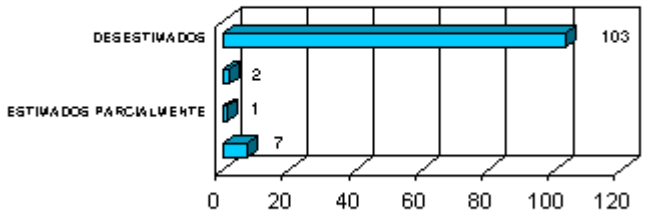
PROCEDIMIENTOS DE LAS AAPP
INICIADOS POR PROVINCIAS
GRAFICO INSPECCIÓN Nº 6 BIS

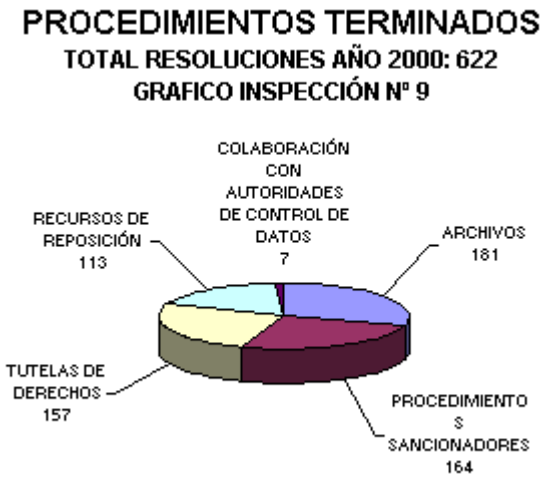


PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR SECTORES
GRAFICO INSPECCIÓN Nº 7



RECURSO DE REPOSICIÓN
GRAFICO INSPECCIÓN Nº 8





2. PLANES SECTORIALES DE OFICIO

Para cumplir con una de las principales funciones que la LOPD atribuye a la APD: "*Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación*" (art. 37.a), la Agencia cuenta con un instrumento esencial: los Planes Sectoriales de Oficio. Con estos planes, que puntualmente se realizan cada año a diferentes sectores de la actividad del país, tanto de ámbito público como privado, se pretende pulsar o comprobar el grado de cumplimiento y adecuación de las empresas y entidades más significativas de cada sector, esto es, aquellas que manejan mayor número de ficheros con gran número de datos personales, a las prescripciones de la legislación sobre protección de datos.

Lo que se pretende con este tipo de inspecciones sectoriales no es primordialmente ejercer la potestad sancionadora, sino tratar de conocer el estado y situación que de los tratamientos de datos personales hacen dichos sectores a fin de disciplinarlos en el conocimiento y aplicación de la LOPD. De aquí que, esencialmente y salvo casos extremos y flagrantes de violación del derecho fundamental a la protección de datos que hagan imperiosa la necesidad de restaurar los derechos de los afectados, tales inspecciones suelan concluir con las pertinentes recomendaciones del Director de la APD, dictadas al amparo y en virtud de las potestades que le otorga el art. 5 c) y d) del Real Decreto 426/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, con el fin de que sean conocidas y cumplidas no sólo por las entidades inspeccionadas, sino también por todas las empresas del sector, adecuando los tratamientos que realizan a los principios y prescripciones de la LOPD.

Por ello, y como ya se avanzaba en la Memoria del año 1999, a finales de dicho ejercicio se terminaron las Inspecciones Sectoriales de Oficio realizadas a la Agencia Estatal de Administración Tributaria, Dirección General de Tráfico, al Sector Sanitario (en concreto al Hospital Psiquiátrico de Font Calent, Hospital Militar Gómez Ulla y Centro Nacional de Epidemiología) y al Sector de Investigación Privada. Todas estas inspecciones cuyas CONCLUSIONES ya figuran en la Memoria del ejercicio 1999 dieron lugar a que se dictaran en el primer trimestre del año 2000 las pertinentes

RECOMENDACIONES que se transcriben a continuación en la presente Memoria.

2.1. RECOMENDACIONES DE LOS PLANES SECTORIALES DE OFICIO REALIZADOS DURANTE EL AÑO 1999.

2.1.1. Agencia Estatal de la Administración Tributaria

Entre las actividades desarrolladas por la Agencia de Protección de Datos durante el año 1999 se encuentra el Plan de Inspección de Oficio sobre los ficheros automatizados de la Agencia Estatal de Administración Tributaria (A.E.A.T.), a fin de comprobar el grado de protección que por la misma se otorga en el tratamiento de los datos de carácter personal.

Con este objeto, se inició en el mes de junio y finalizó en diciembre de 1999 una Inspección de Oficio a la A.E.A.T. por ser sus ficheros unos de los más importantes dentro de los de titularidad pública, tanto por su naturaleza y características como por los colectivos a los que afecta, con el fin de determinar su grado de adecuación a la Ley Orgánica 5/1992, de Tratamiento Automatizado de Datos de Carácter Personal, hoy Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Los procedimientos y ficheros seleccionados para su investigación fueron los relacionados con la gestión del Impuesto sobre la Renta de las Personas Físicas (I.R.P.F.) por ser los más numerosos y que mayormente pueden incidir en el tratamiento automatizado de datos que afectan a las personas físicas. Los objetivos fijados en las actuaciones del citado Plan de Inspección así como las conclusiones del mismo se detallaron en

la memoria de 1999.

Del resultado de las actuaciones practicadas por la Inspección de Datos, se observó un grado de funcionamiento de los ficheros de la A.E.A.T. relacionados con la gestión del I.R.P.F. adecuado al cumplimiento de las prescripciones de la Ley Orgánica 5/1992 (en la actualidad Ley Orgánica 15/1999), si bien se encontraron ligeras deficiencias en la operativa de tales ficheros que una vez subsanadas supondrían una mejora indudable en el acatamiento de la citada Ley. En virtud de las potestades que le otorga el art. 5 c) y d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, el Director de la APD ha dictado en marzo de 2000 las siguientes Recomendaciones que deberán ser observadas por la A.E.A.T., al objeto de adecuar plenamente los tratamientos automatizados que realiza a los principios de la Ley Orgánica 15/1999:

RECOMENDACIÓN PRIMERA: DEL DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS.

La A.E.A.T. recaba información para la gestión del I.R.P.F. que es suministrada por los propios interesados a través de los correspondientes impresos o modelos de declaración, así como de entidades públicas y privadas por medio de los pertinentes "modelos".

Sin cuestionar, obviamente, el derecho de la Agencia Tributaria a recabar tales datos al amparo de lo previsto en la normativa tributaria, en particular, el art. 111.1 de la Ley General Tributaria, se observa, sin embargo, la existencia de ciertas deficiencias respecto del deber de información previsto en el art. 5 de la Ley 15/1999 (L.O.P.D.).

En este sentido, la Agencia Tributaria deberá tener en cuenta que, tanto si procede a la recogida de datos personales directamente del interesado como si lo hace a través de impresos o cuestionarios - y aún cuando se den las circunstancias previstas en el art. 5.3 L.O.P.D. -, el responsable de la recogida deberá informar en todo caso de las señaladas en los apartados a) y e) del citado artículo, a cuyo efecto los modelos de impresos o cuestionarios que se aprueben por la A.E.A.T. deberán incluir las correspondientes cláusulas informativas.

Entiende esta Agencia de Protección de Datos que el contenido de los mencionados apartados a) y e) del art. 5.1 de la L.O.P.D. constituyen elementos básicos para ejercer los derechos de acceso, rectificación y cancelación, por lo que son de obligada información por el responsable del fichero, toda vez que cualquier desconocimiento de estos aspectos esenciales de la posición jurídica del afectado constituye una clara infracción de un derecho fundamental.

Por excepción, la Agencia Tributaria podrá omitir el referido derecho de información a los afectados en la recogida de sus datos personales exclusivamente "*cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de la Administración Tributaria...* ", de conformidad con lo previsto en el art. 24. 1 L.O.P.D. Ahora bien, teniendo en cuenta la indefinición legal transcrita, que interpretada en sentido laxo podría suponer en la práctica la desaparición de los derechos de los afectados tratándose de ficheros de titularidad pública, entiende esta Agencia que, dada la naturaleza del derecho a proteger, su interpretación debe ser en todo caso restrictiva y estar, por tanto, suficientemente motivada la omisión del referido derecho de información por parte de la Agencia Tributaria en cada caso concreto.

(1)

RECOMENDACIÓN SEGUNDA : DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN.

De conformidad con lo dispuesto en los arts. 15 y 16 de la L.O.P.D., la Agencia Tributaria deberá facilitar a los interesados el ejercicio de los derechos de acceso, rectificación y cancelación en los términos previstos en dichos artículos.

Por excepción, los responsables de los ficheros de la Hacienda Pública podrán denegar el ejercicio de tales derechos cuando se dan las circunstancias previstas en el apartado 2 del art. 23 de la L.O.P.D. Ahora bien, al igual que en la recomendación anterior y considerando lo indefinido de la expresión "obligaciones tributarias" referida en el citado artículo 23.2, que prácticamente comprende todas las que afectan a la A.E.A.T. (gestión, inspección, liquidación, recaudación, sanción...), la denegación de los aludidos derechos deberá estar lo suficientemente motivada por la Agencia Tributaria en cada caso concreto como para no dejar al ciudadano que pretende ejercitar su derecho en clara situación de indefensión, debiendo asegurarse la Agencia Tributaria de la procedencia o improcedencia de la denegación, conforme exige el art. 23.3 de la L.O.P.D.

(1)

Debe señalarse que esta recomendación se dictó cuando aún no había recaído la STC 292/2000, de 30 de noviembre, que declara inconstitucional y nulo el mencionado inciso del art. 24.1, no obstante lo cual la APD ya había realizado con anterioridad una interpretación restrictiva de la habilitación legal prevista en dicho inciso por entender que de interpretarse con laxitud, en un sentido literal, quedaba desamparado un derecho fundamental de los afectados.

RECOMENDACIÓN TERCERA : DEL CONSENTIMIENTO DEL AFECTADO EN EL TRATAMIENTO DE SUS DATOS PERSONALES.

Por aplicación de lo dispuesto en el art. 6.2 de la L.O.P.D. no será preciso el consentimiento del afectado cuando sus datos personales se recojan para el ejercicio de la función propia de la Agencia Tributaria en el ámbito de sus competencias.

No obstante, la Agencia Tributaria trata datos especialmente protegidos de los regulados en el art. 7 de la L.O.P.D. Así, los relativos a la Asignación Tributaria, Deducciones por Incapacidad y Enfermedad, y cuotas satisfechas a Sindicatos, que pueden revelar datos especialmente protegidos sobre Religión, Salud y Afiliación Sindical. En estos casos, la regla general es la prohibición de su tratamiento, salvo excepciones tasadas por la ley o consentimiento del afectado dado con las garantías y formalidades prescritas en el art. 7.2 y 3 de la L.O.P.D.

Puesto que los datos especialmente protegidos tratados por la Agencia Tributaria cuando son recogidos directamente del afectado cuentan siempre con su consentimiento previo, se hallan dentro de la previsión legal. No obstante, para facilitar el cumplimiento de las funciones encomendadas al retenedor evitando el incumplimiento de la L.O. 15/1999, el modelo de comunicación aprobado al efecto debería incluir un apartado que permita la prestación del consentimiento expreso de los afectados para el tratamiento de los datos de salud, como son los relativos a la declaración de minusvalías de terceros y otros datos especialmente protegidos por el artículo 7 de la L.O.P.D. antes citado, en los supuestos de pensiones compensatorias y anualidades por alimentos.

RECOMENDACIÓN CUARTA : DE LA CESIÓN DE DATOS.

La A.E.A.T. cede datos a diversos organismos cuya cesión está prevista en el art. 6 de la Orden de 27 de julio de 1994, por la que se regulan los ficheros automatizados de la Agencia Tributaria.

Además, de las comprobaciones efectuadas por la Inspección de Datos, se observa que las cesiones que efectúa la Agencia Tributaria a las entidades y órganos citados en el informe de Inspección son conformes a lo previsto en el art. 113.1 de la Ley General Tributaria, en su redacción dada por la Disposición Adicional Décimo quinta de la Ley 40/1998, de 9 de diciembre, del I.R.P.F. Tan sólo el acceso "*on line* " de algunos Juzgados a las bases de datos de la Agencia Tributaria no queda suficientemente justificado, por lo que, en este caso, la cesión deberá ajustarse a lo previsto en el apartado h) del precitado art. 113.1 de la L.G.T.

RECOMENDACIÓN QUINTA : DE LA INSCRIPCIÓN DE LOS FICHEROS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS.

De conformidad con lo previsto en el art. 39 de la Ley Orgánica 15/1999, de 13 de diciembre y art. 5 del Real Decreto 1332/1994, de 20 de junio, deberá procederse a la inscripción en el Registro General de Protección de Datos de esta Agencia de los ficheros denominados ARRENDAMIENTOS y SUBVENCIONES de los que es responsable la Agencia Tributaria.

RECOMENDACIÓN SEXTA : DE LOS MOVIMIENTOS INTERNACIONALES DE DATOS.

En orden a los movimientos internacionales de datos deberá tenerse en cuenta que no podrán realizarse tales transferencias a países que no proporcionen un nivel de protección equiparable al que presta la vigente Ley Orgánica 15/1999, requiriéndose en otro caso la autorización previa del Director de la Agencia de Protección de Datos, a excepción de los supuestos previstos en el art. 34 de la citada Ley Orgánica.

RECOMENDACIÓN SÉPTIMA : DE LA CANCELACIÓN DE DATOS.

La A.E.A.T. mantiene datos tributarios de las personas desde la creación del Sistema de Información en el año 1979 y de ellas más de un millón han fallecido.

La Ley 15/1999, de Protección de Datos de Carácter Personal en su Art. 4 "Calidad de Datos", punto 5. establece: *"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permitan la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados"*.

En este sentido, la A.E.A.T. deberá proceder a la cancelación de todos aquellos datos de carácter personal que hayan dejado de ser necesarios al fin para el que fueron recabados, sin perjuicio de lo dispuesto en el art. 4.5 *in fine* y 16.5 de la L.O.P.D.

RECOMENDACIÓN OCTAVA : DE LAS MEDIDAS DE SEGURIDAD.

Habiéndose publicado con posterioridad al inicio de las actuaciones inspectoras el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, resulta conveniente recordar las exigencias del mismo y particularmente:

* Que los Sistemas de Información que no se encontraran en funcionamiento a la entrada en vigor de la norma citada, deberán cumplir las medidas de seguridad correspondientes desde que se produzca su puesta en funcionamiento.
* Que dado los datos de carácter personal a tratar por esa Agencia, sus ficheros deberán adaptarse a las medidas calificadas como de nivel medio por el citado Reglamento de Seguridad cuando contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública o cualesquiera otros datos de los mencionados en el art. 4.2 del citado Reglamento, y a las calificadas como de nivel alto cuando contengan datos de ideologías, creencias, origen racial, salud o vida sexual o cualesquiera otros datos de los expresados en el art. 4.3 del mismo Reglamento.
* El plazo de implantación de las citadas medidas, conforme a lo dispuesto en la disposición transitoria única al mencionado Reglamento de Seguridad, será de un año para las medidas de nivel medio y dos años para las de nivel

alto, en ambos casos desde su entrada en vigor el 26 de junio de 1999. No obstante lo anterior, las medidas de seguridad de nivel básico, deben cumplirse, en todo caso, a partir del 26 de marzo de 2000, de conformidad con lo dispuesto en el Real Decreto 195/2000, de 11 de febrero.

2.1.2. Dirección General de Tráfico

Como consecuencia de la inspección de oficio que se realizó en la Dirección General de Tráfico durante el año 1999, el Director de la Agencia dictó las

RECOMENDACIONES que se recogen a continuación, con el fin de permitir a ese organismo una mejor adecuación de sus tratamientos automatizados a los principios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

PRIMERA: DEL DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS Y PRESTACIÓN DEL CONSENTIMIENTO DEL AFECTADO PARA SU TRATAMIENTO.

* Con carácter general, los cuestionarios o impresos que utilice la Dirección General de Tráfico para la recogida de datos de carácter personal en el ejercicio de las funciones que legalmente tiene atribuidas deberán informar al interesado, en forma claramente legible, de todas las advertencias a que se refiere el apartado 1 del art. 5 de la L.O.P.D.. Igual principio deberá observarse si la recogida de dichos datos se efectúa directamente, sin cuestionarios o impresos.
* En particular, cuando se recaben datos para ser tratados en los ficheros de

Accidentes, **Personas** o **Sanciones** , puesto que en ellos se tratan datos especialmente protegidos, su recogida y posterior tratamiento deberá contar como regla general con el consentimiento expreso de los afectados, de conformidad en lo dispuesto en el art. 7 de la L.O.P.D., salvo que exista norma legal habilitante en contrario.

* No obstante lo anterior, en el fichero **Accidentes** , por su peculiar idiosincrasia, no será necesario cumplir con los requisitos del citado art. 5.1, pudiendo ser tratados los datos de carácter personal sin consentimiento del afectado cuando se den las circunstancias previstas en el art. 7.6 *in fine* de la L.O.P.D. Así mismo, en los ficheros **Personas** y **Sanciones** tampoco se requerirá cumplir con los requisitos del art. 5.1 y 2 de dicha Ley cuando su recogida impida o dificulte gravemente la persecución de infracciones penales o administrativas, de acuerdo con lo dispuesto en el art. 24. 1 de la misma Ley. Y finalmente, en los ficheros **Personas** y

Sanciones podrán tratarse sin consentimiento del afectado aquellos datos personales, incluso los especialmente protegidos a que se refiere el art. 7.3 de la L.O.P.D., para la finalidad prevista en el art. 85 del Real Decreto 772/1997, de 30 de mayo, por el que se aprueba el Reglamento General de Conductores, que desarrolla el Real Decreto Legislativo 339/1990, de 2 de marzo por el que se aprueba el Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial (Art. 5.4 en relación con los Arts. 60, 67 y concordantes del mencionado Real Decreto Legislativo).

* En este orden de ideas, debe recordarse que los datos recabados por la Agrupación de Tráfico de la Guardia Civil, aun sin olvidar su consideración de Fuerza y Cuerpo de Seguridad, cuando son recogidos para fines administrativos y no estrictamente policiales, su régimen jurídico está sujeto al régimen general de la Ley 15/1999 en cuanto a finalidad, recogida, consentimiento del afectado y demás principios de dicha Ley, de conformidad con lo establecido en el art. 22. 1 de la misma. Tan sólo cuando se den estrictamente las circunstancias previstas en el art. 22.2 y 3 de la L.O.P.D., podrán excepcionarse los mencionados principios en la recogida de datos personales por la mencionada Agrupación de Tráfico de la Guardia Civil y posterior tratamiento de los mismos.

SEGUNDA: DE LA COMUNICACIÓN O CESIÓN DE DATOS PERSONALES

En las cesiones de datos que realice la Dirección General de Tráfico deben distinguirse dos supuestos distintos: a) Cesiones o comunicaciones a terceros y b) Cesiones o comunicación de datos entre Administraciones Públicas.

* La cesión o comunicación de datos **a un tercero** deberá cumplir acumulativamente las dos condiciones exigidas por el art. 11.1 de la L.O.P.D.: que se haga para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario (lo que exige así mismo que los datos tratados sean pertinentes, proporcionados y oportunos para el fin que se pretende conseguir, de conformidad con el art. 4.1 de la Ley) y que se cuente con el previo consentimiento del afectado. Todo ello sin perjuicio de las excepciones contenidas en el art. 11.2, supuestos en que no será preciso el consentimiento del afectado, en particular cuando la cesión está autorizada en una Ley.
* En este último sentido, tal autorización legal se encuentra en el Art. 5 del Real Decreto Legislativo 339/1990, anteriormente citado, y sus normas de desarrollo reglamentario, en particular el Real Decreto 2822/1998, de 23 de diciembre, por el que se aprueba el Reglamento General de Vehículos, cuyo Art. 2 dispone que: *"El Registro de Vehículos tendrá carácter puramente administrativo, será público para los interesados y terceros que tengan interés legítimo y directo mediante simples notas informativas o certificaciones (...) Tendrá también función coadyuvante de las distintas Administraciones Públicas, Órganos Judiciales y Registros Civiles o mercantiles en los que se relaciona".*
* Por consiguiente, las consultas al fichero Vehículos sólo podrán ser informadas por la Dirección General de Tráfico a los interesados y terceros que acrediten un interés legítimo y directo en su consulta, de conformidad con el artículo transcrito.

(1)

* La cesión o comunicación de datos **entre Administraciones Públicas** deberá sujetarse a las siguientes recomendaciones:
* La cesión total de datos, entendida como cesión masiva e indiscriminada de los datos obrantes en los ficheros de **Vehículos** y **Personas** de la Dirección General de Tráfico, a la Dirección General de la Policía, deberá acomodarse, incluso en el supuesto de que se haga referencia genérica a la misma en la Orden de creación del fichero, a los principios contenidos en la L.O.P.D., esencialmente, en su artículo 4. Una cesión de este tipo deberá tomar como punto de partida lo dispuesto en el art. 22 de la L.O.P.D. de manera que se cumplan las siguientes condiciones:

Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.

Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.

(1)

En análogo sentido se ha pronunciado posteriormente la Sentencia de casación el Tribunal Supremo, Sala 3ª, Sección 6ª, de 31 de octubre de 2000.

Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.

Que, en cumplimiento del artículo 22.4 de la L.O.P.D., los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

* Las cesiones parciales o puntuales de datos de la Dirección General de Tráfico a otras Administraciones Públicas deberán ajustarse a lo prevenido con carácter general en el art. 21.1 de la L.O.P.D., de manera que los datos obtenidos por esa entidad para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo que la comunicación estuviere prevista por la norma de creación del fichero o por disposición de superior rango que regule su uso, o tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

(1)

* Por excepción, cuando se trate de la comunicación o cesión de datos a la Agencia Estatal de Administración Tributaria, no regirá lo señalado en el párrafo anterior, de conformidad con la Disposición Adicional Cuarta de la L.O.P.D. En este sentido, sí podrá suministrarse a la Agencia Tributaria los datos que solicite de esa Dirección General de Tráfico sin necesidad de contar con el consentimiento del afectado y ajustarse a las previsiones del citado art. 21.1 de la L.O.P.D., y ello como consecuencia de que los arts. 112 y 113 de la Ley General Tributaria cumplen con la previsión de la cesión efectuada por Ley conforme a lo establecido en el art. 11.2. a) de la L.O.P.D.
* En análogo sentido, sería válida la cesión de los datos personales contenidos en el fichero **Personas** a la Tesorería General de la Seguridad Social por estar prevista en el art. 36.6 de la Ley General de la Seguridad Social.
* En las cesiones a través de consultas "ON LINE" a favor de Ministerios y Órganos de las Administraciones Públicas que se enumeran anteriormente, deberá tenerse en cuenta que la cesión al Ministerio u Órgano en concreto ha de estar expresamente prevista por la norma de creación no bastando a estos efectos referencias genéricas, y que los datos cedidos sean adecuados y no excesivos para el ejercicio de sus competencias legítimas, entendiendo como tales las que le hayan sido legalmente atribuidas.

(1)

Véase la STC 292/2000, de 30 de noviembre. Esta recomendación no se hubiera podido dictar en tales términos tras la publicación de la citada sentencia puesto que ha declarado inconstitucional y nulo el inciso: "salvo que la comunicación estuviera prevista por la norma de creación del fichero o por disposición de superior rango que regule su uso".

* En ningún caso se podrán ceder datos de carácter personal a ficheros de titularidad privada, salvo que sea con el consentimiento del afectado o una ley prevea otra cosa, de conformidad con lo dispuesto en el art. 21.3 de la L.O.P.D.
* Para la comunicación o cesión de datos al Defensor del Pueblo, Ministerio Fiscal, Jueces o Tribunales o el Tribunal de cuentas, o instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, no será preciso el consentimiento del interesado, conforme a lo establecido en el art. 11.2.d) de la L.O.P.D.
* Los datos especialmente protegidos a que se refiere el art. 7 de la L.O.P.D. y que están recogidos en el fichero **Personas** , no podrán ser cedidos sin el consentimiento previo del afectado, salvas las excepciones legales previstas en el art. 11 de la L.O.P.D.

TERCERA: DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

* El ejercicio de estos derechos deberá facilitarse a los interesados de conformidad con lo previsto en los arts. 15 a 17 de la L.O.P.D., en los términos y plazos en ellos previstos.
* En particular, el derecho de acceso será gratuito conforme a lo prevenido en el art. 15.1 de la Ley, de manera que a partir de la entrada en vigor de la Ley 15/1999, el 14 de enero de 2000, la Dirección General de Tráfico no podrá exigir

contraprestación alguna, sea tasa o precio público, cuando el interesado solicite información de sus propios datos de carácter personal sometidos a tratamiento en el ejercicio del derecho de acceso.
* Ello no excluye la posibilidad de exigir tal contraprestación cuando lo que se solicite no sea el ejercicio del derecho de acceso a los propios datos personales del solicitante, sino la comunicación de datos de terceros, datos de carácter no personal o la prestación de determinados servicios tales como el cambio de titularidad de vehículos, la emisión de certificaciones, o la expedición de permisos de circulación, de conformidad con lo previsto en la Ley 8/1999, de 13 de abril, de Tasas y Precios Públicos, Ley 16/1979, de 2 de octubre y demás normas aplicables sobre la materia.
* Se deberán cancelar de oficio los datos de carácter personal cuando estos no sean necesarios para los fines para los que fueron recabados, no pudiendo ser conservados en forma que permita la identificación del interesado durante un período de tiempo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados, conforme a lo dispuesto en el art. 4.5 de la L.O.P.D., y debiendo ser conservados durante los plazos previstos en las disposiciones que sean aplicables (art. 16.5 L.O.P.D.).

CUARTA: DE LA INSCRIPCIÓN EN EL REGISTRO DE PROTECCIÓN DE DATOS

* La Dirección General de Tráfico deberá establecer los procedimientos oportunos para que la información que obra en los ficheros de los que es responsable se corresponda fielmente con los tratamientos que realiza, cumpliéndose las prescripciones señaladas en el art.20 de la L.O.P.D. Para ello se deberá notificar a esta Agencia de Protección de Datos la creación de nuevos ficheros, así como la rectificación o cancelación de los ya creados, en particular, para adecuarlos a las novedades introducidas por la nueva Ley 15/1999 a partir de su entrada en vigor, en relación con las posibles transferencias de datos que se prevean a terceros países y las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

QUINTA: DE LOS MOVIMIENTOS INTERNACIONALES DE DATOS

* En orden a los movimientos internacionales de datos deberá tenerse en cuenta que no podrán realizarse tales transferencias a países que no proporcionen un nivel de protección equiparable al que presta la vigente Ley 15/1999, requiriéndose en otro caso la autorización previa del Director de la Agencia de Protección de Datos conforme al art. 33 de dicha Ley y a excepción de los supuestos previstos en el art. 34 de la misma.

SEXTA: DE LAS MEDIDAS DE SEGURIDAD

Habiéndose publicado con posterioridad al inicio de las actuaciones inspectoras el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, resulta conveniente recordar las exigencias del mismo y particularmente:

* Que los sistemas de información que no se encontraran en funcionamiento a la entrada en vigor de la norma citada, deberán cumplir las medidas de seguridad correspondientes desde que se produzca su puesta en funcionamiento.
* Que dado los datos de carácter personal a tratar por esa Institución, sus ficheros deberán adaptarse a las medidas calificadas como de nivel medio por el citado Reglamento de Seguridad cuando contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública o cualesquiera otros datos de los mencionados en el art. 4.2 del citado Reglamento, y a las calificadas como de nivel alto cuando contengan datos de ideologías, creencias, origen racial, salud o vida sexual o cualesquiera otros datos de los expresados en el art. 4.3 del mismo Reglamento.
* El plazo de implantación de las citadas medidas, conforme a lo dispuesto en la disposición transitoria única al mencionado Reglamento de Seguridad, será de un año para las medidas de nivel medio y dos años para las de nivel alto, en ambos casos desde su entrada en vigor el 26 de junio de 1999. No obstante lo anterior, las medidas de seguridad de nivel básico, deben cumplirse, en todo caso, a partir del próximo día 26 de marzo, de conformidad con lo previsto en el Real Decreto 195/2000, de 11 de febrero.

2.1.3. Sector Sanitario

Con el mismo objeto de comprobar el grado de adecuación de las Instituciones públicas y ficheros privados a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal, el Director de la Agencia acordó el inicio de un Plan Sectorial de Inspección de Oficio de los ficheros automatizados que contuvieran datos personales en el sector de las Instituciones Sanitarias de carácter público, a fin de comprobar el grado de protección que por las mismas se otorga en el tratamiento de los datos relativos a la salud, que la Ley califica como especialmente protegidos.

Como continuación a lo publicado en la Memoria de 1999 respecto a las inspecciones realizadas en los hospitales General Militar Gómez Ulla y Psiquiátrico Penitenciario de Alicante, con dependencias funcionales del Ministerio de Defensa y de Justicia, respectivamente, además de la realizada en el Registro Nacional de SIDA, encuadrado en el Centro Nacional de Epidemiología, en el año 2000 el Director de la Agencia dictó las siguientes

RECOMENDACIONES:

* **Hospital General Militar Gómez Ulla**

PRIMERA: DEL DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Dejando al margen el procedimiento de recogida de datos de carácter personal llevado a cabo por el ISFAS a través de la denominada Tarjeta Sanitaria, que no ha sido objeto de las presentes actuaciones de inspección, cuando sea el propio Hospital Militar GÓMEZ ULLA el que proceda a la recogida de dichos datos de sus propios pacientes, deberán

cumplirse las previsiones establecidas en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de manera que deberá informarse a los afectados de todas las circunstancias previstas en dicho artículo y, en todo caso, de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, así como de la identidad y dirección del responsable del fichero.

Igualmente, cuando se utilicen formularios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legibles, las advertencias o circunstancias mencionadas.

No será necesario suministrar dicha información cuando el tratamiento de los datos del afectado sea necesario para salvaguardar el interés vital del afectado o de otra persona en el supuesto de que el afectado esté física o jurídicamente incapacitado o resulte necesario para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria y demás circunstancias previstas en el art. 7.6 de la Ley Orgánica 15/1999.

SEGUNDA: DEL TRATAMIENTO DE LOS DATOS ESPECIALMENTE PROTEGIDOS Y DEL CONSENTIMIENTO DEL AFECTADO

El art. 7 de la vigente Ley Orgánica 15/1999 regula el tratamiento de datos especialmente protegidos, limitando dicho tratamiento de datos relativos a la salud a aquellos casos en que lo autorice una ley o se obtenga el previo consentimiento del afectado. Sin embargo, el apartado 6 de dicho artículo y el art. 8 contienen una regulación específica para salvar la colisión entre el interés particular del afectado a la confidencialidad de los datos relativos a su salud y el interés general concretado en el derecho a la protección de la salud que reconoce el art. 43 de la Constitución.

Este interés general representado por la salud de todos los ciudadanos permite que en las instituciones y centros sanitarios públicos y privados, así como por los profesionales sanitarios se pueda proceder al tratamiento automatizado de datos de carácter personal cuando dicho tratamiento "*resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.*

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuanto el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento " (art. 7.6) o se refiera a datos de salud "*de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad* " (art. 8).

En estos casos la Ley excepciona el previo consentimiento del afectado para tratar sus datos de salud

Teniendo en cuenta que las presentes recomendaciones se dirigen exclusivamente al Hospital Militar GÓMEZ ULLA, este Centro podrá tratar los datos de sus pacientes sin el previo consentimiento de los mismos cuando se den las circunstancias previstas en los transcritos artículo 7.6 y 8 de la susodicha Ley Orgánica, si bien garantizando suficientemente la confidencialidad de los datos de salud de los pacientes y su estancia en la institución sanitaria, toda vez que el art. 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad, en concordancia con las previsiones de la Ley Orgánica 15/1999, reconoce el derecho del ciudadano a la confidencialidad de sus datos de salud y su estancia en las instituciones sanitarias públicas y privadas.

TERCERA: DEL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Sin perjuicio del derecho que pudieran tener los interesados para ejercitar estos derechos ante otros organismos del Ministerio de Defensa, deberá tenerse en cuenta que el responsable del tratamiento de los datos personales está obligado a facilitar a los interesados el ejercicio de los derechos de acceso, rectificación y cancelación en los términos expuestos en los arts. 15 y 16 de la Ley Orgánica 15/1999.

Así mismo, los interesados podrán oponerse al tratamiento de sus datos personales y deberá reconocérseles este derecho cuando se den las circunstancias previstas en el art. 6.4 de la citada Ley.

CUARTA: DE LA COMUNICACIÓN O CESIÓN DE DATOS En los términos del art. 11.1 de la Ley Orgánica 15/1999, se permite la comunicación o cesión de datos relativos a la salud sin el previo consentimiento del afectado "*cuando sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica* " (art. 11.2.f).

Así mismo, la Ley Orgánica 3/1986, de 14 de abril, de medidas en materia de Salud Pública, legitima a las Administraciones Públicas, en materia de enfermedades transmisibles, para adoptar las medidas oportunas para el adecuado control de los enfermos, además de las acciones preventivas de carácter general.

En consecuencia, el Hospital Militar GÓMEZ ULLA podrá comunicar o ceder a las Comunidades Autónomas y otras Administraciones Sanitarias los datos de salud por él tratados en los términos expuestos. Dadas las potestades de claro alcance discrecional que la Ley concede a las Administraciones sanitarias, tales cesiones deberán ser lo suficientemente motivadas como para justificar la limitación de los derechos de los afectados, en lo que a la confidencialidad de los datos relativos a la salud se refiere.

Cualquier cesión de otros datos personales que, como las nóminas de los empleados del Centro o los relativos al

Servicio de Farmacia, no se corresponda con las funciones y servicios sanitarios antes descritos y permitidos por la Ley, sólo podrá efectuarse de conformidad con el art. 11.1 de la Ley 15/1999 cuando se den acumulativamente dos condiciones: que sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, y que se cuente con el consentimiento previo del afectado.

QUINTA: DE LA INSCRIPCIÓN DE FICHEROS

De conformidad con lo previsto en el art. 39 de la Ley Orgánica 15/1999 y art. 5 del Real Decreto 1332/1994, de 20 de junio, deberá procederse a la inscripción en el Registro General de Protección de Datos de esta Agencia de todos los ficheros con datos de carácter personal, sean departamentales o no, de los que sea responsable ese Hospital.

SEXTA: DE LOS CONTRATOS CON OTRAS EMPRESAS

Dado que los contratos suscritos con las empresas Shared Medical Systems Corp. (S.M.S.) y Centro de Cálculo Sabadell (C.C.S.) lo han sido con la Secretaría General Técnica del Ministerio de Defensa y no con el Hospital Militar GÓMEZ ULLA, destinatario del Plan de Inspección de Oficio de esta Agencia, no cabe hacer recomendaciones al efecto.

SÉPTIMA: DE LAS MEDIDAS DE SEGURIDAD

Habiéndose publicado con posterioridad al inicio de las actuaciones inspectoras el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, resulta conveniente recordar las exigencias del mismo y particularmente:

Que los sistemas de información que no se encontraran en funcionamiento a la entrada en vigor de la norma citada, deberán cumplir las medidas de seguridad correspondientes desde que se produzca su puesta en funcionamiento.

Que dado los datos de carácter personal a tratar por esa Institución, sus ficheros deberán adaptarse a las medidas calificadas como de nivel medio por el citado Reglamento de Seguridad cuando contengan datos relativos a la Hacienda Pública o cualesquiera otros datos de los mencionados en el art. 4.2 del citado Reglamento, y a las calificadas como de nivel alto cuando contengan datos de salud o cualesquiera otros datos de los expresados en el art. 4.3 del mismo reglamento.

El plazo de implantación de las citadas medidas, conforme a lo dispuesto en la disposición transitoria única el mencionado Reglamento de Seguridad, será de un año para las medidas de nivel medio y dos años para las de nivel alto, en ambos casos desde su entrada en vigor el 26 de junio de 1999. No obstante lo anterior, las medidas de seguridad de nivel básico, deberán cumplirse, en todo caso, a partir del próximo día 26 de marzo, de conformidad con lo dispuesto en el Real Decreto 195/2000, de 11 de febrero.

* **Hospital Psiquiátrico Penitenciario de Alicante**

PRIMERA: En cuanto al ejercicio del derecho de rectificación de los datos personales de los reclusos contemplado en el art. 9.1 del Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario, deberá tener en cuenta que el responsable del tratamiento tendrá la obligación de hacer efectivo tal derecho en el plazo de diez días, de conformidad con lo dispuesto en el art. 16.1 de la citada Ley Orgánica 15/1999, y no en el plazo de dos meses previsto en el mencionado Reglamento Penitenciario, habida cuenta del obvio mayor rango normativo de la primera.

SEGUNDA: Respecto a los datos de Salud de los internos, deberán observarse las prescripciones establecidas en el art. 7 de la Ley Orgánica 15/1999 para los datos especialmente protegidos, de manera que para tratar o ceder datos de salud deberá contarse siempre con el previo consentimiento expreso del afectado. No obstante ello, dadas las características que normalmente presentarán los internos, no será necesario tal consentimiento cuando el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

TERCERA: En orden a los movimientos internacionales de datos deberá tenerse en cuenta que no podrán realizarse tales transferencias a países que no proporcionen un nivel de protección equiparable al que presta la vigente Ley 15/1999, requiriéndose en otro caso la autorización previa del Director de la Agencia de Protección de Datos, a excepción de los supuestos previstos en el art. 34 de la citada Ley.

CUARTA: De conformidad con lo previsto en el art. 39 de la Ley Orgánica 15/1999 y art. 5 del Real Decreto 1332/1994, de 20 de junio, deberá procederse a la inscripción en el Registro General de Protección de Datos de esta Agencia los ficheros denominados ARCHIVO y SOCIAL de los que es responsable esa entidad.

QUINTA: Habiéndose publicado con posterioridad al inicio de las actuaciones inspectoras el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, resulta conveniente recordar las exigencias del mismo y particularmente:

Que los sistemas de información que no se encontraran en funcionamiento a la entrada en vigor de la norma citada, deberán cumplir las medidas de seguridad correspondientes desde que se produzca su puesta en funcionamiento.
Que dado los datos de carácter personal a tratar por esa Institución, sus ficheros deberán adaptarse a las medidas calificadas como de nivel medio por el citado Reglamento de Seguridad cuando contengan datos relativos a la comisión de infracciones administrativas o penales, y a las calificadas como de nivel alto cuando contengan datos de ideologías,

creencias, origen racial, salud o vida sexual o contengan datos recabados para fines policiales, sin consentimiento de las personas afectadas. El plazo de implantación de las citadas medidas, conforme a lo dispuesto en la disposición transitoria única el mencionado Reglamento de Seguridad, será de un año para las medidas de nivel medio y dos años para las de nivel alto, en ambos casos desde su entrada en vigor el 26 de junio de 1999. No obstante lo anterior, las medidas de seguridad de nivel básico, deben cumplirse, en todo caso, desde el pasado 26 de diciembre de 1999.

* **Centro Nacional de Epidemiología. Registro Nacional del SIDA.**

PRIMERA: DE LA RECOGIDA Y TRATAMIENTO DE DATOS ESPECIALMENTE PROTEGIDOS

El art. 7 de la vigente Ley Orgánica 15/1999 regula el tratamiento de datos especialmente protegidos, limitando el tratamiento de datos relativos a la salud a aquellos casos en que lo autorice una Ley o se obtenga el previo consentimiento del afectado. Sin embargo, el apartado 6 de dicho artículo y el Art. 8 contienen una regulación específica para salvar la colisión entre el interés particular del afectado a la confidencialidad de los datos relativos a su salud y el interés general concretado en el derecho a la protección de la salud que reconoce el Art. 43 de la Constitución.

Este interés general representado por la salud de todos los ciudadanos permite que en las instituciones y centros sanitarios públicos y privados, así como por los profesionales sanitarios se pueda proceder al tratamiento automatizado de datos de carácter personal cuando dicho tratamiento *"resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto"* (Art. 7.6), o se refiera a datos de salud *" de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad" (* Art. 8).

En estos casos la Ley excepciona el previo consentimiento del afectado para tratar sus datos de salud.

Por su parte, la Ley 14/1986, de 25 de abril, General de Sanidad, permite en su Art. 8, como base del sistema sanitario, la obtención de una información suficiente que permita efectuar los estudios epidemiológicos necesarios para la prevención de la salud y la planificación sanitaria.

Así mismo, el Art. 10.3 de dicha Ley recoge el derecho del ciudadano a la confidencialidad de sus datos de salud y su estancia en instituciones públicas y privadas, y el Art. 23 de la misma permite a la Administración sanitaria crear registros y elaborar análisis de información para un mejor conocimiento de la situación que pueda justificar la intervención de las autoridades sanitarias.

En consecuencia y a tenor de lo expuesto, el Centro Nacional de Epidemiología podrá recabar y tratar datos de los afectados del SIDA que acudan directamente al Centro o su tratamiento de datos personales resulte necesario en los términos del art. 7.6 de la Ley Orgánica 15/1999, y siempre garantizando suficientemente la confidencialidad de sus datos de salud y estancia en la institución sanitaria, de conformidad con lo previsto en el citado Art. 10.3 de la Ley General de Sanidad.

En otro caso, deberá contarse con el consentimiento previo del afectado para tratar sus datos de salud, de conformidad con lo dispuesto en el art.7 de la Ley Orgánica 15/1999, de no resultar ello excepcionado por lo establecido en el art. 7. 6 y 8 de la citada Ley.

SEGUNDA: DEL DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Dado que conforme al art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, el derecho de información al afectado debe cumplirse al solicitarse sus datos de carácter personal y que la fuente de información son los médicos que diagnostican al enfermo (art. 33 R.D. 2210/1995, de 28 de diciembre) deberán ser estos profesionales, en dicho momento, los que informen al interesado de las circunstancias previstas en el citado art. 5. En otro caso, los responsables sucesivos del tratamiento de los datos, al no haberlos recabado directamente del interesado, tendrían la obligación de informar al afectado dentro de los tres meses siguientes al registro de los datos, salvo que existiera una ley que expresamente excluyera tal obligación (art. 5.4 Ley Orgánica 15/1999).

TERCERA: DE LAS CESIONES DE DATOS

En los términos del art. 11.1 de la Ley Orgánica 15/1999, se permite la comunicación o cesión de datos relativos a la salud sin el previo consentimiento del afectado *"cuando sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica"* (Art. 11.2.f).

Así mismo, la Ley Orgánica 3/1986, de 14 de abril, de medidas en materia de Salud Pública, legitima a las Administraciones Públicas, en materia de enfermedades transmisibles, para adoptar las medidas oportunas para el adecuado control de los enfermos, además de las acciones preventivas de carácter general.

En consecuencia, el Centro Nacional de Epidemiología podrá comunicar o ceder a las Comunidades Autónomas y otras Administraciones Sanitarias los datos de salud por él tratados en los términos expuestos. Dadas las potestades de claro alcance discrecional que la Ley concede a las Administraciones Sanitarias, tales cesiones deberán ser lo suficientemente motivadas como para justificar la limitación de los derechos de los afectados, en lo que a la confidenciali-

dad de los datos relativos a la salud se refiere.

CUARTA: DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN

En todo caso, deberá facilitarse a los interesados el ejercicio de los derechos de acceso, rectificación y cancelación de sus datos personales, en los términos establecidos en los artículos 15 y 16 de la Ley Orgánica 15/1999.

Igualmente, deberá reconocerse el derecho de oposición al tratamiento de sus datos personales, a iniciativa del afectado, en los términos recogidos en el art. 6.4 de la citada Ley Orgánica.

QUINTA: DE LOS MOVIMIENTOS INTERNACIONALES DE DATOS

En orden a los movimientos internacionales de datos deberá tenerse en cuenta que no podrán realizarse tales transferencias a países que no proporcionen un nivel de protección equiparable al que presta la vigente Ley 15/1999, requiriéndose en otro caso la autorización previa del Director de la Agencia de Protección de Datos, a excepción de los supuestos previstos en el art. 34 de la citada Ley, en especial su apartado c).

No obstante lo anterior, en la medida en que los datos transferidos al Centro Europeo de la O.M.S. estén disociados, no será necesaria la referida autorización.

SEXTA: DE LAS MEDIDAS DE SEGURIDAD

Habiéndose publicado con posterioridad al inicio de las actuaciones inspectoras el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, resulta conveniente recordar las exigencias del mismo y particularmente:

Que los sistemas de información que no se encontraran en funcionamiento a la entrada en vigor de la norma citada, deberán cumplir las medidas de seguridad correspondientes desde que se produzca su puesta en funcionamiento.

Que dado los datos de carácter personal a tratar por esa Institución, sus ficheros deberán adaptarse a las medidas calificadas como de nivel medio por el citado Reglamento de Seguridad cuando contengan datos relativos a la comisión de infracciones administrativas o penales, y a las calificadas como de nivel alto cuando contengan datos de ideologías, creencias, origen racial, salud o vida sexual.

El plazo de implantación de las citadas medidas, conforme a lo dispuesto en la disposición transitoria única el mencionado Reglamento de Seguridad, será de un año para las medidas de nivel medio y dos años para las de nivel alto, en ambos casos desde su entrada en vigor el 26 de junio de 1999. No obstante lo anterior, las medidas de seguridad de nivel básico, deberán cumplirse, en todo caso, a partir del próximo día 26 de marzo, de conformidad con lo dispuesto en el Real Decreto 195/2000, de 11 de febrero.

2.1.4. Detectives privados

Como consecuencia del plan de oficio por el que se inspeccionó durante el año 1999 el sector de los detectives privados, cuya actividad se regula en la Ley 23/92, de 30 de julio, de Seguridad Privada y en el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, el Director de la Agencia dictó las

RECOMENDACIONES que se recogen a continuación, con el fin de permitir a este sector una mejor adecuación de sus tratamientos automatizados a los principios establecidos en la Ley Orgánica 15/1999.

PRIMERA: DE LA RECOGIDA DE DATOS

Aquellas entidades que para la realización de las funciones que les encomienda el art. 19.1 de la Ley 23/1992, de 30 de julio, de Seguridad Privada, y el art. 101.1 del Reglamento de Seguridad Privada aprobado por R.D. 236/1994, de 9 de diciembre, recaben datos de carácter personal de sus clientes, que sean personas físicas, deberán informarles previamente de modo expreso, preciso e inequívoco, de todas las circunstancias previstas en el apartado 1 del art. 5 de la Ley 15/1999, de 13 de diciembre, si sus datos fueran a ser tratados automatizadamente.

Sin embargo, si de la relación contractual con su cliente se dedujera claramente el contenido de dicha información, sólo será preciso informar de las circunstancias previstas en los apartados a) y e) del citado art. 5.1, de conformidad con lo previsto en su apartado 3.

No obstante lo anterior, tratándose de datos especialmente protegidos mencionados en el art. 7 de la citada Ley, los mismos sólo se podrán recabar con el consentimiento expreso del afectado, consentimiento que, además, deberá ser por escrito si tales datos revelan la ideología, afiliación sindical, religión o creencias del afectado.

SEGUNDA: DE LA RECOGIDA LÍCITA Y LEAL

Teniendo en cuenta lo expuesto anteriormente en el apartado *in fine* del punto relativo al "origen de la información", deberá observarse escrupulosamente por las entidades del sector el principio de la recogida lícita y leal establecido en el art. 5.7 de la Ley 15/1999, conforme al cual se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos, de manera que cada entidad responderá de la adecuación a este principio de cualquier dato recogido por sus

empleados o mandatarios.

TERCERA: DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS Y DEL CONSENTIMIENTO DEL AFECTADO

Los mismos principios señalados en la recomendación anterior para la "recogida" de datos de carácter personal, han de regir para su "tratamiento automatizado", de manera que el consentimiento del afectado habrá de ser otorgado de forma inequívoca, de acuerdo con lo dispuesto en el art. 6.1 de la Ley, y salvo las excepciones previstas en el art. 6.2 de la misma.

Tratándose de datos especialmente protegidos, relativos a origen racial, salud o vida sexual sólo podrán ser tratados si el afectado consiente expresamente o hay excepción legal; consentimiento que además deberá constar por escrito si se tratan datos de ideología, afiliación sindical, religión y creencias, conforme a lo preceptuado en el art. 7 de la Ley.

Estas recomendaciones deberán ser especialmente observadas por aquellas entidades que conforme al art. 108 del Reglamento de Seguridad Privada llevan un Libro Registro Automatizado autorizado por el Ministerio del Interior en el que constan datos de carácter personal de los clientes y personas investigados, así como las que usan procesadores de textos para la confección de sus informes.

CUARTA: DE LA PROHIBICIÓN DE ALMACENAR DATOS SENSIBLES

Las entidades de referencia no podrán en ningún caso crear ni tener ficheros con la finalidad exclusiva de almacenar datos de carácter personal especialmente protegidos, de conformidad con lo prevenido en el art. 7.4 de la Ley 15/1999.

QUINTA: DE LA PROHIBICIÓN DE INCLUSIÓN DE CIERTOS DATOS EN FICHEROS PRIVADOS

Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas no podrán ser incluidos en los ficheros de las entidades objeto de este Plan de Inspección, de conformidad con lo dispuesto en el art. 7.5 de la citada Ley 15/1999.

SEXTA: DE LOS DATOS OBTENIDOS DE FUENTES ACCESIBLES AL PÚBLICO

A partir del 14 de enero de 1999, fecha de entrada en vigor de la Ley 15/1999, de 13 de enero, las entidades del Sector de la Investigación Privada deberán tener presente que el origen de la información obtenida en el ejercicio de sus funciones, cuando se trate de fuentes públicas, solamente tendrá tal consideración cuando se obtenga de alguna de las fuentes de acceso al público que expresa y taxativamente enumera el art. 3, apartado j) de la citada Ley.

En consecuencia, la obtención de datos de carácter personal de cualquier fuente que, como los Registros de la Propiedad o Mercantil, fuese distinta de las enumeradas en el citado art. 3.j), deberá contar con el consentimiento previo del interesado si sus datos fuesen a ser automatizados.

SÉPTIMA: DE LA CONSERVACIÓN Y CANCELACIÓN DE LOS DATOS PERSONALES

Las entidades de referencia deberán cumplir y atenerse al principio de conservación limitada de datos de carácter personal consagrado en el art. 4.5 de la Ley, de manera que no se conservarán datos en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Así mismo, dichos datos deberán ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Esta cancelación procederá hacerla de oficio y es obligatoria para el responsable del fichero, a diferencia de la prevista en el art. 16 de la Ley, que se produce a petición del afectado.

OCTAVA: DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN EN FICHEROS NO AUTOMATIZADOS

Sin perjuicio de lo señalado en la recomendación anterior y del plazo de adecuación previsto en la Disposición Adicional Primera de la Ley Orgánica 15/1999, las entidades del sector que tengan ficheros o hagan tratamiento no automatizado de datos personales, deberán en todo caso, y ya se trate de ficheros anteriores o posteriores a la entrada en vigor de la mencionada Ley Orgánica, facilitar el ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados desde la entrada en vigor de dicha Ley, el día 14 de enero de 2000.

NOVENA: DE LA COMUNICACIÓN O CESIÓN DE DATOS

No habiéndose constatado ni evidenciado en la inspección practicada a las entidades del sector cesión alguna o comunicación de datos a terceros contraria a la Ley, pero teniendo en cuenta que no todas las entidades del sector han sido inspeccionadas, sólo cabe recordar a los efectos del cumplimiento de tan importante previsión legal que, salvadas las excepciones previstas en el número 2 del art. 11 de la Ley, la comunicación de datos a terceros sólo podrá hacerse de conformidad con el art. 11.1 cuando se den acumulativamente dos condiciones: que sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario; y que se cuente con el consentimiento previo del interesado.

DÉCIMA: DE LA CALIDAD DE LOS DATOS

Por la misma razón anterior, cabe hacer una recomendación de tipo general respecto al cumplimiento por dichas entidades del principio de pertinencia y adecuación en la recogida y tratamiento de datos personales, regulado en el art. 4. 1 de la Ley, así como del principio de finalidad recogido en el apartado 2 del mismo artículo.

UNDÉCIMA: DEL REGLAMENTO DE MEDIDAS DE SEGURIDAD

Habiéndose publicado con posterioridad al inicio de las actuaciones inspectoras el Real Decreto 994/1999, de 11 de junio, resulta conveniente recordar las exigencias del mismo y, particularmente:

* Que los sistemas de información que no se encontraran en funcionamiento a la entrada en vigor de la norma citada, deberán cumplir las medidas de seguridad correspondientes desde que se produzca su puesta en funcionamiento.
* Que los ficheros automatizados que utilicen las entidades del Sector de la Investigación Privada deberán adaptarse a las medidas calificadas como de nivel medio por el citado Reglamento de Seguridad cuando contengan datos relativos a servicios financieros o la prestación de servicios de información sobre solvencia patrimonial y crédito, y a las calificadas como de nivel alto cuando contengan datos sobre ideologías, creencias, origen racial, salud o vida sexual o contengan datos recabados para fines policiales, sin consentimiento de las personas afectadas.

El plazo de implantación de dichas medidas conforme a lo dispuesto en la disposición transitoria única del mencionado Reglamento de Seguridad, será de un año para las medidas de nivel medio y de dos años para las de nivel alto, en ambos casos desde su entrada en vigor el 26 de junio de 1999. No obstante lo anterior, las medidas de seguridad de nivel básico deberán cumplirse, en todo caso, a partir del próximo día 26 de marzo, de conformidad con lo dispuesto en el Real Decreto 195/2000, de 11 de febrero.

2.2. PLANES SECTORIALES DE OFICIO 2000

Como se decía a modo de prólogo de este mismo apartado 2, la Agencia de Protección de Datos, siguiendo el mismo criterio y orientación de ejercicios anteriores, ha prestado durante el año 2000 una especial importancia a los Planes Sectoriales de Oficio desarrollando durante este año una intensa actividad en el marco de las inspecciones de oficio que la LOPD permite, al objeto de comprobar, como ya se dijo, el grado de adecuación de diversos sectores económicos a las prescripciones de dicha Ley. Tras el análisis de las inspecciones realizadas la APD dictará las oportunas RECOMENDACIONES dirigidas no sólo a las entidades inspeccionadas, sino también a las asociaciones y entidades más representativas del sector implicado.

A tal fin se iniciaron y concluyeron durante el año 2000 las siguientes inspecciones que afectan: al sector del comercio electrónico; a proveedores de servicios de internet; a la gestión de tarjetas en grandes superficies comerciales; al sector de las telecomunicaciones; y al Consorcio de Compensación de Seguros, con los resultados que se exponen a continuación.

2.2.1. Comercio Electrónico

En su *Estudio de Situación del Comercio Electrónico en España* , de mayo de 1999, el Ministerio de Fomento definió esta actividad como "cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de telecomunicación como Internet", incluyendo por tanto "no sólo la compra y venta electrónica de bienes, información o servicios, sino también el uso de la Red para actividades anteriores o posteriores a la venta, como son: la publicidad; la búsqueda de información sobre productos, proveedores,...; la negociación entre comprador y vendedor sobre precio, condiciones de entrega,...; la atención al cliente antes y después de la venta; la cumplimentación de trámites administrativos relacionados con la actividad comercial; la colaboración entre empresas con negocios comunes".

En este mismo estudio se distinguían cinco tipos básicos de comercio electrónico: entre empresas o B2B (business to business), entre empresa y consumidor o B2C (business to consumers), entre empresa y Administración o B2A (business to administrations), la venta directa entre consumidores y las transacciones económicas entre ciudadano y Administración.

El propio Departamento de Fomento consideraba que algunos de los problemas que el comercio electrónico plantea como nuevos o que agudiza, en relación con el comercio tradicional son, precisamente, "*la protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales* " y "*la seguridad de las transacciones y medios de pago electrónicos* ". Así mismo, entendía que entre las barreras iniciales para el crecimiento del comercio electrónico figura la reticencia de los usuarios a, por ejemplo, enviar los datos de su tarjeta de crédito a través de Internet para efectuar un pago, o su preocupación respecto del uso que el vendedor hará de sus datos personales.

La Agencia de Protección de Datos es consciente de que en la actualidad existe una gran diversidad en cuanto a los niveles de seguridad y procedimientos de compra que debe utilizar el ciudadano en función de la web a la que acceda, incluyendo la forma en que se presenta la información, los sistemas de pago aceptados o la información que recibe del vendedor en el momento de realizar su compra. Es objetivo de este organismo contribuir, dentro de las competencias que legalmente tiene atribuidas, al desarrollo de esta actividad, tratando de armonizarlo con la atención efectiva de los derechos que el ciudadano tiene reconocidos y estableciendo un marco específico que pueda ser utilizado por el sector

como referencia, en aras de un mejor cumplimiento de la Ley.

Siguiendo esta línea, durante los meses de septiembre, octubre y noviembre de 2000, la Agencia de Protección de Datos ha llevado a cabo una inspección sectorial cuyo objetivo ha sido precisamente determinar si las entidades que actualmente desarrollan su actividad comercial a través de Internet cumplen con los principios de la legislación vigente en materia de protección de datos: calidad de los datos almacenados, información facilitada a los afectados, consentimiento, datos especialmente protegidos, seguridad, deber de secreto, comunicación de datos, movimiento internacional y ejercicio de los derechos del ciudadano. En este sentido, nuestro análisis se ha circunscrito a dos de las modalidades de comercio electrónico en las que el ciudadano tiene una clara participación: el modelo B2C y la venta directa entre consumidores.

En relación con el mundo de Internet, hasta el momento la Agencia había inspeccionado varias de las entidades que ofrecen servicios de acceso, alojamiento y correo electrónico (proveedores de servicios de Internet, PSI), habiéndose observado que casi todas ellas también realizaban prácticas de comercio electrónico. Dado que cada vez cobran mayor importancia los servicios de certificación electrónica, se estudió la posibilidad de analizar el funcionamiento de las compañías y organismos que en la actualidad actúan en calidad de fedatarios. Sin embargo, se consideró más conveniente centrarse en una primera fase sólo en las entidades que actúan en calidad de comerciantes o que alojan las páginas a través de las que se comercializan productos y servicios, dejando para más adelante la investigación sobre los otros intervinientes en el negocio.

Por otra parte, también se decidió circunscribir el análisis a las entidades que comercian a través de la Red, dejando de momento a un lado a aquellas otras que tan sólo disponen de portales generalistas entre cuyos servicios no se ofrece la adquisición on-line de productos o servicios, a pesar de que también estas compañías recaban gran cantidad de datos sobre los usuarios que deciden registrarse. En este sentido, sólo se han incluido en nuestro análisis algunos portales que sí realizan actividades de comercio electrónico. Las conclusiones vertidas aquí, por tanto, se han obtenido como resultado de las actuaciones de inspección practicadas en las denominadas "*tiendas virtuales* ", entendiendo como tales las webs que permiten al usuario la compra, directa o indirectamente, de un producto o servicio, de forma tal que la transacción comercial (a excepción de la entrega del bien adquirido) quede cerrada on-line.

Junto con la legislación específica en materia de protección de datos, se consideraron también otras normas jurídicas que de alguna manera eran aplicables al mundo Internet: *Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior* (Directiva sobre el comercio electrónico, actualmente en trámites de transposición al derecho español, y cuyo *considerando 14* remite a las Directivas 95/46/CE y 97/66/CE*); Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de la contratación* ; *Real Decreto Ley14/1999, de 17 de septiembre, sobre firma electrónica y regulación de los prestadores de servicios de certificación* ; *Orden de 21 de marzo de 2000, del Ministerio de Fomento, por la que se regula el sistema de asignación de nombres de dominio de Internet bajo el código de país correspondiente a España (.es)* .

Respecto de la protección de datos en las actividades de comercio electrónico, también se han tenido en cuenta las iniciativas privadas de autorregulación en esta materia: la de la Asociación Española de Comercio Electrónico (¡Error! Marcador no definido.) y la Federación Española de Comercio Electrónico y Marketing Directo (¡Error! Marcador no definido., en su *Código Ético de Protección de Datos personales en Internet* (que fue inscrito en el año 1998 en el Registro General de Protección de Datos, y de cuyo cumplimiento hacen gala algunas de las tiendas virtuales investigadas, a través del denominado "*Sello de garantía de protección de datos")*, y el *Código de Deontología Profesional de las Empresas Proveedoras de Servicios de Internet* , de la Asociación Multisectorial de Empresas Españolas de Electrónica (ASIMELEC).

Durante los citados meses de septiembre, octubre y noviembre de 2000 se han analizado 44 webs desde las que actualmente se desarrollan actividades de comercio electrónico. Considerando la gran diversidad existente en el sector, en el análisis previo se ha optado por seleccionar varios representantes de cada uno de los siguientes grupos:

* Portales generalistas: webs que, aparte de ofrecer servicios electrónicos como noticias, correo web o foros, incorporan además la venta de productos o servicios en general.
* Grandes centros comerciales: versión electrónica de algunos grandes centros comerciales (" *híper* ", "*súper* ").
* Tiendas especializadas en la venta de determinados productos y servicios: libros, música, cine, bebidas alcohólicas, viajes, ocio, cosmética, informática o telecomunicaciones. En este apartado, y considerando las implicaciones de la adquisición de algunos productos en cuanto a la posible categorización de los compradores con un determinado perfil sexual o sanitario, se ha prestado especial atención a las webs desde las que se venden productos eróticos (orientados en exclusiva al público adulto), así como a aquéllas otras que ofrecen correctores de determinadas discapacidades físicas (ortopedia) o productos curativos (excluyendo los medicamentos, dado que el artículo 3.4 de la Ley 25/1990, de 20 de diciembre, del Medicamento, prohibe su venta por correo o por cualquier otra forma de venta indirecta al público). No se ha seleccionado en este grupo ninguna compañía del sector asegurador a pesar de que muchas de ellas ya disponen de webs diseñadas específicamente para que el usuario realice on-line sus solicitudes de póliza, aportando para ello una gran variedad de datos personales, incluidos los relativos a su estado de salud. Ello es debido a las especiales características que rodean a este sector, las cuales requerirían un estudio más específico que quizás podría acometerse más adelante.
* Intermediarios comerciales: webs que no son tiendas propiamente dichas pero desde las cuales el usuario puede seleccionar la tienda virtual que más se adecúa a sus necesidades ("*buscadores de tiendas*") y también aquéllas otras webs desde las que los usuarios compran y venden sus propios productos siguiendo la modalidad de subasta.

El estudio realizado se ha desarrollado en dos fases. Durante la primera se analizaron diversos aspectos generales de 44 webs, a través de un ordenador conectado a Internet y ubicado en la sede de la propia Agencia. Teniendo como base la información obtenida en la fase anterior, se seleccionaron 11 webs (la cuarta parte de las analizadas), a cuyos responsables se realizó una visita de inspección, durante la cual se verificó exhaustivamente el nivel de cumplimiento respecto de los principios legales de protección de datos, incluyendo un análisis más pormenorizado de las medidas de seguridad adoptadas. La siguiente tabla muestra una clasificación de las tiendas analizadas en la primera fase, de acuerdo a las agrupaciones mencionadas en el apartado anterior.

TIPOLOGÍA	Webs
Portales generalistas	3
Grandes Centros Comerciales ("híper", "super")	3
Tiendas especializadas	30
Bebidas	1
Informática	3
Libros, Música, Cine	6
Perfumes, Cosmética	2
Productos eróticos, exclusivamente para adultos	5
Productos naturales	1
Productos ortopédicos	1
Telecomunicaciones	2
Todo tipo de productos en general	7
Viajes, Ocio	2
Intermediarios comerciales	8
Subasta (compraventa) de productos en general	2
Otros intermediarios	6

En la totalidad de las webs analizadas se ha podido determinar el nombre de la compañía que ha registrado el dominio correspondiente en Internet, verificándose que no siempre se informa desde la propia web del nombre del responsable del fichero en el que se incorporan los datos personales que se recaban. En este sentido, se ha comprobado también que en 12 de las 44 webs analizadas (27%) no se hace ninguna referencia a la información que establece el apartado 1 del artículo 5 de la LOPD, mientras que en el resto sí se incluye un texto que pretende cubrir en mayor o menor medida ese requisito legal. Es bastante significativo que entre esas 12 webs se hallan precisamente las 5 que se dedican a la comercialización de productos eróticos y la que vende productos ortopédicos.

Por otra parte, también se ha verificado que los responsables de 16 de las 44 webs analizadas (36%) no figuran en la actualidad inscritos en el Registro General de Protección de Datos, cuando en la práctica totalidad de los casos resulta evidente que recaban datos personales desde las citadas webs.

Se ha comprobado que, en la mayor parte de los casos, los usuarios deben registrarse con carácter previo a la realiza - ción del oportuno pedido, facilitando para ello sus datos identificativos (NOMBRE COMPLETO, DIRECCIÓN POSTAL, DIRECCIÓN ELECTRÓNICA, NÚMERO DE TELÉFONO) y, en ocasiones, EDAD o FECHA DE NACIMIENTO, NÚMERO DE D.N.I. Una vez registrado, el usuario dispone de un código que le permitirá identificarse (generalmente coincidente con su dirección electrónica) y una contraseña para autenticar su identidad. De esta forma, al realizar cada pedido sólo tendrá que identificarse, sin necesidad de facilitar en cada ocasión sus datos personales. Generalmente, todas las compras realizadas a través de la web quedarán asociadas al identificador de usuario seleccionado. Por otra parte, si el usuario decide realizar el pago mediante su tarjeta de crédito/débito, cada vez que realiza una compra debe también facilitar el código identificativo de la misma (16 dígitos) y su fecha de caducidad.

En materia de seguridad, de las 44 webs analizadas sólo 24 (54%) utilizan el protocolo HTTPS para establecer un " *canal seguro* " de comunicación entre el servidor y el usuario para el envío de sus datos personales. Así, los datos se envían cifrados al servidor, de tal forma que, aun en el supuesto de que la línea fuese *"escuchada"* por terceros no autorizados, éstos no podrían acceder a los datos de forma inteligible. Para ello, el dominio en el que se ubica la web ha debido ser convenientemente certificado por alguna entidad reconocida (en la mayor parte de las webs analizadas, la americana VERISIGN, Inc.). En general, el canal seguro sólo se establece para la recogida de los datos asociados al pedido realizado, entre los que puede figurar, como ya se ha comentado, el código identificativo de la tarjeta de pago. Sin embargo, algunas webs también establecen un canal seguro para la recogida de los datos facilitados por el usuario en el momento de registrarse.

Finalmente, según se ha podido comprobar, en la actualidad 10 de las 44 compañías (22%) cuyas webs se han analizado están adheridas a la Asociación Española de Comercio Electrónico.

A continuación, se recopilan algunas de las situaciones más frecuentes o significativas que se han presentado a lo largo de las actuaciones practicadas por la Inspección.

2.2.1.1. Responsabilidad del tratamiento de datos de carácter personal

Se ha podido comprobar que en algunas de las tiendas investigadas no se identifica explícitamente al responsable del fichero o tratamiento, lo que deja de alguna forma indefenso al afectado de cara al ejercicio de sus derechos, puesto que, como ya se ha señalado, dicha figura jurídica no siempre coincide con la de la entidad o persona que ha registrado el dominio en Internet. Es más, en algunos casos ni siquiera se identifica a ésta última a través de la web, lo que obligaría al afectado a averiguarlo por su cuenta, a través del organismo registrador correspondiente.

Por otra parte, en Internet resulta sencillo navegar entre páginas cuya ubicación real es transparente para el usuario, de tal forma que con sólo hacer "*click* " en un icono es posible dejar de visualizar una página ubicada en territorio español para pasar a ver otra página almacenada, por ejemplo, en Estados Unidos. Esta circunstancia hace que, en ocasiones, el usuario crea estar facilitando sus datos personales a una entidad cuando en realidad es otra (radicada probablemente en otro lugar del mundo) la que los está obteniendo, siendo muchos los casos en los que ésta última no se identifica claramente en la web.

2.2.1.2. Modelos de colaboración entre entidades para la venta en Internet

La Inspección ha comprobado la diversidad de modelos que existen hoy en día en relación con la colaboración que establecen las compañías para vender sus productos a través de la red. A continuación se relacionan los más frecuentes.

* Hiperenlace a tiendas

Desde la página de una compañía (generalmente, portales o intermediarios comerciales) se accede (con sólo hacer click) a la página de otra compañía desde la que ésta ofrece productos y servicios. A este procedimiento se le denomina "*link* " o hiperenlace. La primera compañía actúa en calidad de comisionista de los beneficios obtenidos por la segunda a partir de las ventas que se han realizado desde su propia página como resultado de este procedimiento.

En este modelo los compradores facilitan sus datos personales a la segunda compañía, que generalmente mantiene el anonimato de sus compradores con respecto a la primera compañía.

Sin embargo, cabe reseñar el caso de una web, propiedad de una compañía americana especializada en subastas, que ofrece ciertos contenidos para el público en general y que ha llegado a un acuerdo con otra compañía española para el patrocinio de la web en nuestro país. En virtud de este acuerdo, cuando un usuario accede a la web (haciendo click en la zona correspondiente del portal de la compañía española) lo que visualiza son las mismas páginas que si accediera directamente a la web americana (en su versión en castellano), pero con una particularidad: se sustituye el nombre de la empresa americana por una marca comercial que no corresponde a ninguna denominación social, pero que identifica plenamente a la compañía nacional. Es más, esa marca comercial figura como garante de la confidencialidad de la información solicitada sobre los usuarios de la página, a pesar de que al parecer los datos personales son recabados por la compañía americana. Para mayor confusión, en estas páginas se hace constar (en castellano) que las informaciones nominativas son consignadas en un fichero bajo control de la citada marca, teniendo como base la legislación francesa de protección de datos.

Por otra parte, existen casos en los que la primera compañía ofrece una bonificación especial (canjeable por descuentos) a los usuarios que compren a través de la web de la segunda habiendo accedido para ello mediante un hiperenlace desde su propia web. En estas ocasiones, la bonificación se materializa necesariamente teniendo como base un fichero entregado por la segunda compañía a la primera, en el cual se hacen constar los puntos que corresponden a cada comprador (al que se identifica por el número de su D.N.I.). Sin embargo, se puede dar el caso de que la persona que compre en la segunda web no se haya registrado previamente como usuario de la primera (aunque sí haya hiperenlazado desde esta web) y no le corresponda, por tanto, ninguna bonificación. El resultado final es que los datos del comprador acaban en poder de ambas compañías cuando la relación comercial sólo la ha establecido con la segunda.

* Oferta del catálogo de productos de otra compañía

Una compañía incluye en su propia página (generalmente a través de un subdominio) el catálogo de productos de otra compañía (cuya denominación o marca también se hacen constar), de tal forma que la primera compañía actúa como comisionista de las ventas realizadas de esos productos.

En las webs inspeccionadas que siguen este modelo se ha comprobado que ambas compañías incorporan a sus ficheros los datos personales de los compradores.

* Explotación conjunta de contenidos

Son habituales los casos en los que una compañía, cuya web ha triunfado en un determinado ámbito de negocio, ofrece un programa de afiliación mediante el cual otras compañías (incluso de otros países) pueden beneficiarse de los

contenidos y del "*know-how* " de aquélla, adaptándolos al mercado de su propio entorno. La confusión crece en los usuarios, dado que muchas veces no saben si sus datos irán a parar a la primera compañía, a la segunda o, incluso, a ambas.

En este sentido, la Inspección ha podido verificar la existencia de una página española (ubicada en un dominio registrado por una sociedad nacional con gran implantación en nuestro país) desde la que se recaban datos cuyo destino es una compañía sueca radicada en Chipre, que registró su propio dominio desde Gibraltar y cuyos ficheros se almacenan probablemente en los ordenadores de otra compañía en Gran Bretaña. Sin embargo, en la página correspondiente no se informa acerca de ninguna de estas circunstancias.

* Intervención de compañías colaboradoras

La entrega de los productos y servicios adquiridos a través de Internet requiere la ejecución de determinadas operaciones logísticas que, en ocasiones, no son realizadas por la compañía vendedora sino encargadas a empresas especializadas en este tipo de labores. Esta colaboración requiere, al menos, el acceso a la dirección postal del destinatario.

Así mismo, se ha observado que en ocasiones también es precisa la participación activa de los suministradores de determinados productos y servicios, como pueden ser las agencias de viajes o los establecimientos de entrega de flores a domicilio, los cuales necesariamente deben conocer los datos personales de los titulares del bien adquirido. Se ha verificado que sólo en algunos de estos casos el propio vendedor reconoce contractualmente al suministrador la condición de "*encargado del tratamiento* " en los términos del artículo 12 de la LOPD.

2.2.1.3. Información facilitada en la recogida de datos

* *Respecto del contenido*

Una de las carencias más notables que se han observado es precisamente la insuficiente información que se facilita al visitante de la tienda en el momento de recabar sus datos personales (cuando el usuario se registra como cliente o cuando efectúa un pedido). Es significativo que en más de la cuarta parte de los casos analizados no se facilite en absoluto la información que prevé la LOPD en su artículo 5, ni se pueda deducir claramente ésta de la naturaleza de los datos personales recabados ni de las circunstancias en que se recaban.

Por otra parte, las fórmulas informativas utilizadas en el resto de los casos tampoco se ajustan siempre a lo que establece la Ley. Como ya se ha mencionado antes, son numerosas las webs en las que no se identifica explícitamente al responsable del fichero o del tratamiento, lo que se agrava especialmente en aquellos casos en los que el usuario accede a una página a través de un hiperenlace, de tal forma que no sabe a ciencia cierta adónde irán a parar sus datos, ni por tanto a quién podría pedir responsabilidades por su uso indebido.

Además, por las especiales características del mundo Internet, en ocasiones resulta complicado para el usuario distinguir claramente la figura del comerciante (con quien realmente el comprador establece la transacción comercial) de la figura de mero intermediario (que pone en contacto -virtual- a ambos). En este sentido, el usuario debería ser consciente de que, una vez que ha facilitado sus datos, éstos pueden pasar por las manos de los distintos intervinientes en el proceso: el que gestiona los servidores web por cuenta del comerciante, el propio comerciante, el que autoriza la transacción financiera, el que se encarga de emitir los documentos que otorgan la titularidad del producto (por ejemplo, una agencia de viajes), el que se encarga de servir el producto (logística), el que se encarga de prestar la atención al cliente... Dado que no siempre coinciden estas figuras en una misma entidad jurídica, es muy importante que el comprador sepa quién de todos ellos es el que finalmente decidirá sobre el uso y finalidad de sus datos personales.

Por otra parte, son muy numerosas las webs en las que se informa al ciudadano de que sus datos serán compartidos con "*otras compañías del mismo grupo empresarial* ", lo que no siempre es suficiente para que el comprador pueda conocer la identidad de los cesionarios. Este hecho tiene una importante repercusión, si se consideran los frecuentes cambios que se producen en el accionariado de las compañías de Internet, las cuales dejan de pertenecer a un grupo empresarial para integrarse en otro debido a una modificación de su estrategia de negocio, como ha podido comprobarse en varios de los establecimientos inspeccionados. En tales casos, el usuario puede verse desconcertado al descubrir que sus datos son conocidos y utilizados por compañías a las que no era consciente de habérselos facilitado.

En relación con el ejercicio de los derechos que asisten al ciudadano, por regla general se facilita un buzón electrónico, a través del cual se reciben las solicitudes, aunque no son pocas las compañías que también hacen constar su dirección postal como medio alternativo.

Finalmente, junto con la información preceptiva, algunas compañías han incorporado un aviso acerca de la "*colocación de cookies* " en el ordenador del usuario, así como de su finalidad, tal y como prevé el artículo 4 del *Código Ético de Protección de Datos Personales en Internet* , de la AECE.

* *Respecto de la forma*

Generalmente, las webs analizadas incorporan la información a la que se refiere el artículo 5 de la LOPD como cláusulas adicionales a las condiciones generales que rigen la vinculación del vendedor con el comprador, aunque se ha observado que en algunos casos esa información se limita a una mera mención al hecho de que "*los datos que nos facilite serán protegidos de acuerdo a la Ley* ", de lo que no puede deducirse en ningún caso que los derechos del comprador estén convenientemente garantizados.

Por otra parte, en muchas ocasiones se ha observado que la información se sitúa dentro de la web en un lugar cuyo acceso no resulta evidente para el usuario.

2.2.1.4. Calidad de los datos

* *En relación con la finalidad*

En el texto informativo que figura en gran parte de las webs analizadas se reconoce que los datos que tratarán relativos a los clientes tienen la finalidad de perfeccionar la relación comercial con éstos, así como de adaptar la oferta a sus intereses. Sin embargo, ninguna de las compañías inspeccionadas ha reconocido que hasta el momento haya efectuado prácticas de segmentación de clientes a partir de los datos recabados de éstos.

La totalidad de las compañías inspeccionadas han reconocido que almacenan "*cookies* " en los ordenadores de los usuarios que se conectan a sus webs. En estos ficheros se almacena información que es tratada por cada compañía con la finalidad de personalizar los subsiguientes accesos a su web. La tipología de esta información difiere en cada caso, aunque suele ser muy básica: un identificador de conexión, fecha y alguna referencia a los productos que se incorporan al "*carrito (o cesta) virtual* " pero que finalmente no se solicitan a la tienda. De esta forma, cuando un usuario se conecta se descargan sobre su "*carrito* " todos los productos que no adquirió en su última conexión a la web. Como ya se ha mencionado, algunas de estas compañías han incorporado en su web un aviso para el usuario acerca de la colocación de estas " *cookies* ".

Por otra parte, la propia tecnología de Internet permite que los servidores en los que se alojan las webs almacenen voluminosos ficheros denominados "*log de visitas* ", en los que se deja constancia de las visitas que diariamente recibe cada web. La información contenida en estos ficheros no recoge datos identificables y se identifica por la dirección IP que le ha asignado dinámicamente al usuario su propio proveedor de servicios de acceso (PSI), siendo éste el único que podría averiguar la identidad del usuario a través de esa dirección. Estos ficheros son generalmente tratados de forma estadística, con objeto de conocer el número de visitas periódicas recibidas o la distribución de éstas en función de las franjas horarias.

Es evidente que los usuarios que se han registrado en una determinada tienda y que se identifican al conectarse (suministrando el identificador que se les asignó en el momento de registrarse) son perfectamente reconocibles por la tienda. No ocurre así con los usuarios que simplemente visitan las páginas de la web sin identificarse. Sin embargo, cabe señalar que el anonimato de las visitas podría perderse sobre todo en aquellos casos en los que la web se aloja precisamente en los servidores del PSI del usuario, dado que entonces sí sería posible averiguar qué usuario concreto tenía asignada una determinada dirección IP en un determinado momento (cruzando el fichero "*log de visitas*" con el fichero "*log de accesos* "). Esta dualidad tiene lugar precisamente en las compañías que, aparte de comercializar productos, ofrecen (generalmente de forma gratuita) los servicios de acceso a Internet. Precisamente, dos de las entidades inspeccionadas disponen de portales generalistas que ofrecen ambos tipos de servicios, aunque en ninguno de los casos se ha detectado que lleven a cabo esa práctica. En cualquier caso, la mayor parte de las compañías inspeccionadas también ha declarado que no conserva los ficheros de log durante más de un mes.

Por otra parte, es práctica común de las tiendas virtuales el envío periódico de comunicaciones comerciales a sus usuarios registrados, informándoles de novedades y otros asuntos de interés. Estos envíos se dirigen generalmente al buzón electrónico del usuario, quien debería poder ejercer su derecho de oposición al tratamiento de sus datos con esa finalidad. En este sentido, algunas han habilitado esta opción en el formulario de registro y también a través de cada uno de sus mensajes, donde sugieren al destinatario no interesado que devuelva el mensaje concretando su deseo en el campo "*Asunto* ".

* *En relación con la cancelación*

Aunque la creación de la mayor parte de las webs data de hace unos pocos meses, se ha observado que casi todas las inspeccionadas cuentan con procedimientos específicos para la cancelación de los datos personales de los compradores, cuando han dejado de ser necesarios o pertinentes para la gestión.

Sin embargo, algunas de estas compañías han manifestado que siguen conservando los datos con objeto de acreditar documentalmente el vínculo con sus clientes y así poder atender las responsabilidades nacidas del tratamiento (tributarias, entre otras), durante el plazo de prescripción de éstas.

Finalmente, es preciso señalar que en algunos casos se ha observado que la cancelación de datos no es real, es decir, no produce el borrado físico, sino que se materializa mediante una marca lógica que permite evitar el tratamiento de los datos aunque éstos sigan estando disponibles.

2.2.1.5. Datos especialmente protegidos

A través de ninguna de las webs analizadas se recaban del ciudadano datos de los que protege el artículo 7 de la LOPD (ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, comisión de infracciones penales o administrativas). Sin embargo, como ya se ha comentado, es evidente que aunque el ciudadano no declare estas circunstancias acerca de sí mismo, sí es posible presumir (aunque sea erróneamente) algunas de ellas en función de su comportamiento como comprador. La gama de especialidades es amplia, pues algunas de estas webs están organizadas de acuerdo a las preferencias del visitante. En el caso de las sex-shops, por ejemplo, los productos eróti-

cos aparecen en ocasiones clasificados de la siguiente forma: zoofilia, gay, bisexual, transexual, "*sadomaso*", jovencitas, A nadie se le escapa la categorización que podría realizarse de los clientes a partir de su historial de compras, que consta en los ficheros de estas compañías.

Resulta claro que en estos casos el vendedor no recaba del comprador información acerca de sus preferencias sexuales, sino que se limita a dejar constancia en sus ficheros de los productos que el comprador ha solicitado, los cuales pueden ser marcadamente orientativos de unos determinados gustos sexuales, aunque éstos no tengan por qué corresponder necesariamente al comprador. En este sentido, lo que habría que analizar es si el mero hecho de comprar un determinado producto (catalogado de acuerdo a unas determinadas preferencias sexuales) es indicativo o no de la vida sexual del comprador en los términos que la Ley establece.

Las sex-shops son las entidades que menos información facilitan al usuario acerca del tratamiento de datos relativos a su persona: ninguna de las cuatro webs analizadas informa de lo especificado en el artículo 5 de la LOPD, ni tampoco se deduce que el usuario haya consentido expresamente en su tratamiento. Lo mismo puede decirse de la web analizada que comercializa productos ortopédicos. También cabe destacar que uno de los fallos de seguridad más flagrantes que la Inspección ha detectado ha tenido lugar precisamente en una de estas webs, habiéndose verificado que los datos de algunos compradores eran fácilmente visualizables desde Internet en determinadas condiciones, circunstancia que fue achacada por los responsables de la web a un error de programación y que, no obstante, ha sido subsanada con posterioridad a la realización de la inspección.

2.2.1.6. Datos sobre menores de edad

Considerando las especiales características del mundo Internet, es preciso prestar una atención particular a ciertos sujetos merecedores de una mayor protección: aquellos que aún no han adquirido la mayoría de edad y que, por lo tanto, están menos preparados para hacer frente a las prácticas abusivas que se llevan a cabo a través de este canal, tan atractivo para ese público.

Se ha podido comprobar que algunas de las webs analizadas solicitan a través de sus formularios la fecha de nacimiento del usuario, con objeto de rechazar al menos todos aquellos pedidos que provengan de interesados que se han reconocido menores de edad. Evidentemente, a través de Internet resulta imposible determinar los casos en los que el usuario se atribuye una edad distinta a la real, pero de esta manera el vendedor puede acreditar su voluntad de no establecer relaciones comerciales con menores, especialmente cuando la legislación prohibe la venta de determinados productos, orientados exclusivamente al público adulto.

En este sentido, a falta de una regulación específica, cabe considerar lo expuesto en el capítulo III (Tratamiento de datos sobre los menores) del Código Ético de la AECE, que en su artículo 13 propone: "*En ningún caso podrán recabarse del menor de edad datos relativos o relacionados con la situación económica o la intimidad de los otros miembros de la familia".* Así mismo, el artículo 16 establece que "*además del respeto a la opción de los padres de limitar la recopilación de estos datos on-line, las empresas anunciantes deberán limitar la utilización de datos proporcionados por los menores a la única finalidad de la promoción, venta y suministro de sus productos y servicios dirigidos a menores* " y que "*en ningún caso podrán cederse los datos relativos a menores, ni utilizarse para campañas que sean inadecuadas para la edad correspondiente al menor* ".

2.2.1.7. Acceso a los datos por cuenta de terceros

Como ya se ha comentado antes, son muchos los agentes que intervienen en el negocio electrónico. Las compañías generalmente restringen su actividad a las tareas puramente comerciales, encargando a otras compañías más especializadas tareas como la atención telefónica, las operaciones logísticas o los servicios informáticos.

En este último caso, además existe una amplia gama de modalidades, que incluyen: colocación y almacenamiento de equipos (generalmente, propiedad de la organización que encarga los servicios), conexión de los equipos a Internet, asistencia técnica, colaboración en la resolución de averías y otras tareas de mantenimiento. Al conjunto de estos servicios se le suele denominar "*housing* ". Cuando el servicio prestado supone exclusivamente la administración de los servidores se le denomina "*hosting* ". En ambos casos, aunque de diferente forma, el personal que presta los servicios suele tener acceso a los ficheros de la compañía, pues tanto para unas tareas como para las otras se requiere un perfil de usuario con privilegios generalmente reservados al administrador de la máquina.

También se han encontrado varios casos en los que los servicios de "*hosting* " o "*housing* " se prestan por compañías establecidas en otros países del mundo. En muchas ocasiones las condiciones aplicables a la prestación del servicio se recogen en un documento-tipo, que utiliza habitualmente el prestador y cuya redacción no se ha adaptado en absoluto a la legislación española.

Otro de los intervinientes en la transacción comercial a través de Internet es la entidad financiera que actúa como "*pasarela de pago* ". La participación de estas entidades es frecuente, fundamentalmente en webs que son propiedad de grandes compañías y que ofrecen a sus clientes el pago on-line de los productos o servicios solicitados. Para ello, en el momento de efectuar la compra se requieren los datos identificativos de la tarjeta de crédito/débito (número y fecha de caducidad, sin identificar al comprador), datos éstos que en la mayor parte de los casos son remitidos directamente a los servidores de la entidad financiera, quien se encarga de aceptar o rechazar la transacción tras consultar telemáticamente al correspondiente centro autorizador. Sin embargo, algunas de las compañías inspeccionadas han reconocido que, aparte de remitir los datos a la entidad financiera, conservan en sus ficheros tales datos con objeto de poder acreditar en el futuro la transacción realizada.

2.2.1.8. Comunicación de datos

Muchas de las compañías inspeccionadas han manifestado su pertenencia a grandes grupos empresariales cuya actividad se ha diversificado en muy diferentes ámbitos. Como es habitual en otros sectores, las compañías que desarrollan su actividad a través de Internet también han considerado los beneficios de compartir su cartera de clientes con las demás empresas de su grupo, por lo que en su propia web incluyen cláusulas informativas con las que pretenden cubrir el requisito legal del previo consentimiento del interesado. Las fórmulas utilizadas suelen consistir en una referencia a la "*posible cesión de datos a otras empresas del grupo* ", en orden a que tales datos sean utilizados con la finalidad de remitir "*informaciones comerciales de su interés*". Sin embargo, es precisamente la diversidad de actividades que pueden coincidir en un mismo grupo lo que puede introducir un elemento de inseguridad de cara al ciudadano, especialmente en casos en los que el grupo está formado por un número de compañías que puede llegar a 200. Es evidente, además, que en esos casos el grupo empresarial puede llegar a manejar una información muy completa acerca de los hábitos de las personas con las que las compañías participadas han establecido una relación comercial, una circunstancia esta de la que quizá no sean del todo conscientes los clientes.

Por otra parte, se ha tenido conocimiento de situaciones en las que una determinada compañía perteneciente a cierto grupo empresarial ha sido adquirida por otro grupo, de manera tal que todos sus activos (incluida la cartera de clientes) han pasado a formar parte de éste. La trascendencia de cara a los clientes es grande pues los datos que iban a ser compartidos con ciertas compañías (según se les informó en la recogida) pasan a ser compartidos con otras compañías distintas, sin que el cliente haya podido decidir acerca de esta circunstancia.

En otras ocasiones, se han detectado cambios en la titularidad de ciertos servicios prestados a través de Internet (por ejemplo, el acceso gratuito o el correo electrónico), que han supuesto el consiguiente cambio respecto a la responsabilidad del fichero en el que se almacenan los datos de las personas a las que se presta el servicio.

El ejemplo que a continuación se presenta pone de manifiesto hasta qué punto se difuminan los límites en la actuación de las diferentes compañías integrantes de un grupo empresarial. Se ha detectado el caso de un determinado grupo del sector eléctrico, cuyo interés en promocionar la web gestionada por una de sus compañías le ha llevado a ofrecer importantes descuentos a los clientes de la empresa matriz, cuando éstos adquieren determinados servicios de otra entidad ajena al grupo (una agencia de viajes), con la única condición de identificarse como tales. La consecuencia más relevante de esta iniciativa es que la compañía titular de la web acaba recibiendo información detallada acerca de las condiciones en que se ha contratado el paquete de viajes, incluyendo los datos personales del contratante, cuando es posible que éste ni siquiera sea cliente de esa compañía.

2.2.1.9. Movimiento internacional de datos

Al hilo de lo expuesto en el apartado anterior, son también especialmente significativos los casos de compañías multinacionales que disponen de establecimientos comerciales en diversos países del mundo, incluido España. Generalmente se trata de webs cuyo diseño se ha adaptado a las singularidades nacionales y cuya infraestructura común ha favorecido una gestión centralizada, con el consiguiente ahorro de recursos, tanto humanos como materiales. Este modelo de organización tiene, sin embargo, una repercusión clara en lo relativo a la protección de los datos de los clientes, en función precisamente de las garantías que cada país ofrece. Particularizando en el caso español, se da la circunstancia de que, por ejemplo, así como datos de clientes extranjeros son accesibles desde la filial española, de la misma manera datos de clientes españoles son accesibles desde los establecimientos de las filiales extranjeras, sin que quepa suponer que aquellos países estén ofreciendo a los ciudadanos las mismas garantías que ofrece la legislación española.

Por otra parte, como también se ha mencionado antes, algunas compañías han optado por encargar los servicios informáticos a otras entidades especializadas que en ocasiones se han establecido en países extranjeros, algunos de los cuales no son Estados miembros de la Unión Europea o no son Estados respecto de los cuales la Comisión de las Comunidades Europeas, en ejercicio de sus competencias, haya declarado que garantizan un nivel de protección adecuado.

Algunas de las compañías afectadas han optado por acogerse a la excepción prevista en el apartado e) del citado artículo 34 de la LOPD: que "*el afectado haya dado su consentimiento inequívoco a la transferencia prevista* ". Así, han incluido entre las cláusulas informativas (que el interesado debe conocer al iniciar su relación comercial con la tienda) un texto, de cuya lectura se desprende que los datos facilitados por el comprador serán almacenados en un fichero ubicado en el país en cuestión.

2.2.1.10. Ejercicio de los derechos de acceso, rectificación, oposición y cancelación

La mayor parte de las compañías han establecido distintas vías para facilitar al ciudadano el ejercicio de los derechos que la Ley le reconoce. Dado que la propia naturaleza de Internet permite una interrelación fácil y rápida entre comprador y vendedor, generalmente se ha utilizado la vía del correo electrónico como fundamental tanto para canalizar las solicitudes de acceso, rectificación, oposición y cancelación, como para remitir las consiguientes contestaciones por parte del responsable del fichero.

Así mismo, muchas de las compañías han habilitado una zona especial en la web que permite al usuario consultar fácilmente los datos que constan en su fichero (incluido el seguimiento de los pedidos realizados), para lo que se requiere que previamente el usuario se identifique y que se autentique su identidad a través de la contraseña que eligió

en el momento de registrarse. Esta vía facilita considerablemente al usuario el ejercicio de su derecho de acceso e introduce un mayor nivel de transparencia por parte del responsable del fichero.

Aparte de Internet, se ha podido verificar que habitualmente las compañías también ofrecen las vías más clásicas de interrelación entre vendedor y comprador, es decir, la comunicación telefónica (por lo general, un servicio de atención específico) y la comunicación postal (en muchas ocasiones, un apartado de correos).

2.2.1.11. Seguridad de los datos

Tras la entrada en vigor del *Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal* , aprobado mediante Real Decreto 994/1999, de 11 de junio, siguen existiendo entidades que aún no han elaborado e implantado su propia normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. La Inspección ha podido comprobar que dos de las compañías inspeccionadas no disponían del Documento de Seguridad al que se hace referencia en el citado Reglamento.

En general, puede decirse que los ficheros analizados presentan una estructura de datos tal que, en aplicación del artículo 4 del Reglamento, cabría exigir la adopción de las medidas de seguridad calificadas como de nivel básico, dado que los datos son puramente identificativos o estrictamente relativos a la relación comercial entre vendedor y comprador. No obstante, es preciso considerar dos excepciones. La primera, se refiere a los ficheros que contienen datos relativos al historial de compra de determinados productos, de cuyo conocimiento podrían desprenderse valoraciones acerca de la vida sexual de los compradores. En segundo lugar, figuran los ficheros que contienen un conjunto de datos suficientes que permiten obtener una evaluación de la personalidad del individuo.

En otro orden de cosas, ya se ha mencionado que sólo la mitad de las webs analizadas establecen un "*canal seguro* " para salvaguardar la confidencialidad en el envío de datos personales, fundamentalmente cuando entre ellos figura la identificación de la tarjeta de pago. Sin embargo, ni siquiera las webs que cifran la información están a salvo de accesos no autorizados a los datos, dado que se ha detectado que en algunos casos se utilizan vías no seguras para la confirmación al usuario de sus propios datos de registro (incluida su contraseña de acceso) o de los datos asociados a su pedido. Son los casos en los que esta información se remite por correo electrónico, no aplicándose en ningún caso procedimientos adicionales de cifrado, de forma tal que esos mensajes podrían ser captados y leídos por personas suficientemente expertas, vulnerándose así la confidencialidad de los datos que contienen.

Este mismo procedimiento implica precisamente la consideración de los clientes como usuarios con acceso al fichero de clientes, aunque con la salvedad de que dicho acceso está restringido a sus propios datos. Esta consideración hace que sea aplicable lo establecido por el artículo 11 del Reglamento, relativo a los procedimientos de identificación y autenticación. En este sentido, una de las carencias más notables que se han encontrado es el almacenamiento no ininteligible de las contraseñas, lo que supone que cualquier persona con acceso al fichero en el que se almacenan pueda suplantar la identidad de los usuarios. Por otra parte, no hay que desdeñar el hecho de que muchos internautas emplean una misma contraseña para conectarse a múltiples sistemas, de tal forma que una vez conocida esa clave podría abrirse la puerta de todos los sistemas en los que el usuario se hubiera registrado con idéntica clave.

También se ha detectado que algunas compañías utilizan las "*cookies* " como método de autenticación de usuarios, permitiendo a éstos ciertas funcionalidades de la web (entre ellas el acceso a sus datos) por el solo hecho de haberse registrado previamente en la web. De esta forma, en el ordenador del usuario se guarda constancia del identificador que se le asigna en el momento del registro, siendo este nombre reconocido por el servidor al conectarse nuevamente el usuario a la web, sin requerírsele su contraseña como medio para autenticar su identidad. El resultado es especialmente trascendental en aquellos casos en los que el ordenador desde el que se accede es utilizado por varias personas (por ejemplo, en cibercafés), dado que se permitiría a un usuario acceder a los datos personales de otro usuario previamente registrado en la misma web.

Respecto de las medidas concretas previstas en el Reglamento, una de las que, hasta el momento, han demostrado menos implantación es la que emana de su artículo 10, relativa a la necesidad de que exista un registro para el soporte del procedimiento de notificación y gestión de incidencias. Se ha podido comprobar que este registro existe muy pocas veces y en algunos de estos casos ni siquiera se utiliza de forma habitual.

Otra carencia significativa es la que se ha observado con respecto al requisito legal de que en el contrato de prestación de servicios se estipulen las medidas de seguridad que el encargado del tratamiento está obligado a implementar. Son muy pocas las compañías que incluyen estas estipulaciones.

2.2.1.12. Notificación e inscripción registral de los ficheros

Como se ha mencionado antes, en más de un tercio de las webs analizadas (desde las que se recaban datos personales, en su práctica totalidad) no se cumple con lo establecido en el artículo 26 de la LOPD, dado que no se ha obtenido constancia de que sus responsables hayan notificado a la Agencia algún fichero para su inscripción en el Registro General de Protección de Datos.

Por otra parte, en algunas ocasiones los ficheros inscritos son ficheros genéricos de clientes y de la información que figura inscrita no se deduce que contengan también los datos que se recaban a través de Internet, puesto que no se ha hecho constar un procedimiento telemático de recogida o una finalidad compatible con el comercio electrónico, quizá porque en el momento de notificarse a la Agencia aún no hubiesen adoptado esta modalidad de negocio. De ello se

deduce la necesidad de que los responsables de los ficheros modifiquen convenientemente la inscripción de sus ficheros o bien notifiquen la creación de nuevos ficheros, según los procedimientos establecidos en el Registro General de Protección de Datos.

Así mismo, en algunos casos se ha detectado que en la inscripción del fichero no se ha hecho constar una ubicación que se corresponda con la realidad, especialmente cuando las labores de tratamiento habían sido encargadas a otra compañía, cuya identificación y localización ni siquiera figuran en la inscripción, lo que es aún más significativo en los casos en los que esta última compañía se ha establecido en algún país extranjero.

2.2.2. Proveedores de Servicios de Acceso a Internet

Entre los meses de septiembre de 1999 y febrero de 2000, la Subdirección General de Inspección de Datos realizó actuaciones de inspección sobre diversas entidades que prestan a sus clientes servicios de acceso a Internet. Estas actuaciones se inscribían dentro del Proyecto de Colaboración organizado por la Agencia de Protección de Datos junto con el Registratiekamer holandés, con la participación de otras Autoridades europeas de protección de datos, con el cual se pretendía armonizar el modo de actuar de los distintos departamentos de Inspección a nivel europeo.

A continuación, se exponen brevemente algunas de las conclusiones obtenidas a partir de las inspecciones realizadas en tres entidades establecidas en nuestro país.

2.2.2.1. Perfil de las entidades inspeccionadas

La primera entidad, integrada en un grupo británico de telecomunicaciones, presta servicios de acceso a Internet (que incluyen correo electrónico y hospedaje de páginas personales), por los que cobra periódicamente a sus clientes una cuota de conexión. Por otra parte, a través de una compañía del mismo grupo empresarial ofrece al público en general servicios de comercio electrónico (concretamente, la comercialización de productos musicales). Así mismo, dispone de un portal generalista.

La segunda compañía, que centra su actividad en el negocio bancario, ofrece gratuitamente a sus clientes los servicios de acceso a Internet (que incluyen correo electrónico). Así mismo, ofrece a sus propios clientes la posibilidad de realizar operaciones bancarias y bursátiles a través de su web. Por otra parte, también dispone en Internet de una plataforma a través de la que se comercializan productos de diversos establecimientos.

La tercera de las compañías inspeccionadas desarrolla su negocio en el sector de las telecomunicaciones, particularmente por su condición de operador de telefonía. Por otra parte, ofrece al público en general los servicios de acceso a Internet (que incluyen correo electrónico y hospedaje de páginas personales) en dos modalidades: gratuita o mediante el abono de un importe fijo que permite al usuario conectarse por un número máximo de horas al mes (evitándose en este caso el pago de las llamadas al correspondiente operador local de telefonía). Así mismo, dispone de un portal generalista y en el pasado ofreció servicios de comercio electrónico (concretamente la comercialización de una tarjeta virtual de prepago de la propia compañía), aunque en la actualidad ha abandonado el proyecto.

2.2.2.2. Calidad de los datos

Las tres entidades inspeccionadas han reconocido que periódicamente remiten mensajes electrónicos a sus clientes con objeto de informarles acerca de las novedades e incidencias relacionadas con la prestación del servicio. Por otra parte, la compañía de telecomunicaciones está desarrollando en la actualidad un proyecto mediante el que se pretende constituir un "*datawarehouse* " que permitirá explotar conjuntamente toda la información generada por la prestación de los diferentes servicios ofrecidos, incluida la de tráfico y facturación.

Las tres entidades inspeccionadas almacenan referencias (que incluyen el número de teléfono desde el que se realiza la conexión) de cada uno de los accesos que los usuarios (clientes propios) realizan a sus servidores. Los datos registrados diariamente en los ficheros de "*log*" de acceso (que incluyen: identificador de usuario, dirección IP, fecha y hora de conexión y desconexión, y número de teléfono llamante) son utilizados para solucionar incidencias técnicas planteadas por los usuarios, atender los requerimientos planteados por los órganos judiciales, prevenir el fraude y, en el caso de la tercera compañía inspeccionada, facturar a los clientes. Por otra parte, todas las compañías visitadas tratan esta información, una vez disociada, con fines estadísticos.

Respecto del correo electrónico, las dos primeras entidades utilizan un protocolo (POP 3) que permite al usuario decidir acerca del momento en que desea eliminar el contenido de su buzón, aunque por defecto los mensajes son eliminados del servidor cuando el destinatario los "*baja* " a su propio ordenador. Los servidores de esas compañías registran también en un fichero de "*log* " referencias a cada uno de los mensajes recibidos por sus clientes. Estas referencias son incluso conservadas en soporte óptico por una de las citadas compañías. En cuanto a la tercera compañía, que emplea un protocolo de correo diferente, también permite que sea el propio usuario el que decida cuándo vaciar su buzón.

Las tres entidades también registran diariamente información relativa a las visitas realizadas por el público en general a sus propios sitios en Internet (incluyendo, además, los portales que dos de ellas tienen disponibles). Estos datos permiten conocer la dirección IP asignada al internauta que visita en cada momento la página correspondiente. Durante las inspecciones realizadas se ha comprobado que cada compañía puede identificar a los visitantes de sus páginas en el caso de que la dirección IP utilizada pertenezca al rango de direcciones que la compañía tiene asignado como proveedor de servicios de acceso. Para ello, basta con cruzar esta información (dirección IP, fecha y hora de visita) con la que figura en el correspondiente " *log* " de accesos.

La política de conservación de datos de las tres compañías inspeccionadas consiste en mantener la información precisa para la gestión del servicio durante el tiempo máximo que fija la legislación aplicable. En relación con la información sobre los accesos a Internet de sus propios clientes, que los servidores registran en los correspondientes "*log* ", dos de las tres compañías inspeccionadas no han borrado hasta el momento la información registrada desde el comienzo de sus actividades. Respecto de la información registrada en los "*log* " de visitas, tan sólo una de las compañías ha declarado que la conserva después de procesarla estadísticamente.

Las tres compañías comercializan o han comercializado productos a través de Internet, por lo que también disponen de ficheros con datos acerca de los compradores, quienes los han facilitado por la red a través de un formulario en el momento de realizar la solicitud. No se han hallado evidencias de que tales datos hayan sido utilizados para otras finalidades distintas a la que emana de la propia relación comercial, a pesar de que en algún caso se ha comunicado al comprador la posible utilización de sus datos para la promoción comercial.

2.2.2.3. Derecho de información en la recogida

A través de sus respectivas páginas web, las tres compañías proporcionan información acerca de la incorporación a sus ficheros de los datos de los clientes y otras personas que voluntariamente facilitan sus datos (por ejemplo, los visitantes de los portales), así como de la posibilidad que todos ellos tienen de ejercer sus derechos de acceso, rectificación y cancelación.

Se ha comprobado también que las últimas entidades inspeccionadas han actualizado sus cláusulas informativas con ocasión de la entrada en vigor de la LOPD.

2.2.2.4. Consentimiento del afectado

En general, puede entenderse que al solicitar los servicios de Internet prestados por alguna de las tres compañías el interesado manifiesta su interés en establecer una relación comercial con ésta, para cuyo desarrollo es preciso conocer los datos identificativos del futuro usuario.

La primera de las compañías incluye en su cláusula informativa la fórmula "*consentimiento expreso* " para el tratamiento automatizado de los datos tanto de sus clientes como de los visitantes de su portal, de tal forma que la aceptación de la citada cláusula supondría una manifestación explícita acerca de la voluntad positiva del interesado.

En el caso de la entidad bancaria inspeccionada existe una relación adicional con el cliente, la cual también implica necesariamente el tratamiento automatizado de sus datos personales, que en ocasiones (como ocurre con las transacciones bancarias y bursátiles) se produce incluso simultáneamente. El banco *informa* de que, como consecuencia de la contratación de cualquier producto o servicio, todos los datos facilitados serán objeto de incorporación a los ficheros automatizados existentes en el banco. Así mismo, se incluye una cláusula por la que "*el cliente acepta que el banco o sus sociedades filiales y participadas, le remitan información sobre cualesquiera bienes o servicios que comercialicen directa o indirectamente o que en el futuro puedan comercializar".*

Finalmente, en el caso de la compañía de telecomunicaciones, junto a la cláusula informativa se incluye otra según la cual "*el cliente autoriza, de conformidad con la normativa vigente, al tratamiento de sus datos de tráfico y facturación para fines de promociones comerciales propias* ". También se informa de que "*cualquier otra utilización de los datos de carácter personal contenidos en el fichero, requerirá el previo y expreso consentimiento del cliente* ". La información facilitada es idéntica para los visitantes del portal del que es responsable la compañía.

2.2.2.5. Datos especialmente protegidos

No se han encontrado evidencias de que ninguna de las entidades inspeccionadas traten datos especialmente protegidos.

2.2.2.6. Seguridad de los datos

En el período de tiempo en el que se realizaron las inspecciones las tres compañías se hallaban en proceso de adaptación a los requisitos establecidos por el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado mediante el real decreto 994/1999, de 11 de junio.

2.2.2.7. Cesión de datos

Las tres entidades han coincidido al declarar que no han cedido a ninguna otra compañía los datos personales de sus clientes o de los visitantes que se han registrado voluntariamente a través de sus portales. Sin embargo, las tres entidades han previsto una cláusula contractual en la que informan de que los datos facilitados serán compartidos con fines comerciales por otras compañías de sus respectivos grupos empresariales o incluso por otras sociedades con las que se concluyan acuerdos de colaboración (por ejemplo, los canales de distribuidores y agentes).

Respecto de los visitantes del portal, junto a la cláusula informativa de la primera compañía se incluye una autorización a la misma *o a empresas del grupo* para que los datos facilitados sean utilizados por éstas con la finalidad de prestar el servicio, así como para el envío de información relacionada con los contenidos y servicios ofrecidos en su portal.

En cuanto a los visitantes del otro portal, la compañía de telecomunicaciones utiliza las mismas cláusulas informativas que para los clientes a los que presta servicios de acceso, por lo que también se prevé la posible cesión de datos a otras empresas del grupo.

2.2.2.8. Derechos de las personas

Las tres compañías facilitan el ejercicio de los derechos de acceso, rectificación y cancelación a través del servicio de atención telefónica. También es habitual la recepción de mensajes electrónicos solicitando la cancelación de datos o desautorizando el uso comercial de éstos.

En general, las compañías disponen de normas escritas para la tramitación de las solicitudes de ejercicio de los derechos de acceso, rectificación y cancelación.

Por otra parte, es reseñable que las personas que se han registrado en uno de los portales pueden acceder y rectificar sus datos de forma directa a través del portal. 2.2.3. Gestión de tarjetas en Grandes Superficies Comerciales

En el año 2000 la Agencia de Protección de Datos inició un Plan de Oficio con el objeto de determinar los procedimientos y tratamientos que aplican las grandes superficies comerciales sobre los datos de sus clientes, en relación con las tarjetas de pago y fidelización que emiten, así como en la utilización como medio de pago de otras tarjetas externas, verificando su adecuación a lo dispuesto en la LOPD.

Se seleccionaron para ser inspeccionados algunos de los centros comerciales más representativos, tanto por volumen de ventas como por su implantación a nivel nacional. También fueron inspeccionados los establecimientos financieros de crédito emisores de las tarjetas financieras de cada centro comercial.

Durante la inspección se verificó la existencia de los tres tipos de ficheros siguientes:

* *Ficheros de Tarjetas de pago de grandes superficies comerciales*: Contienen los datos de los solicitantes y titulares de tarjetas emitidas por los establecimientos financieros de crédito bajo la marca del centro comercial correspondiente, con las cuales se pueden abonar las compras y solicitar financiación de las mismas en cada uno de los centros comerciales inspeccionados.
* *Ficheros de otras Tarjetas de pago* : Contienen los datos derivados o relacionados con las operaciones que efectúen los clientes utilizando otras tarjetas distintas de las anteriores, emitidas por entidades financieras y que permiten comprar y pagar con ellas en la generalidad de los establecimientos.
* *Ficheros de fidelización de clientes* : Contienen los datos de aquellos clientes que son socios de los Clubes de fidelización promovidos por los propios centros comerciales.

A continuación se exponen las principales conclusiones de la inspección para cada una de estas tres clase de ficheros.

2.2.3.1. Ficheros de Tarjetas de pago de grandes superficies comerciales

* Relación contractual establecida con los establecimientos financieros de crédito

Cada una de las grandes superficies comerciales tiene establecida una relación contractual con los correspondientes establecimientos financieros de crédito en forma de acuerdos de adhesión al sistema de pago de la tarjeta, de manera que dichas tarjetas sean admitidas como medio de pago en todos sus centros, pudiendo también solicitar los clientes financiación sobre las compras que realicen.

* Ficheros automatizados e inscripción registral

Los datos de las solicitudes de tarjetas y de los titulares de las mismas se recogen en ficheros automatizados, los cuales se encuentran inscritos en el Registro General de Protección de Datos. Los responsables de estos ficheros son los establecimientos financieros de crédito como entidades emisoras de estas tarjetas.

* Recogida de los datos de solicitud de Tarjetas

Los datos son recogidos habitualmente a través de formularios de solicitud que cumplimenta directamente el propio interesado o el personal del centro comercial, debiendo ser suscritos con su firma por el interesado para que tengan validez. Entre los datos recabados se encuentran los siguientes:

* Identificativos y de domicilio: Número de DNI, nombre y apellidos, fecha de nacimiento, sexo, nacionalidad, domicilio y número de teléfono.
* Situación familiar: estado civil, número de hijos o personas a su cargo, régimen económico del matrimonio.
* Profesionales: nombre de la empresa, domicilio, cargo, número de teléfono, antigüedad en el puesto y situación (fijo, eventual o pensionista).
* Económicos: Ingresos mensuales, situación de la vivienda habitual (en alquiler, en propiedad, con padres, en hotel), otros ingresos y datos bancarios.

Algunas entidades también solicitan documentación acreditativa de la situación económica del interesado, como su última nómina y el documento que acredite el mantenimiento de una cuenta bancaria en la que domiciliará los pagos de los recibos.

* Derecho de información y consentimiento de los afectados

En los formularios de solicitud y contratos de Tarjeta se informa de la inclusión de los datos personales aportados por el afectado y otros que en el futuro pueda aportar, en un fichero automatizado cuyo responsable es el establecimiento financiero, así como de la inclusión en un fichero cuyo responsable es el centro comercial, si éste no pertenece al grupo de empresas del establecimiento financiero. También se informa de la finalidad de la recogida de los datos (gestión y registro de las operaciones que el Titular efectúe, así como la valoración del riesgo de las operaciones solicitadas) y de la obligación de facilitar los datos solicitados, en cuanto a que son necesarios para la valoración del riesgo y para el mantenimiento y efectividad de la relación contractual que se establece.

* Igualmente, se informa sobre la posibilidad del ejercicio de los derechos de acceso, rectificación y cancelación, comunicando las direcciones de los responsables de los ficheros ante los que pueden ejercitarse tales derechos.
* Tratamientos de datos

Los datos aportados por los clientes son sometidos a los siguientes tratamientos: Estudio de las solicitudes de emisión de tarjeta

Las solicitudes de tarjeta son analizadas por los propios establecimientos financieros, los cuales siempre disponen de sistemas automáticos (ya sean de scoring o sistemas expertos) que proceden a evaluar el riesgo de la situación crediticia del interesado. El resultado final del análisis se concreta en una decisión acerca de la solicitud, aprobando o denegando la misma. Esta decisión es, en algunos casos, revisada por una persona y, en otras, el resultado de la denegación por el sistema automático supone directamente la no concesión de la tarjeta.

Los establecimientos financieros tienen en cuenta para autorizar la concesión de la tarjeta la posible inclusión de los datos personales del interesado en ficheros externos de solvencia patrimonial, así como el hecho de que conste en sus ficheros automatizados algún impagado derivado de relaciones comerciales que haya mantenido anteriormente con ellos.

Diseño de la tarjeta

Las tarjetas emitidas por las entidades financieras cumplen con las especificaciones recogidas en estándares ISO. Entre los datos que se recogen grabados en el anverso de la misma figuran: código identificativo de la entidad emisora, número de tarjeta y apellidos y nombre del titular. En la banda magnética existente en el reverso se almacena, entre otra, la siguiente información: número de cuenta, apellidos e inicial del nombre y fecha de caducidad.

Pagos realizados con la tarjeta

Para abonar las compras que realice en los centros comerciales el cliente debe aportar su tarjeta, procediéndose a la lectura de la banda magnética a través de los terminales punto de venta y capturándose la información necesaria para proceder a la autorización de la operación y para la impresión del ticket de compra.

Con el fin de aprobar la operación, el terminal punto de venta establece comunicación con los sistemas informáticos del establecimiento financiero correspondiente. Entre los datos enviados referidos al cliente sólo se encuentra su número de tarjeta.

Recibida la transacción en los sistemas informáticos del establecimiento financiero se procesa la misma y se procede a autorizar o denegar la operación, enviando la correspondiente respuesta al terminal punto de venta.

Envío de publicidad

Los establecimientos financieros incluyen habitualmente junto al extracto mensual de las operaciones realizadas información publicitaria de productos que se ofertan en los centros comerciales o en otras sociedades del Grupo al que pertenecen.

Asimismo, en algún caso se realizan estudios de hábitos de compra para el envío de publicidad a sectores determinados de clientes.

Gestión de impagados

Todas las gestiones realizadas por los establecimientos financieros para la recuperación de recibos devueltos o que son finalmente impagados, como pueden ser envío de cartas o conversaciones telefónicas mantenidos por los clientes, se recogen en sus ficheros automatizados. Alguna entidad mantiene dicha información en la historia del cliente incluso después de que la deuda haya sido regularizada.

* Comunicaciones de datos y transferencias internacionales

Los establecimientos financieros remiten al Banco de España para su inclusión en el fichero Central de Información de Riesgos, los datos de aquellos clientes que hayan realizado compras a crédito por importes superiores a un millón de pesetas. Asimismo la gran mayoría comunican los datos de sus impagados a ficheros de incumplimiento de obligaciones dinerarias.

También es habitual que las remesas de recibos y facturas que envían los establecimientos financieros a las entidades bancarias, para su cargo en la cuenta de los clientes, se remitan telemáticamente a través de entidades bancarias intermediarias, las cuales se encargan de remitirlos finalmente al banco donde el cliente ha domiciliado sus recibos.

Respecto de las transferencias internacionales ninguna entidad ha manifestado haber realizado alguna.

* Cancelación de solicitudes de tarjeta denegadas

Se ha verificado que los establecimientos financieros eliminan periódicamente de sus ficheros automatizados los datos de las solicitudes de tarjeta que resultaron denegadas, razón por la que el cliente no llegó a establecer ninguna relación comercial. No obstante, se comprobó que una entidad mantenía en sus ficheros automatizados información de un gran número de solicitudes que habían resultado denegadas hace ya varios años.

* Acceso a los datos por cuenta de terceros

La gran mayoría de los establecimientos financieros suelen establecer contratos y acuerdos de confidencialidad con otras empresas para la prestación de diferentes servicios, lo que supone la entrega de soportes conteniendo los datos personales de sus clientes. Entre los servicios prestados se han detectado los siguientes:

* Estampación de la Tarjeta
* Impresión, manipulación y envío de los extractos de cuenta y recibos mensuales, así como de la publicidad que remiten.
* Autorización de las operaciones efectuadas con Tarjeta
* Prestación de diversos servicios informáticos incluyendo la gestión diaria del propio fichero de clientes
* Revisión de las solicitudes de Tarjeta y estudio de autorización o denegación de las mismas.
* Atención telefónica incluyendo la gestión de recuperación de impagados.

En el caso de un establecimiento financiero, el contrato para la prestación de servicios de impresión de los extractos mensuales de la cuenta de tarjeta, así como su manipulación, ensobrado y puesta en Correos, había sido suscrito por la empresa matriz del Grupo al que pertenece, en vez de por ella misma.

Asimismo, es muy habitual que el personal de los centros comerciales tenga acceso a los ficheros de clientes de los establecimientos financieros, para poder realizar las gestiones que soliciten los clientes en sus lugares de compra habituales.

2.2.3.2. Ficheros de otras Tarjetas de pago

* Sistema informático

Los centros comerciales disponen de equipos servidores específicos conectados a los terminales punto de venta, en los cuales se consolidan los datos de las operaciones efectuadas por los clientes.

* Pagos realizados con tarjeta

El cliente para abonar las compras que realice en los centros comerciales debe aportar su tarjeta, procediéndose a la lectura de la banda magnética a través de los terminales punto de venta y capturándose la información necesaria para proceder a la autorización de la operación y para la impresión del ticket de compra.

* Autorización de la operación

El terminal punto de venta determina el tipo de Tarjeta y establece comunicación con su correspondiente centro autorizador. Entre los datos que se envían a dicho centro para la aprobación de la operación, siguiendo protocolos estándar (como puede ser PRICE), se encuentran: número de tarjeta, centro comercial donde se efectúa la compra, su importe y fecha y hora de realización, no enviándose otros datos de carácter personal como el nombre y apellidos del cliente.

En algunos casos los centros comerciales establecen comunicación a través de una entidad bancaria intermediaria, que es la encargada de establecer las comunicaciones oportunas para proceder la autorización de la operación.

Como respuesta a la transacción recibida del centro comercial, el centro autorizador analiza los datos de la operación y devuelve un resultado de aprobación o denegación de la misma.

* Ficheros automatizados

Los centros comerciales disponen de ficheros de Log de cajas y de movimientos de las operaciones que se efectúen utilizando tarjetas, en los cuales se recaban entre otros los siguientes datos: Número de tarjeta, fecha de caducidad, importe de la compra, entidad emisora de la tarjeta y departamento de venta; no recogiéndose ningún otro dato que permita identificar al titular de la tarjeta.

Por ello, las entidades consideran que estos ficheros no contienen datos de carácter personal al no poder identificar a su titular, ya que no disponen de ninguna otra información respecto del mismo, considerando también que no procede

la notificación de dichos ficheros al Registro General de Protección de Datos.

* Facturación/Consolidación de las operaciones

Los centros comerciales consolidan los datos de las operaciones efectuadas por sus clientes con la información de facturación remitida por las entidades bancarias. Éstas no suelen coincidir con la entidad bancaria en la que el cliente ha domiciliado los cargos realizados con la Tarjeta, sino que son otras, denominadas "bancos Merchant", que realizan labores de intermediación en la gestión del cobro de las operaciones, percibiendo una comisión por ello.

En una entidad se analizaron los ficheros resultantes de la conciliación y se comprobó que se almacenan los siguientes datos: fecha de operación, número de tarjeta, importe, compra/anulación, comisión y campo asociado, número de autorización y fecha de conciliación.

2.2.3.3. Ficheros de fidelización de clientes

* Ficheros automatizados e inscripción registral

Algunos centros comerciales son responsables de ficheros automatizados en los que se recogen los datos de sus clientes que pertenecen a sus propios Clubes de fidelización.

* Recogida de los datos, derecho de información y consentimiento de los afectados

Los datos de los socios son recabados por los centros comerciales a través de formularios específicos, que en algún caso son firmados por los propios interesados. Asimismo en dichos formularios figura que el interesado autoriza la automatización de sus datos personales y se le informa de aspectos tales como:

* Obligación de facilitar los datos contenidos en el formulario para convertirse en socio del Club.
* Comunicaciones de datos de los socios a otras empresas del Grupo y a otras que gestionan los servicios del Club.
* Posibilidad de ejercicio de los derechos que la Ley Orgánica 15/1999 reconoce a los afectados, ya sea por vía telefónica o por correo.
* Explotación de datos

Un centro comercial dispone de un datawarehouse en el que se almacenan los datos de sus socios y de las compras que éstos hayan realizado, detalladas por cada uno de los artículos adquiridos. Esta información se utiliza para realizar estudios de mercado y para campañas de promociones y lanzamiento de productos, obteniéndose los datos personales de aquellos socios entre los que se lanzará la promoción.

* Transferencias internacionales de datos

Los datos contenidos en estos ficheros no son objeto de transferencias internacionales.

* Acceso a los datos por cuenta de terceros

Los centros comerciales han establecido contratos y acuerdos de confidencialidad con empresas para la prestación de diferentes servicios, para lo cual hacen entrega de soportes conteniendo los datos personales de sus socios. Entre los servicios que se prestan se encuentran los siguientes:

* Impresión, manipulación y envío de información relacionada con los Clubes, así como de la publicidad que se remita.
* Mantenimiento del fichero (altas, actualizaciones).
* Atención telefónica a socios.

A continuación se presentan las conclusiones más relevantes de los aspectos que se han revisado en relación al cumplimiento del Reglamento de medidas de seguridad:

A excepción de un establecimiento financiero, todos ellos han considerado a los ficheros que recogen los datos relativos a la gestión de las Tarjetas que emiten como de nivel de seguridad medio.

Todas las entidades inspeccionadas disponen de uno o varios documentos en los que se recoge la normativa de seguridad y que en líneas generales recoge los aspectos que se exigen en el Reglamento, estando en unas entidades más detallado que en otras.

Así mismo, todas las entidades disponen de registros donde se recogen todas las incidencias que se producen, no sólo las específicas de seguridad, recabándose en general los datos que se detallan en el Reglamento.

El mecanismo que se utiliza en todos los sistemas, para asegurar la identificación y autenticación de los usuarios, es la asignación a éstos de un código y de una contraseña. No obstante, no existe una asignación personalizada de usuarios para el personal de los centros comerciales que tiene acceso a los ficheros de clientes de los establecimientos financieros, creándose usuarios genéricos u otorgándose permisos específicos de acceso en función de la ubicación del terminal desde el que se vaya a acceder.

En general todos los sistemas inspeccionados están diseñados para permitir a los usuarios el acceso a los datos del

fichero teniendo en cuenta las funciones que desempeñan.

El acceso a los locales donde se encuentran ubicados los equipos informáticos y los ficheros se encuentra restringido, ya sea utilizando medidas como el mantenimiento de una puerta cerrada bajo llave, hasta otras más sofisticadas como la implantación de un sistema de control de acceso biométrico mediante huella dactilar.

Todas las entidades tienen definidos procedimientos para la realización de copias de respaldo de los datos contenidos en sus ficheros, ya que mantienen un claro interés en preservar la disponibilidad de la información y contemplan la figura del responsable de seguridad. 2.2.4. Operadores de telefonía móvil.

Por su propia naturaleza las empresas que operan en el campo de las telecomunicaciones han de tratar un ingente número de datos personales y de aquí la importancia y especial atención que la APD presta a estas operadoras a la hora de planificar sus inspecciones sectoriales. Por ello, y de la misma manera que durante el ejercicio 1999 se articuló y culminó un Plan Sectorial de Oficio sobre los operadores de telefonía fija, el año 2000 ha sido el año en el que se planificó y culminó la inspección de los operadores de telefonía móvil.

Se decidió realizar este Plan debido al fuerte crecimiento que este sector ha tenido en nuestro país, donde el volumen de clientes ha crecido de forma considerable, llegando incluso a sobrepasar el número de líneas móviles al número de líneas de telefonía fija. El elevado número de clientes, unido a la fuerte competencia entre los operadores por incrementar su cuota de mercado, hacen de este sector uno de los más dinámicos y uno de los que más invierte en marketing. Por todo ello, se consideró necesario analizar qué tratamientos se realizan en el sector con los datos personales de los clientes y estudiar su adecuación a la normativa de protección de datos.

En esta ocasión y dado que son sólo tres los concesionarios que en España operan con las correspondientes licencias, se decidió realizar actuaciones sobre todos ellos: **Telefónica Servicios Móviles, S.A.,** que comercializa los servicios bajo las denominaciones MoviLine y MoviStar; **Airtel Móvil, S.A.,** que los comercializa con la denominación Airtel; y **Retevisión Móvil, S.A.**, que comercializa el suyo bajo la denominación de Amena.

El alcance que se ha dado a las inspecciones ha sido la normativa general de protección de datos con inclusión del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, así como la normativa específica de protección de datos en el sector de las telecomunicaciones recogida en el Título V del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones.

Al cierre del año 2000 ha quedado finalizado el trabajo de campo sobre los tres operadores, si bien, dada la profundidad con la que se han realizado dichas inspecciones, al cierre de la presente memoria no ha concluido el análisis completo de la información recabada. De las conclusiones de dicho análisis y las pertinentes recomendaciones dictadas por el Director de la APD se informará oportunamente en la Memoria del ejercicio próximo.

En las inspecciones efectuadas se han analizado la gran mayoría de los ficheros inscritos por los citados operadores en el Registro General de Protección de Datos de la Agencia de Protección de Datos y que engloban básicamente la gestión de clientes y la de empleados, así como otros ficheros con distintas finalidades como los ficheros dedicados al control de acceso a las instalaciones, los de proveedores y otros.

A continuación se realiza un breve estudio de los distintos riesgos, desde el punto de vista de la privacidad, existentes en una red telefonía móvil, para finalmente describir de forma genérica los tratamientos que en líneas generales realizan los operadores con los datos personales de que disponen.

* *Riesgos a la privacidad en los servicios de telefonía móvil por intervención de terceros:*

Los servicios digitales GSM 900 y DCS 1800 se encuentran regulados en sus respectivas normativas del ETSI (Instituto Europeo de Estandarización en Telecomunicaciones). Estas normativas incluyen mecanismos que afectan a la parte de radiofrecuencia del sistema y hacen que el riesgo de la seguridad sea mínimo.

Por el contrario, los servicios de telefonía móvil analógicos no incluyen en sus especificaciones ningún mecanismo que cubra estos riesgos, por ser su concepción más antigua. No obstante, el número de clientes de estos servicios va en disminuyendo en favor de los digitales.

Entre los riesgos existentes se encuentran los siguientes:

Accesos no autorizados. La normativa GSM y DCS incluyen mecanismos de autenticación del terminal de tal forma que es extremadamente difícil acceder desde un teléfono móvil a la red haciéndose pasar por otro. Debido a la construcción y diseño de la red, tampoco es factible acceder desde un terminal telefónico no autorizado, tanto al sistema informático como a la configuración del sistema de comunicaciones de la red.

Posibilidad de interceptar las comunicaciones. Las normativas GSM y DCS incorporan mecanismos de cifrado de las comunicaciones mediante el denominado algoritmo A5, por lo que resulta extremadamente complejo para un tercero interceptar las conversaciones.

* *Gestión de clientes:*

Los usuarios de telefonía móvil pueden disponer del servicio con dos modalidades diferentes de abono:

Prepago: Representa esta modalidad aproximadamente un 70% del colectivo de clientes totales de telefónica móvil y se caracteriza por que no existe contrato escrito de abono al servicio.

Los usuarios disponen de un terminal (teléfono) que se activa por medio de una tarjeta de prepago, adquirida previamente y con un saldo inicial que va disminuyendo a medida que se hacen llamadas, hasta que el saldo se queda a cero pesetas o se recarga de nuevo la tarjeta. En definitiva, se paga el servicio con antelación a su utilización.

Los operadores apenas disponen de datos personales de este colectivo de clientes debido a que no es necesario identificarse, ya que no existe contrato ni facturas. De hecho, el operador ignora, en la mayoría de los casos, si la línea corresponde a una persona física o jurídica. Los pocos datos de que disponen los operadores sobre los clientes de este colectivo han sido recabados principalmente mediante promociones en las que se ofrecía tiempo gratuito de llamadas a cambio de facilitar los datos personales.

Esta situación de anonimato respecto de los abonados de prepago españoles es atípica dentro del entorno europeo, donde en la mayoría de países se exige la identificación completa del abonado a la hora de contratar el servicio. La exigencia viene fundada en requerimientos legales, y fundamentalmente en la obligada colaboración de los operadores con las fuerzas y cuerpos de seguridad de cada Estado.

Postpago: Representa esta modalidad aproximadamente un 30% del colectivo de clientes totales de telefónía móvil y se caracteriza por la existencia de un contrato escrito entre el abonado y el operador. En este caso, el abonado ha de facilitar sus datos personales, así como los relativos a la domiciliación del cobro de la correspondiente factura. En este caso, y al contrario que en la modalidad de prepago, el pago se produce con posterioridad a la utilización del servicio.

* *Solicitud de servicio, estudio y alta del cliente.*

El primer tratamiento de datos que se realiza consiste en la recogida de datos de la persona que solicita el servicio. En general, dicha solicitud puede realizarse de forma telefónica, a través de los centros de atención al cliente del operador, o a través de distribuidores concertados.

En ambos casos, y respecto de los que solicitan la modalidad de pospago, al operador le llegan los datos básicos del solicitante: nombre, apellidos, domicilio, datos bancarios para el cobro de las facturas, etc. En el caso de un operador concreto, además de los datos anteriores se recaban datos adicionales entre los que figuran profesión, puesto de trabajo, antigüedad en la empresa y datos familiares (personas a su cargo, tipo de vivienda y estado civil).

Con los datos anteriormente recabados, el operador realiza un estudio o análisis de riesgos sobre el cliente cuya grado de profundidad varia de un operador a otro. Por ejemplo, todos los operadores consultan si el solicitante es o ha sido cliente de la empresa y cual ha sido su comportamiento de pago con la misma.

También realizan los tres operadores consultas a un fichero que recoge incumplimientos de obligaciones dinerarias con diversas entidades (bancos, cajas de ahorros, entidades financieras, otras empresas de telecomunicaciones, etc.).

Adicionalmente, uno de los operadores realiza un estudio o *scoring* en el que tiene en cuenta toda la información recabada en la solicitud.

La justificación de este análisis de riesgos radica en que en la modalidad de pospago, y como el propio término indica, el servicio se paga con posterioridad a su utilización, por lo que la factura a una fecha recoge las llamadas producidas en los treinta días anteriores para el caso de las llamadas originadas desde España, y las llamadas producidas varios meses atrás en el caso de las realizadas en itinerancia o *roaming* (llamadas efectuadas desde el teléfono móvil cuando se encuentra en un país extranjero) .

En este último caso, el retraso de hasta varios meses es debido a que la llamada de un abonado en itinerancia es tarificada por el operador extranjero que le facilita la cobertura, quien la remite a un centro de compensación internacional que agrupa a todos los operadores entre los que existe acuerdo de itinerancia, para llegar finalmente al operador nacional del abonado que le factura dicha llamada.

El retraso entre la prestación del servicio y el pago del mismo supone un riesgo para el operador, riesgo que crece cuanto mayor es dicho retraso ya que se pueden acumular importes mayores. Por esta razón, la normativa de telecomunicaciones permite a los operadores de telefonía móvil condicionar la prestación de determinados servicios al depósito por parte del abonado de una fianza previa, fianza que se fija por el operador en función del resultado del estudio o análisis de riesgo del cliente y que puede llegar hasta un millón de pesetas.

Una vez realizado el estudio, se le comunica al cliente que se va a proceder al alta del servicio o, en caso contrario, que se condiciona dicho alta o alguno de los servicios al deposito de una fianza previa. En este último caso es el solicitante el que tiene la última la palabra, pudiendo optar entre las diferentes opciones: depositar la fianza, solicitar el alta en otro operador u optar por un servicio en la modalidad de prepago.

En la modalidad de prepago, la situación a este respecto es distinta, ya que al pagarse el servicio con carácter previo a su utilización, no existe riesgo de impago.

En la práctica, el colectivo de solicitantes a los que se les condiciona el servicio al depósito de una fianza es pequeño comparado con el volumen total de solicitudes.

Una vez aceptadas las condiciones se procede al alta del abonado, tanto en el sistema de información de gestión de clientes, como en el sistema de gestión de la red que proporciona el servicio de telefonía.

* *Repertorio de abonados.*

Dos de los tres operadores disponen de dicho repertorio o directorio. En ambos casos existe repertorio en la modalidad de consulta telefónica, siendo atendido por operadores que únicamente facilitan el número del teléfono móvil a partir del nombre del abonado.

Si bien ambos operadores reconocen el derecho del abonado a excluir sus datos del repertorio, la política de alta no es común, ya que en un caso se requiere la solicitud previa del abonado, mientras que en el otro el alta se produce siempre que el abonado no especifique lo contrario.

En la situación actual, cada operador mantiene su propio repertorio conteniendo exclusivamente sus abonados, no existiendo ningún repertorio común. Tampoco existe acceso al repertorio de forma on-line ni se publica en ningún tipo de soporte.

* *Datos de tráfico para la facturación.*

En la utilización normal del servicio, el sistema de gestión de la red genera los denominados registros de datos de llamadas o CDR`s. Del tratamiento de dichos registros se obtienen los datos de las llamadas que han tenido lugar en la red de telefonía. Estos datos generados en el sistema de gestión de red se vuelcan en el sistema de facturación donde las llamadas se tarifican y se asignan a cada cliente con el fin de facturarlas.

Respecto de la facturas, los tres operadores recogen por defecto el detalle de las llamadas con indicación del número de destino, fecha, hora de inicio y duración de cada llamada.

Los tres operadores disponen, de conformidad con el artículo 66 del Real Decreto 1736/1998, de la opción para el abonado de recibir facturas no detalladas. No obstante, no se ha publicado aún la resolución de la Secretaría General de Comunicaciones que establezca las distintas modalidades de facturación detallada que los abonados puedan solicitar a los operadores, según establece el citado artículo.

* *Análisis y control del fraude.*

Los tres operadores disponen de unidades encargadas de vigilar y prevenir situaciones de riesgo y fraude que puedan suponer un riesgo económico para la empresa. Estas situaciones suelen ir asociadas a consumos elevados en cortos períodos de tiempo, así como a altas fraudulentas en las que los datos facilitados por el titular son falsos o suplantan a otra persona.

Con el fin de comprobar la veracidad de los datos facilitados por los abonados, detectar datos falsos y evitar suplantaciones de identidad, algunos operadores tratan de confirmar los datos facilitados por los abonados con las entidades bancarias en las que se han domiciliado los pagos. En algunos casos estas verificaciones son realizadas por empresas contratadas al efecto en régimen de prestación de servicios.

* *Tratamiento de impagados.*

Cuando se produce el impago de una factura se desencadena una serie de procedimientos tendentes al cobro de la misma. Los procedimientos definidos por los tres operadores para dicho tratamiento presentan bastantes semejanzas y en líneas generales el procedimiento seguido dispone de tres fases diferentes:

En primera instancia se suele producir una serie de contactos telefónicos con el abonado a iniciativa de personal del operador, de cara a conocer el motivo del impago y si existe o no intención de pago.

Si los contactos telefónicos fracasan se desencadena una serie de envíos por escrito requiriendo el pago de la deuda y facilitando el procedimiento a seguir para el pago de la misma.

Finalmente, si los requerimientos por escrito fracasan, dos de los operadores recurren a empresas especializadas en cobro de impagados, que tramitan el pago de las deudas en régimen de prestación de servicios.

Dependiendo de cada operador, en un momento dado del impago se bloquea el teléfono móvil del abonado deudor, de forma que únicamente se permite la recepción de llamadas. Si el impago persiste se puede llegar incluso al bloqueo total del teléfono.

Los tres operadores también tiene en común el facilitar los datos de deuda de sus clientes a un mismo fichero de incumplimiento de obligaciones dinerarias, por lo que los datos de una deuda con un operador van a ser conocidos por los otros operadores.

* *Tratamiento de los datos con fines comerciales.*

Los tres operadores disponen de sistemas especializados en el tratamiento masivo de datos del tipo *datawarehouse.* Sobre este tipo de sistemas los operadores vuelcan diversas tipologías de datos: análisis del cliente previo al alta del mismo, servicios contratados, datos de tráfico y facturación, información del análisis del fraude y de impagados, etc. Una de las finalidades para la que se realiza tratamiento de datos en el sistema de datawarehouse es la de promoción comercial de bienes y servicios propios. En este sentido, adquiere especial relevancia para dicho fin el tratamiento de los datos de tráfico y facturación, ya que para dicho tratamiento existe una previsión normativa específica establecida en el artículo 65 del Real Decreto 1736/1998, de 31 de julio. Según dicha previsión, del conjunto global de datos de tráfico y facturación únicamente pueden ser tratados con fines comerciales los que se detallan a continuación, siempre y cuando se haya recabado el consentimiento previo de los afectados: <OL>

* El número o la identificación del abonado.
* La dirección del abonado y el tipo de equipo terminal empleado para las llamadas.
* El número total de unidades que deben facturarse durante el ejercicio contable.
* El número del abonado que recibe la llamada.
* El tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitidos.
* La fecha de la llamada o del servicio.
* Otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes. </OL>

La información contenida en el *datawarehouse* se encuentra dividida en diversos bloques o universos con información y usuarios específicos cada uno de ellos.

Mediante el cruce de los datos contenidos en cada universo es posible realizar un análisis sobre el comportamiento de los clientes.

* *Servicio de atención al cliente:*

Estos servicios, denominados *Call Center*, son atendidos en su gran mayoría por empresas especializadas, en régimen de prestación de servicios.

El personal de este servicio tiene acceso, de forma general, a la mayoría de los datos personales de los clientes entre los que se incluyen datos sobre las llamadas efectuadas y la facturación. El acceso a dichos datos se justifica en la necesidad de atender las llamadas procedentes de clientes planteando cuestiones muy diversas: consultas, modificaciones de datos, reclamaciones, etc.

El índice de rotación del personal de las empresas que prestan estos servicios es elevado y en la mayor parte de los casos no queda constancia de los accesos efectuados.

* *Servicio de identificación de llamadas:*

En general y de acuerdo con lo previsto en el título V del Real Decreto 1736/1998, los operadores proporcionan los servicios de identificación de línea llamante y disponen de los mecanismos para la supresión de la identificación de la línea llamante tanto en la modalidad de llamada a llamada como en la de por línea.

* *Servicio de mensajes cortos:*

Respecto del servicio de mensajes cortos o SMS, cabe destacar que todos los operadores proporcionan este tipo de servicio a sus clientes, tanto de prepago como de pospago.

En dicho servicio se ha analizado la remisión de mensajes SMS por parte del operador cuando son efectuados por procedimientos automáticos (sin intervención humana). En este sentido, los operadores remiten mensajes cortos SMS a los teléfonos móviles de los clientes ofreciendo descuentos y la posibilidad, como promoción, de utilizar gratis temporalmente un servicio de valor añadido.

* *Seguridad:*

Se ha analizado en los tres operadores lo dispuesto en el artículo 9 de la Ley Orgánica 15/99, así como en el Real Decreto 944/1999 por el que se desarrolla dicho artículo y aprueba el Reglamento de Medidas de Seguridad.

Los operadores han catalogado sus sistemas de información de acuerdo a la clasificación de niveles establecida en el Reglamento de Medidas de Seguridad, adoptando las medidas correspondientes a dichos niveles.

En general, los operadores han elaborado documentos de seguridad, si bien con criterios distintos. Algunos operadores han elaborado los documentos de seguridad de acuerdo a los ficheros inscritos en el Registro General de Protección de Datos de la Agencia y otros han confeccionado un único documento de seguridad que aglutina a todos los sistemas de información de la empresa.

En general, todos los operadores han definido la figura del responsable de seguridad, han establecido controles de accesos a la información con mecanismos de identificación y autenticación, han implantado un registro de incidencias, realizan gestión de los soportes y disponen de procedimientos de copias de respaldo y recuperación.

En lo relativo a auditoría, únicamente uno de los tres operadores ha realizado ya una auditoria de seguridad. No obstante, aún no ha finalizado el plazo para realizarlas. 2.2.5 Consorcio de Compensación de Seguros

También dentro de los Planes Sectoriales de Oficio, el Director de la APD acordó inspeccionar durante el año 2000 los ficheros del Consorcio de Compensación de Seguros (CONSORCIO) cuya actividad vienen regulada en el Estatuto Legal de la Entidad y la Ley 21/1990, sobre adaptación del Derecho Español a la Directiva 88/357/CEE, rigiéndose en cuanto a sus funciones aseguradoras por lo previsto en la Ley de Contrato de Seguro.

El CONSORCIO se constituye como Entidad de Derecho Público con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, dotado de patrimonio distinto al del Estado, que ajustará su actividad al ordenamiento jurídico privado. Se encuentra adscrito al Ministerio de Economía según establece el Real Decreto 1371/2000. 2.2.5.1. Objetivos.

Los objetivos a nivel general que se establecieron en el plan de inspección fueron los siguientes:

* Conocer los Sistemas de Información y procedimientos utilizados por el CONSORCIO para el cumplimiento de las funciones que tiene asignadas en las que intervienen datos de carácter personal.
* Determinar el grado de cumplimiento con las disposiciones de la Ley Orgánica 15/1999 y del Real Decreto 994/1999 respecto de los ficheros automatizados de los que es responsable el CONSORCIO.
* Establecer, en su caso, las deficiencias que pudieren existir en los tratamientos automatizados y dictar las pertinentes recomendaciones con objeto de subsanarlas. 2.2.5.2. Estudio preliminar.

Una vez establecidos los objetivos se procedió al estudio de los siguientes ficheros automatizados que el CONSORCIO tiene notificados en el Registro General de Protección de Datos:

* **Gestión de Siniestros:** con la denominación "EXPESINI", incluye los datos personales de los afectados necesarios para tramitar una reclamación como consecuencia de un siniestro sobre un bien o persona asegurada, que el CONSORCIO está obligado a indemnizar. Inscrito con el código 1942235163.
* **Fichero Informativo de Vehículos Asegurados:** con la denominación "FIVA", contiene los datos personales del peticionario, relativo al aseguramiento de vehículos a motor de forma temporal. Inscrito con el código 1961690004.
* **Seguros Directos:** con la denominación "SEGURIDE", incluye los datos personales de los afectados, del vehículo e importes de las primas de los asegurados, que contratan una póliza de responsabilidad civil con el CONSORCIO. Inscrito con el código 1942235165.
* **Gestión de Personal:** con la denominación "PERSONAL", contiene la información necesaria para la gestión de los recursos humanos de la organización. Inscrito con el código 1942235164.
* **Control de Visitas:** con la denominación "VISICONTROL", incluye la identidad de las personas que acceden a las dependencias de los servicios centrales del CONSORCIO. Inscrito con el código 1993500003.

En base a la naturaleza de la información que contienen y atendiendo al punto de vista de su repercusión para los ciudadanos, los ficheros que se seleccionaron para su investigación fueron los denominados "EXPESINI", "FIVA" y "SEGURIDE". Con este objetivo, durante los meses de septiembre a noviembre del año 2000 se realizaron diversas inspecciones en las dependencias de los Servicios Centrales del CONSORCIO, en la Delegación Provincial en Madrid de la citada Entidad y en la sociedad que se encarga de la prestación de servicios informáticos. 2.2.5.3. Conclusiones de la Inspección.

De las actuaciones efectuadas por la Inspección de Datos y del análisis de la documentación recabada en relación con la normativa vigente en materia de Protección de Datos y de Seguros, se desprenden las siguientes conclusiones:

* Respecto a la Información utilizada por el CONSORCIO.
* El Sistema de Información "EXPESINI" gestiona la información referente a la tramitación de los Expedientes de Siniestros, derivados, entre otros, de Riesgos Extraordinarios o del Seguro de Responsabilidad Civil del Automóvil de Suscripción Obligatoria, con un volumen actual de un millón de expedientes.
* El Sistema de Información "FIVA" registra la información relativa al Aseguramiento de Vehículos, con datos de más de 21 millones de matrículas y de los peticionarios de información efectuadas al mismo.
* El Sistema de Información "SEGURIDE" incluye información de las pólizas del Seguro de Responsabilidad Civil del Automóvil de Suscripción Obligatoria, con un volumen de unas 250.000 pólizas. Del análisis de los Sistemas de Información utilizados por el CONSORCIO no se ha constatado que la tipología de la información que incluyen no sea la necesaria para el desempeño de las funciones que legalmente tiene atribuidas.
* Respecto a la Procedencia de la información.

La información que gestiona el CONSORCIO es facilitada por los propios ciudadanos, sea como consecuencia de la contratación de un seguro del automóvil, la reclamación por siniestro o la solicitud de información sobre el aseguramiento de un vehículo, a través de "impresos" establecidos por la entidad al efecto.

Por otra parte, para la tramitación de reclamaciones de siniestros pueden remitir información al CONSORCIO: Jueces y Tribunales, Instituciones Sanitarias Públicas y Privadas y Peritos, según establecen los Convenios suscritos entre las partes y la normativa vigente.

De acuerdo a lo establecido en la Directiva 90/232/CEE, la Ley 30/1995 y la RESOLUCIÓN de 8 de marzo de 1996 de la Dirección General de Seguros, la información referente al aseguramiento de los vehículos incluida en el fichero "FIVA", es remitida al CONSORCIO por todas las compañías del sector.

* Respecto a la Calidad de los datos.

El hecho más significativo respecto a la calidad de los datos personales tratados por el CONSORCIO consiste en que no se han realizado cancelaciones de la información incluida en sus Sistemas de Información desde la implantación de los mismos, habiéndose verificado que:

* En el Sistema de Información "EXPESINI" figuran datos personales desde el año 1968, con un total de un millón de expedientes, encontrándose unos 200.000 en situación "cerrado" con anterioridad al año 1990.
* En el Sistema de Información "SEGURIDE" constan datos personales desde el año 1975, correspondientes a 100.000 pólizas de aseguramiento de vehículos particulares, de las cuales más de la mitad se encuentran en situación de "no vigentes".
* Respecto al Derecho de información en la recogida de datos.

En los impresos establecidos por el CONSORCIO con objeto de recabar los datos personales de los afectados: "Hoja de Comunicación de Siniestro", "Declaración Amistosa de Accidente de Automóvil", "Solicitud de Seguro Ramo de Automóviles" y "Consulta de datos de Aseguramiento de Vehículos"; así como en la "Póliza de Seguro de Automóviles", se ha comprobado que no figura en ninguno de ellos información de los requisitos a los que se refiere el artículo 5 de la LOPD.

* Respecto al Consentimiento del afectado para el tratamiento.

El CONSORCIO no solicita el consentimiento de los afectados para el tratamiento automatizado de los datos de carácter personal. No obstante, se debe tener en consideración:

* La gestión de la póliza del Seguro del Automóvil está sujeta al régimen general de la Ley de Contrato de Seguro y debe ser suscrita por ambas partes.
* La información relativa a las reclamaciones por siniestro es facilitada al CONSORCIO de conformidad con lo dispuesto en la normativa vigente, Ley 50/1980, Ley 21/1990 y Ley 30/1995.
* Respecto a Datos especialmente protegidos. El CONSORCIO procede al tratamiento automatizado de datos de carácter personal relativos a la salud en la tramitación de las reclamaciones de siniestros en los que se han producido daños personales. La citada información es facilitada en la mayoría de los casos por los propios afectados, los Tribunales o profesionales sanitarios. En este sentido, la normativa vigente establece la obligatoriedad por parte del afectado de facilitar toda clase de informaciones sobre las circunstancias y consecuencias del siniestro.

Se ha constatado por parte de la Inspección de Datos que la citada información es evaluada e incluida en el fichero automatizado por personal adscrito a la Asesoría Médica, si bien puede ser consultada por todas las personas que tienen acceso autorizado a la tramitación del siniestro. También se ha verificado que dicho fichero contiene 12.501 reclamaciones en las que figuran datos de salud, siendo las más antiguas del año 1996.

* Respecto a la Comunicación de datos.

El CONSORCIO facilita información parcial y puntual referente a los Expedientes de Siniestros, a través de medios telemáticos, a entidades bancarias con objeto de la gestión de los pagos a que dan lugar los mismos, y a la Agencia Estatal de Administración Tributaria en relación a las operaciones con terceras personas, de acuerdo a lo establecido en el art. 112 de la Ley General Tributaria y en el Real Decreto 2027/1995.

Por otra parte, se facilita documentación de los siniestros a los Tribunales y a la Oficina Española de Aseguradores de Automóviles, en virtud de la Orden de 25 de septiembre de 1987 del Ministerio de Economía y Hacienda.

Con respecto al Sistema de Información "FIVA", la finalidad del mismo es facilitar información puntual a las personas físicas y jurídicas implicadas en un accidente de circulación, según establece la Directiva 90/232/CEE y la Ley 30/1995.

* Respecto al Acceso a los datos por cuenta de terceros.

Las actividades que implican tratamiento automatizado de datos de carácter personal y que son efectuadas por empresas externas son:

* Servicios informáticos para la gestión del Sistema de Información "FIVA".
* Servicio de Atención Telefónica de información general y de la tramitación de un siniestro, mediante contrato suscrito con una compañía del sector en el cual se especifican aspectos relativos a la Ley Orgánica 5/1992.
* Respecto a los derechos de las personas: acceso, rectificación y cancelación.

El CONSORCIO no dispone de un procedimiento documentado con objeto de la tramitación de solicitudes del ejercicio de los derechos de acceso, rectificación y cancelación. No obstante, aunque los procedimientos no se encuentren formalmente definidos, no se han encontrado evidencias de que no se atiendan correctamente el ejercicio de estos derechos.

Por otra parte, los afectados pueden requerir en cualquier momento, incluso por teléfono, información sobre la situación de tramitación de un siniestro y solicitar la rectificación de los datos personales incluidos en el expediente.

* Respecto a la creación, notificación e inscripción registral.

En las actuaciones practicadas por la Inspección se ha comprobado que ciertos aspectos de los ficheros automatizados cuya titularidad corresponde al CONSORCIO no coinciden con el contenido de la inscripción de los mismos en el Registro General de Protección de Datos.

Con respecto al fichero "SEGURIDE" y al "EXPESINI" la información relativa a la estructura del fichero y la descripción de los tipos de datos de carácter personal no se ajusta a la situación real, e incluso los datos especialmente protegidos que contiene el fichero "EXPESINI" no constan en la notificación.

Con respecto al fichero "FIVA" los apartados "*Ubicación principal*", "*Encargado del tratamiento* ", "*estructura* ", "*procedencia* " y "*cesiones* " no están debidamente comunicados al citado Registro.

* Respecto al Reglamento de medidas de seguridad.

Por Real Decreto 994/1999, se ha aprobado el Reglamento que especifica los requisitos y condiciones en materia de seguridad que deberán adoptarse en los ficheros automatizados que contengan datos de carácter personal. De acuerdo con lo establecido en el mismo, las medidas de nivel básico y medio han entrado en vigor respecto de los ficheros que se encontraban en funcionamiento en el momento de su publicación, como es el caso de los ficheros cuyo responsable es el CONSORCIO. A continuación se describen los aspectos más relevantes referentes al Reglamento de medidas de seguridad:

* *Niveles de seguridad.* El nivel de seguridad que deben cumplir los ficheros cuyo responsable es el CONSORCIO, atendiendo a la naturaleza de la información que contienen, es el básico para los ficheros denominados "SEGURIDE" y "FIVA". En cuanto al fichero "EXPESINI", deberá cumplir además de las medidas de nivel básico las calificadas como nivel medio y alto, ya que incluye datos referentes a la salud de los afectados.
* *Documento de Seguridad.* El Documento de Seguridad facilitado por el CONSORCIO a la Inspección de Datos no incluye aspectos a que hace referencia el Real Decreto 994/1999, entre otros, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento, las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado y el personal autorizado con acceso a los locales donde se encuentren ubicados los Sistemas de Información con datos de carácter personal.

Funciones y obligaciones del personal.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los Sistemas de Información del CONSORCIO no se encuentran definidas y documentadas, de conformidad con lo dispuesto en el artículo 9 del mencionado Reglamento, ni se han difundido entre el personal con acceso a los datos automatizados de carácter personal y a los Sistemas de Información.

* *Identificación y autenticación.*

El acceso a los Sistemas de Información se realiza mediante procedimientos de identificación y autenticación, que permite la identificación de forma inequívoca y personalizada de los usuarios que intenten acceder al sistema. El mecanismo de autenticación se basa en la existencia de contraseñas que deben ser cambiadas mensualmente por parte del usuario. Sin embargo, el CONSORCIO no dispone de un mecanismo para los de nivel medio que permita limitar la posibilidad de intentar reiteradamente el acceso no autorizado a los Sistemas de Información, según establece el artículo 18.2 del Real Decreto 994/1999..

* *Medidas de seguridad de nivel alto.*

En el fichero "EXPESINI" figuran datos especialmente protegidos sobre información referente a la salud. Por ello deberán adoptarse las medidas calificadas como de nivel alto en el plazo establecido en el Real Decreto 994/1999 (26/06/01), ya que en las actuaciones de Inspección de Datos se ha verificado que en la actualidad no se tienen implementadas.

A modo de RECAPITULACIÓN de todo el apartado **2.2** de esta Memoria y a efectos solamente informativos, cabe concluir indicando que durante el año 2001 se dictarán las pertinentes recomendaciones consecuencia de las inspecciones realizadas en el Plan Sectorial de Oficio hasta aquí analizado, recomendaciones de las que se dará cuenta en la Memoria del próximo año.

3. ACTUACIONES MÁS RELEVANTES EN EL ÁMBITO DE LOS FICHEROS DE TITULARIDAD PÚBLICA

La LOPD regula en su Título IV, dedicado a las disposiciones sectoriales, dos clases de ficheros: Ficheros de titularidad pública y ficheros de titularidad privada estableciendo un diferente régimen jurídico para ambas categorías de ficheros. Así mientras que para crear y modificar ficheros privados la Ley exige únicamente su notificación, previa a la inscripción, a la Agencia de Protección de Datos (arts. 26 LOPD y 6 R.D. 1332/1994, de 20 de junio), la creación, modificación y supresión de ficheros públicos requiere en toda caso la adopción de una disposición general publicada en el Boletín Oficial correspondientes (art. 20 LOPD y 5 y 7 R.D. 1332/1994).

La Ley no define expresamente qué debemos entender por ficheros públicos, limitándose a indicar que tienen tal

carácter los ficheros de los que son titulares las Administraciones Públicas (art. 20). En este sentido, además de los ficheros de los órganos constitucionales, tendrán la consideración de ficheros públicos los creados por las Administraciones territoriales (Administración General del Estado, Comunidades Autónomas y Entidades que integran la Administración Local) y como regla general también los de la Administración Institucional (Entidades de Derecho Público con personalidad jurídica propia vinculadas o dependientes de cualquier Administración territorial). Más problemático es, sin embargo, determinar cuándo los ficheros de la denominada Administración corporativa (Colegios Profesionales y Cámaras Oficiales de Comercio, Industria y Navegación) pueden ser considerados ficheros de titularidad pública, si bien en una primera aproximación puede decirse que su catalogación como fichero público o privado dependerá de la naturaleza jurídica que se otorgue a los colegios Profesionales y Cámaras Oficiales, es decir, de su consideración o no como Administraciones Públicas. Tomando en consideración este criterio, los ficheros corporativos habrán de ser concebidos como de naturaleza pública o privada en atención a la finalidad que por los mismos se persiga. Así serán de naturaleza pública los ficheros cuya finalidad sea el ejercicio por el responsable de las potestades administrativas conferidas por las leyes y reglamentos, siendo de titularidad privada los ficheros corporativos vinculados al desempeño de actividades propias de Derecho privado.

Durante el ejercicio correspondiente al año 2000, las más importantes actuaciones de la APD en el campo de los ficheros de titularidad pública afectan a las Administraciones Públicas estatal, autonómica y local, que pasamos a exponer seguidamente.

3.1. ADMINISTRACIÓN GENERAL DE ESTADO

A pesar de su incremento respecto del año anterior, debemos destacar el número relativamente bajo de reclamaciones formuladas ante esta Agencia por posibles infracciones de responsables de ficheros cuya titularidad corresponde a las Administraciones Públicas; máxime si se tiene en cuenta que algunos de los organismos que pertenecen al ámbito de la Administración General del Estado disponen de ficheros automatizados que contienen, a nivel nacional, datos personales de millones de ciudadanos y de gran transcendencia para los mismos.

Los Organismos de la Administración General del Estado sobre los que se han centrado las actuaciones de la APD en el año 2000 han sido los siguientes:

* La Agencia Estatal de Administración Tributaria.
* La Tesorería General de la Seguridad Social.
* El Instituto Nacional de la Seguridad Social.
* El Instituto Nacional de Empleo.
* La Dirección General de Tráfico.
* La Delegación del Gobierno en Castilla y León.
* El Ministerio de Defensa.
* El Ministerio de Educación y Cultura.
* El Ministerio de Asuntos Exteriores.

3.1.5. Resoluciones más relevantes del Director de la Agencia de Protección de Datos.

De entre las Resoluciones dictadas por el Director de la Agencia durante el año 2000 referentes a ficheros cuya titularidad corresponde a la Administración General del Estado, merecen especial mención las siguientes:

3.1.5.1. Resolución de Archivo de Actuaciones al Instituto Nacional de la Seguridad Social.

Un ciudadano denunció ante la APD el procedimiento utilizado por el INSS para conseguir los datos personales para el cálculo de las nuevas retenciones del IRPF, constatándose por la Agencia que el Instituto Nacional de la Seguridad Social, en aplicación de lo dispuesto en la Ley 40/1998, remitió a determinados pensionistas un impreso con objeto que se cumplimentara y que sirviera de base para el cálculo de las retenciones del IRPF. Entre los datos personales a facilitar se encontraba, en su caso, el Número de Identificación Fiscal (NIF) del cónyuge, la fecha de nacimiento y el grado de minusvalía de hijos o descendientes y debía ser firmado por el perceptor. En el impreso se especificaba:

* *"Los datos personales y familiares aportados por usted van a ser incorporados a un fichero informático, a efectos de servir de base para el cálculo de las retenciones establecidas en la Ley del IRPF".*
* *"Si prefiere no comunicar alguno de los datos siguientes, la retención que se le practique podría resultar superior".*

Se comprobó por la Inspección de la Agencia que el afectado remitió cumplimentado el impreso relativo a la "*Comunicación de la situación personal y familiar* " y en el mismo no constan datos familiares y tampoco constan en el fichero automatizado que incluye los datos personales del afectado, por lo que en el caso concreto del denunciante procede el Archivo de su reclamación.

El Director de la Agencia acordó proceder al Archivo de la reclamación formulada por un ciudadano, si bien al amparo de las potestades que le otorga el Art. 5 c) y d) del Estatuto de la Agencia, dictó las siguientes RECOMENDACIONES que obligan al citado Instituto a cumplir con el derecho de información en la recogida de datos y a recabar el consentimiento expreso del afectado.

PRIMERA: DE LA RECOGIDA Y TRATAMIENTO DE DATOS PERSONALES

El Instituto Nacional de la Seguridad Social deberá incluir en el Modelo de "comunicación de situación Familiar y Personal", o en otra fórmula alternativa, una cláusula tipo con la información del Art. 5 de la LOPD en la que a los interesados a los que se soliciten datos se les informe de modo expreso, preciso e inequívoco: de la existencia de un

fichero automatizado; del carácter obligatorio o facultativo de su respuesta; de las consecuencias de la obtención de los datos o su negativa; de los derechos de acceso, rectificación, cancelación y oposición; y de la identidad y dirección del responsable del tratamiento, o en su caso de su representante.

SEGUNDA: DEL CONSENTIMIENTO DEL AFECTADO

El Instituto Nacional de la Seguridad Social deberá incluir en dicho modelo, o a través de otra fórmula, un apartado que facilite y recoja el consentimiento expreso del afectado para el tratamiento de datos como los relativos a la "salud" derivados de minusvalías y otros datos especialmente protegidos como alimentos a favor de hijos y pensiones compensatorias al cónyuge.

El Instituto Nacional de la Seguridad Social ha comunicado a la Agencia de Protección de Datos las medidas correctoras adoptadas al efecto en cumplimiento de las precitadas Recomendaciones practicadas en la Resolución de Archivo y que podemos resumir en la incorporación en los nuevos formularios de solicitud de pensiones todas las observaciones efectuadas por el Director de la Agencia de Protección de Datos y así consta en los modelos de formularios remitidos por el citado Instituto a esta Agencia.

3.1.5.2. Resolución de Infracción de las Administraciones Públicas a la Agencia Estatal de Administración Tributaria.

La Agencia Estatal de Administración Tributaria ha utilizado para fines distintos de los tributarios los datos personales de un contribuyente, con objeto de notificar asuntos laborales a otra persona, conculcándose con ello el principio de finalidad del artículo 4.2 de la Ley Orgánica 5/1992, que establece lo siguiente: "*Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos",* y produciéndose la infracción tipificada en el artículo 43.3d) de la mencionada Ley Orgánica.

La Agencia Estatal de Administración Tributaria manifiesta en su descargo que el precepto presuntamente infringido ha sido derogado por la Disposición derogatoria única de la Ley Orgánica 15/1999, de 13 de diciembre, cuya entrada en vigor se produjo el día 14 de enero de 2000; las normas sancionadoras no favorables son irretroactivas vedando toda posible aplicación de la nueva Ley Orgánica a unos hechos acaecidos en el mes de agosto de 1.998.

Sin embargo no puede tenerse en consideración esta alegación ya que los hechos se produjeron en el mes de agosto de 1.998, y el procedimiento sancionador se inició con fecha 20 de diciembre de 1.999, estando, por tanto en ambos momentos, en vigor la Ley Orgánica 5/1992, de 29 de octubre. La Ley Orgánica 15/1999 no ha previsto un régimen transitorio para los procedimientos iniciados antes de la entrada en vigor de la nueva Ley, por lo que es de aplicación de forma supletoria lo establecido en la Disposición transitoria segunda de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en cuyo apartado 1 se determina: "*A los procedimientos ya iniciados antes de la entrada en vigor de la presente Ley no les será de aplicación la misma, rigiéndose por la normativa anterior".* En este caso no cabe entender aplicable el artículo 128.1 de la Ley 30/1992, por cuanto este artículo consagra el principio de irretroactividad que consiste, tal como prescribe el artículo 25. 1 de la Constitución Española, en el derecho a no ser sancionado por conductas que en el momento de su comisión no estuvieran tipificadas como infracción administrativa.

Alega a continuación la Agencia Estatal de Administración Tributaria que no se han utilizado indebidamente los datos automatizados de carácter personal de la denunciante, puesto que la información tributaria tiene como finalidad la eficaz gestión del sistema tributario estatal y aduanero así como el cumplimiento de las demás funciones que la Ley le encomienda; siendo admisible la utilización de dicha información para llevar a cabo con rapidez y plenas garantías jurídicas los trámites inherentes a cualquier cambio en el personal directivo de la Agencia Tributaria, evitando demoras y vacíos en puestos de responsabilidad que repercutirían directamente en la propia gestión tributaria. Esta alegación ha de ser rebatida, ya que la propia Ley General Tributaria, en su artículo 113, consagra el carácter reservado de los datos, informes o antecedentes obtenidos por la Administración Tributaria en el desempeño de sus funciones, pudiéndose utilizar para la efectiva aplicación de los tributos o recursos cuya gestión tiene encomendada. En el caso concreto de este procedimiento se utilizaron los datos que la Administración Tributaria había recabado, por motivos tributarios, de la denunciante, con la finalidad de notificar a su marido el cese y nombramiento de un puesto de trabajo, cese y nombramiento que había sido publicado en el Boletín Oficial del Estado, incumpliendo con ello lo establecido en el artículo 113 de la Ley General Tributaria y el artículo 4.2 de la Ley Orgánica 5/1992.

Por último alega la Agencia Estatal de Administración Tributaria que la nueva Ley Orgánica de Protección de Datos ya no prohibe la utilización de datos para finalidades distintas de aquellas que motivaron su recogida, se prohibe la utilización para finalidades incompatibles, y en este caso concreto no se da la incompatibilidad de finalidades. Esta alegación debe ser rebatida por la razón antes aludida de la no aplicabilidad del mencionado artículo 4.2 de la Ley 15/1999, al no estar vigente en el momento de producirse los hechos imputados, y en cuanto a la alegación de incompatibilidad porque el hecho de que el vocablo de referencia sea un concepto jurídico indeterminado obliga a interpretarlo restrictivamente ya que, de otro modo, mediante interpretaciones más o menos amplias de la compatibilidad, se podría eliminar de facto el principio de autodeterminación.

En el presente caso, no puede apreciarse la compatibilidad, toda vez que los datos tributarios facilitados por un contribuyente a la Agencia Tributaria no pueden utilizarse para notificar a una persona diferente el cese y nombramiento de

un puesto de trabajo. El tratamiento de los datos del contribuyente para notificar asuntos laborales a otra persona debe considerarse a todas luces incompatible a los efectos aquí imputados de desvío de finalidad.

3.1.5.3. Resolución de Infracción de las Administraciones Públicas al Instituto Nacional de Empleo.

El Instituto Nacional de Empleo, no dando cumplimiento a la Resolución del Procedimiento de Tutela de Derechos (TD/114/1999), no envió al afectado el acceso completo a sus datos, por lo que ha infringido lo dispuesto en el artículo 14 de la LOPD, lo que supone una infracción tipificada como leve en el artículo 43.2d) de la citada norma, que precep-túa como falta leve "*Cualquiera otra que afecte a cuestiones meramente formales o documentales que no constituyan infracción grave o muy grave".*

El Instituto Nacional de Empleo envió todos los datos requeridos a excepción de los resultantes de la realización de " *sondeos"*, que consiste en el cruce de ficheros que poseen datos sobre *"ofertas de empleo"* y *"demandas".* Sin embargo, el artículo 13.2) del Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, establece "*La información comprenderá los datos de base del afectado y los resultados de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especi-ficación de los concretos usos y finalidades para las que se almacenaron los datos"* , por lo que el Instituto Nacional de Empleo infringió el citado art. 14 de la Ley.

3.1.1.4. *Resoluciones relacionadas con la gestión externa de historias clínicas.*

Antes de comenzar detallando algunas de las actuaciones más relevantes en el sector de la sanidad pública, se hace necesario mencionar, como continuación a la Memoria del año 1999, una de las actuaciones iniciadas en dicho año y finalizadas en 2000.

* En la citada Memoria se indicaba la inquietud general habida en relación con la gestión de historias clínicas pertene-cientes a Hospitales públicos, debido al traslado de dicha gestión a empresas privadas.
* Por esta causa se abrieron 5 expedientes de investigación que dieron lugar a las pertinentes inspecciones con objeto de estudiar la gestión de historias clínicas en 9 Hospitales ubicados en Pontevedra, Valencia, Gijón y Madrid.

En las inspecciones realizadas se comprobó que todas las empresas contratadas para realizar la gestión y custodia de las historias clínicas generaban ficheros de control de dicha actividad, pero sin encontrarse en ellos datos clínicos, y no efectuándose tratamiento automatizado ni cesión de datos especialmente protegidos relativos a la salud por las empresas que realizaban las labores de gestión y custodia de los archivos de historias clínicas.

Por otra parte, las actuaciones de gestión y custodia realizadas por dichas empresas quedaban amparadas en el artí-culo 27 de la Ley Orgánica 5/1992, al mediar un contrato válido entre las partes implicadas.

Además, dado que las historias clínicas se encontraban en formato papel, dicha gestión quedaba fuera del ámbito de aplicación de la LORTAD, en cuanto que las citadas historias no se hallaban informatizadas, por lo que el Director de la APD resolvió *archivar* las actuaciones al no apreciarse infracción de dicha Ley.

* A principios del año 2000 continuó la inquietud por la gestión y custodia de historias clínicas pertenecientes a Centros públicos, realizadas por empresas privadas. En este sentido y como consecuencia de una pregunta formulada al Director de la Agencia por una Diputada, se abrieron dos expedientes de investigación, uno de ellos a un Hospital de Alicante y el otro a un Centro de Especialidades dependiente del mismo Hospital.
* Tras realizar las oportunas actuaciones de investigación, resultó que la empresa contratada a tal efecto por el Hospital no había automatizado ninguno de los datos contenidos en la historias clínicas. Unicamente había creado dos ficheros en los que como datos identificativos de los pacientes, sólo se encontraban número de historia, nombre y apellidos de los pacientes. Por su parte, el Centro de Especialidades no tenía contratada con empresa alguna la custodia de sus historias clínicas, siendo en el mismo Centro donde se custodiaban.

En ambos casos el Director de la Agencia resolvió *archivar* las actuaciones dado que no se apreciaron indicios de infracción la LORTAD.

3.1.1.5. *Resoluciones relacionadas con la gestión de datos de salud.*

* La Inspección de Datos inició actuaciones por orden del Director de la Agencia, que finalizaron en el año 2000, con el fin de determinar la posible cesión de datos sensibles de salud (invalidez) a una Jefatura Provincial de Tráfico por parte del Instituto Nacional de la Seguridad Social.
* En el transcurso de las actuaciones inspectoras, se detectó que también la Consejería de Salud de la Junta de Anda-lucía proporcionaba igualmente datos de salud de los afectados a la misma Jefatura Provincial de Tráfico.

En el caso de la Consejería de Salud de la Junta de Andalucía, se ha comprobado que el fichero denominado *Incapa-cidad Laboral* creado por O.M. de 25 de julio de 1994, prevé, de manera genérica, realizar cesiones a las Administra-ciones Públicas. Esta referencia es excesivamente indeterminada y, dado que se trata de cesiones de datos que afec-tan a la salud de los afectados, debe exigirse la máxima cautela a la hora de autorizar este tipo de cesiones entre Administraciones Públicas. Así lo exigía la propia LORTAD, que únicamente las permitía si la disposición de creación del fichero así lo prevenía o una norma de superior rango que regulara su uso (el del fichero) así lo contemplaba. En el presente supuesto, no existe norma de creación del fichero que contemple esta determinada y especifica cesión ni norma de rango superior que regulando el uso del fichero contemple la cesión citada.

(1)

Por lo tanto, se precisa el consentimiento expreso de los afectados para la cesión de sus datos personales por tratarse de datos de salud, consentimiento que no existe en el presente caso. En otro caso, al tratarse de datos de salud, la cesión sólo puede permitirse ante una previsión legal que establezca su necesidad por razones de interés general (artículo 7.3).

(1)

Debe advertirse que a la fecha de la inspección referida y consiguiente Resolución del Director de la APD, aún no se había dictado la STC 292/2000, de 30 de noviembre.

* Idéntico razonamiento debe hacerse respecto al fichero denominado *Progespress*, cuyo responsable es el Instituto Nacional de la Seguridad Social, que recoge la declaración de incapacidad parcial, total, absoluta o gran invalidez de los afectados. Este fichero no identifica los destinatarios de las cesiones previstas ni menciona, de forma especifica, a la Jefatura Provincial de Tráfico entre los cesionarios. Por lo tanto, no están permitidas las cesiones de datos a otros ficheros de las Administraciones Públicas, salvo que lo consientan los propios interesados titulares de los datos, consentimiento del que el Instituto Nacional de la Seguridad Social no ha acreditado disponer. Debe igualmente recordarse la vigencia y específica aplicación del citado artículo 7.3.
* A la vista de los hechos, el Director de la Agencia resolvió lo siguiente:
* Declarar que el INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL ha cometido la infracción descrita en el artículo 11, en relación con el 7.3 de la Ley Orgánica 5/1992, de 29 de octubre, de tratamiento automatizado de datos de carácter personal.
* Declarar que la CONSEJERÍA DE SALUD DE LA JUNTA DE ANDALUCIA ha cometido la infracción descrita en el artículo 11, en relación con el 7.3 de la Ley Orgánica 5/1992, de 29 de octubre, de tratamiento automatizado de datos de carácter personal.
* Advertir al INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL y a la CONSEJERÍA DE SALUD DE LA JUNTA DE ANDALUCÍA que deben abstenerse, en lo sucesivo, de efectuar cesiones de datos no permitidas, adoptando las medidas necesarias en orden a evitar nuevas comisiones de tal infracción. Para ello, deben proceder de manera inmediata a publicar, conforme a lo previsto en el artículo 18 y siguientes de la Ley Orgánica 5/1992, de 29 de octubre, la modificación o creación de los ficherados de los que son responsables en orden a la previsión de cesiones a las Jefaturas Provinciales de Tráfico. Caso contrario, podrá procederse a la inmovilización de sus ficheros automatizados, según contempla el artículo 48 de dicho texto legal.

3.1.1.6. *Resoluciones relacionadas con la vulneración del deber de secreto y adopción de medidas de seguridad.*

Entre otras actuaciones de la APD en este ámbito de las Administraciones Públicas, merecen también destacarse las practicadas de oficio a raíz de ciertas noticias publicadas en un medio de comunicación, para analizar los procedimientos de destrucción de documentación por parte de diversos organismos de la Administración General del Estado, toda vez que dichos documentos con datos personales habían sido depositados en los cubos de basura de la vía pública sin las debidas condiciones de seguridad y con posible vulneración del deber de secreto a que están obligadas las Administraciones Públicas. Realizadas las correspondientes actuaciones de investigación, el Director de la Agencia acordó en dos de los casos el inicio de Procedimiento de Infracción de Administraciones Públicas y en los otros dos su archivo. Así:

* Se acordó el inicio de Procedimiento de Infracción de Administraciones Públicas a la Agencia Estatal de Administración Tributaria y al Instituto Nacional de la Seguridad Social por una posible infracción del artículo 10 de la Ley Orgánica 15/1999 y del artículo 9 de la misma norma, en relación con los artículos 4.2, 8.1 y 20 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, y de cuya Resolución se dará cuenta en la Memoria del próximo año.
* Por el contrario, se acordó el archivo de las actuaciones practicadas ante el Ministerio de Defensa y la Agencia Española de Cooperación Internacional del Ministerio de Asuntos Exteriores, ya que los documentos que incluían datos personales, estaban incluidos en fuentes accesibles al público, o correspondían a documentos que los propios afectados habían desechado sin haber procedido a la destrucción física de los mismos.

3.1.6. Actuaciones de colaboración con la CNIL.

Por último, merecen también destacarse una serie de actuaciones realizadas durante el año 2000 en ficheros de las Fuerzas y Cuerpos de Seguridad iniciadas a raíz de diferentes peticiones de colaboración realizadas por el Presidente de la Commission Nationale de L'Informatique et des Libertés (CNIL), autoridad competente en materia de protección de datos en Francia. Se recibieron en total siete solicitudes de colaboración al amparo del artículo 114.2 del Convenio de Schengen, en relación con peticiones de acceso a los ficheros del Sistema de Información Schengen (SIS) y, en su caso, de posible cancelación, sobre personas que figuran incluidas en el SIS como personas no admisibles en territorio Schengen y cuyos datos habían sido introducidos por las autoridades españolas.

Por ello, se iniciaron actuaciones para verificar si los datos de dichas personas habían sido incluidas correctamente al amparo de la legislación vigente. En todos los casos se inspeccionaron los ficheros y archivos de la Comisaría General de Extranjería y Documentación de la Dirección General de la Policía, comprobando que dichas personas habían sido expulsadas del territorio nacional en ejecución de una resolución judicial o administrativa, decretándose la prohibición de entrada en el país. En todos los casos investigados se informó a la CNIL de las actuaciones realizadas, así como del

motivo por el que figuraban dichas personas incluidas en el SIS.

3.2. ADMINISTRACIÓN AUTONÓMICA

Como puede observarse en el Gráfico VI de esta Memoria, han sido los procedimientos relacionados con la Administración autonómica los que más han aumentado en el año 2000. A continuación se destacan las Resoluciones del Director de la APD más relevantes dictadas durante dicho ejercicio, así como las actuaciones de inspección más significativas realizadas durante dicho ejercicio y de cuyo resultado final se dará cuenta en la Memoria del próximo año.

3.2.1. Resoluciones más relevantes del Director de la APD.

* De entre los procedimientos incoados a entidades de la Administración Autonómica cabe destacar catorce que han sido instruidos a otros tantos Institutos Nacionales de Bachillerato en virtud de la denuncia de un ciudadano, que ponía de manifiesto que en períodos próximos a la finalización de los distintos ciclos de estudios de sus hijos, se recibieron en su domicilio cartas remitidas por una Academia sin que hubiera facilitado los datos de su domicilio a dicha entidad. Por parte de la Inspección se comprobó que la Dirección General de Planificació i Centres de la Conselleria d'Educació, Cultura i Esports del Govern Balear redactó una carta, dirigida genéricamente a los directores de los centros educativos de las Islas Baleares, invitando a éstos a que facilitasen al portador de la misma los datos de los alumnos que cursasen segundo de Bachillerato o COU. Diversos Institutos de Educación Secundaria, a la vista del referido escrito, entregaron a dicha Academia sendos listados correspondientes a los cursos académicos 97/98 y 98/99, con los nombres, apellidos y dirección de los alumnos de 2§ de Bachillerato y COU, que fueron obtenidos del fichero que contiene los datos personales de los alumnos de cada Centro. La Agencia resolvió declarar que los diversos Institutos han infringido lo dispuesto en el artículo 11.1 de la LOPD, por facilitar los datos de carácter personal de sus alumnos a la citada Academia sin consentimiento de los afectados, lo que supone una infracción tipificada como muy grave en el artículo 43.4 b) de la citada norma.
* En este ejercicio se dictó también una resolución por infracción del articulo 11 de la Ley Orgánica 5/1992, tipificada como muy grave, a la Dirección General de Urbanismo y Vivienda de La Rioja por haber facilitado un listado conteniendo los datos del nombre, apellidos y dirección del arquitecto, dirección de la obra, número de viviendas y tipo de obra, presupuesto, nombre, apellidos y dirección de la propiedad, a una empresa dedicada a la edición de publicaciones en el ámbito de la construcción.
* Cabe destacar también el procedimiento instruido de oficio por la APD a la Consejería de Salud de la Junta de Andalucía por infracción del articulo 11, en relación con el 7.3. de la Ley Orgánica 5/1992, al que ya se hizo referencia en el apartado 3.1.1.5 anterior.
* En relación al Carnet Joven Euro < 26, se recibió una denuncia del Consejo de la Juventud del Principado de Asturias en la que se manifiesta que los jóvenes que solicitan dicho carnet no son informados de los derechos que les asisten de un modo preciso, expreso e inequívoco. En este caso se comprobó que el impreso de solicitud del Carné Joven Euro < 26 indica expresamente que los datos facilitados van a ser objeto de tratamiento automatizado por parte de una entidad bancaria y del Principado de Asturias para los fines propios del citado Carné, sujetos a la normativa de protección de datos. Por tanto, atendiendo a esta cláusula así como al contenido de los datos personales que se solicitan, se puede entender que la información que exige el artículo 5 de la LORTAD puede ser deducida, sin que se produzca un desconocimiento de los afectados respecto a los usos y finalidades que se van a dar a los datos proporcionados, así como que no existe duda sobre los responsables del tratamiento de dichos datos. Por ello se resolvió decretar el archivo de las actuaciones realizadas e instar al Principado de Asturias, Consejería de Cultura a que adopte las medidas necesarias para adecuar el impreso de solicitud del Carné Joven Euro < 26 a las prescripciones de la Ley, especificando el carácter obligatorio o facultativo de las respuestas, las consecuencias de la falta de respuesta a alguna de las preguntas y la dirección del responsable del fichero donde ejercitar los derechos de acceso, rectificación y cancelación.
* Por ultimo, cabe destacar la resolución de archivo de actuaciones de una investigación donde el denunciante solicita información acerca de si la resolución adoptada por la Comisión de Asistencia Jurídica Gratuita de la Generalitat Valenciana, que le denegó su solicitud de asistencia jurídica gratuita basándose, según aduce, en datos referentes a solicitudes efectuadas previamente por la interesada, resulta acorde con los dictados de la Ley Orgánica 5/1992. Asimismo, pone de manifiesto que en los ficheros de la Comisión de Asistencia Jurídica Gratuita de la Generalitat Valenciana existen datos suyos relativos a asuntos ya acabados y que no se le ha dado la oportunidad de comprobación, rectificación y cancelación. La resolución de archivo se fundamenta en La Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita, que determina en su artículo 9: "*En cada capital de provincia, en las ciudades de Ceuta y Melilla y en cada isla en que existan uno o más partidos judiciales, se constituirá una Comisión de Asistencia Jurídica Gratuita, como órgano responsable, en su correspondiente ámbito territorial, de efectuar el reconocimiento del derecho regulado en la presente Ley* ". El artículo 17 de la citada norma determina: *"Para verificar la exactitud y realidad de los datos económicos declarados por el solicitante del derecho a la asistencia jurídica gratuita, la Comisión podrá realizar las comprobaciones y recabar la información que estime necesarias. (...)",* y en su artículo 20 se especifica *que el estudio de las impugnaciones que se realicen contra las resoluciones de la Comisión corresponde a los Juzgados o Tribunales competentes* , por lo que la Agencia de Protección de Datos carece de competencia para conocer sobre la procedencia o improcedencia de las resoluciones de la Comisión.
En cuanto a la cancelación de los datos existentes en los ficheros de la Comisión, el artículo 4.5 de la Ley Orgánica 15/1999, en su primer párrafo señala: *"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados* ". Señalando el artículo 16. 5 de aquélla: "*Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado* ". En este sentido, el artículo 13 del Decreto 299/1997, del Gobierno Valenciano, de asistencia jurídica gratuita, señala la reiteración manifiestamente abusiva como uno de los criterios a tener en cuenta en la evaluación de una solicitud de asistencia jurídica gratuita, lo que implica la necesidad de conservar los datos relativos a solicitudes

anteriores al objeto de determinar si existe reiteración en las posteriores solicitudes que se formulan y, en su caso, poder calificar dicha reiteración como manifiestamente abusiva, por lo que al no encontrarse vulneración alguna de la legislación sobre protección de datos se decretó el archivo de las actuaciones.

3.2.1. Actuaciones de Inspección más relevantes

Durante el ejercicio 2000 se han tramitado por parte de la Inspección de Datos doce actuaciones previas de investigación relacionadas con el posible incumpliendo de lo establecido en la Ley Orgánica 15/1999 por parte de los responsables de ficheros pertenecientes al ámbito de las Comunidades Autónomas o áreas de su competencia. De estas actuaciones, once de ellas han sido por cesión de datos de los ciudadanos recogidos por la Administración Autonómica correspondiente en virtud de sus competencias y cedidos a otras entidades públicas o privadas. Unicamente una de las actuaciones se refería al ejercicio del derecho de los ciudadanos al acceso, rectificación y cancelación de sus datos.

* De entre estas actuaciones de investigación cabe destacar las iniciadas a distintos Departamentos de la Generalitat de Catalunya por el contrato suscrito con una entidad médica para realizar un seguimiento y control de las bajas por enfermedad de sus empleados. Para realizar este seguimiento, la Generalitat comunica a la empresa médica los datos personales de sus funcionarios y trabajadores sin contar con su consentimiento, incluidas las fechas de alta y baja. Tales datos provienen del fichero automatizado del Sistema de Información de Personal. El personal médico de la empresa visitaba a las personas solicitadas y como resultado de la misma elaboraba un informe médico en el que se recogía el diagnostico médico de la enfermedad que padecía el trabajador. Estos informes se almacenaban en un fichero con el dato de diagnóstico de forma codificada. En el Sistema de Información de Personal de la Generalitat no constaban los datos de diagnóstico que ocasionan la baja del trabajador. A la vista del resultado de las actuaciones previa se procedió a iniciar procedimientos de infracción de administraciones públicas a un Departamento en concreto de la Generalitat así como el correlativo procedimiento sancionador a la empresa encargada de la visita médica, procedimientos que están pendientes de Resolución al final del ejercicio, por lo que se dará razón de ellos en la Memoria correspondiente al año 2001.
* En otro caso, como consecuencia de la publicación en un diario local de una noticia relativa a la entrega por parte del Centro de Salud Cartagena Casco Antiguo de citaciones médicas a pacientes, en las que en el reverso figuraban listados con datos de otros enfermos que habían pasado por el mismo Centro, se abrieron actuaciones de inspección al objeto del esclarecimiento de los hechos.

Tras la realización de las oportunas actuaciones de inspección, se obtuvieron las siguientes conclusiones:

El citado Centro de Salud llevaba utilizando durante al menos dos años las hojas con listados que contenían la relación de pacientes diarios citados para la realización de extracciones de sangre.

En el reverso de dichas hojas se ha estado fotocopiando una preimpresión, incluyendo la información necesaria para confeccionar dos nuevas hojas de cita. Una vez cortadas por la mitad, eran cumplimentadas manualmente para entregar a los pacientes con los datos relativos a la nueva cita asignada, pero constando en el anverso la relación de pacientes citados para la extracción de sangre.

Este hecho supone una vulneración del deber de secreto de los datos de los pacientes del Centro de Salud, si bien hay que señalar que no se han dado datos de salud de los pacientes citados, ya que únicamente aparecía junto al nombre del paciente un número identificador que sólo utilizaban y conocían los profesionales sanitarios del mismo.

Se ha producido por tanto, un incumplimiento del deber de secreto establecido en el art. 10 de la Ley Orgánica 15/1999, que dio lugar a la apertura de Procedimiento de Administraciones Públicas, y de cuya Resolución se informará en la próxima Memoria.

3.3. ADMINISTRACIÓN LOCAL

Durante el ejercicio 2000 la Agencia de Protección de Datos ha tramitado diversos expedientes relacionados con la Administración local que han dado lugar a Resoluciones de archivo, en unos casos, y, en otros, a las correspondientes Resoluciones de procedimientos por infracción de Administraciones Públicas. De unas y otras, cabe destacar como más significativas las siguientes: 3.3.1. Resoluciones más relevantes del Director de la APD

* Dentro de los procedimientos de infracción de Administraciones públicas en el ámbito local se han dictado cinco resoluciones sancionadoras entre las que cabe destacar las referentes a dos Ayuntamientos: Ayuntamiento de Denia (Alicante) y Ayuntamiento de Calonge (Girona), por la cesión de los datos de carácter personal de diversas personas físicas: promotores, arquitectos, aparejadores, propietarios y contratistas de obra, a una empresa cuya actividad se centra en la edición de publicaciones técnicas profesionales dirigidas al sector de la construcción. En ambos casos la resolución dictada declara que se ha infringido lo dispuesto en el artículo 11 de la LORTAD, por ceder datos a la citada empresa, lo que supone una infracción tipificada como muy grave en el articulo 43.4 b) de la citada norma.
* Otra de las resoluciones recaídas en este ejercicio fue instruida al Ayuntamiento de Palma de Mallorca, el cual adoptó el Acuerdo de *aprobar la modalidad de procedimiento descentralizado para la solicitud y expedición de certificados de residencia al efecto de bonificaciones en las tarifas de transporte.*

El virtud del citado Acuerdo el Ayuntamiento de Palma de Mallorca firmó contratos de adhesión con dos entidades bancarias para la solicitud y emisión de certificados de residencia, con la finalidad de conceder bonificaciones en las tarifas del transporte regular aéreo y marítimo, emitiéndose dichos certificados a través de las correspondientes redes

de cajeros automáticos de las entidades bancarias. Asimismo, el Ayuntamiento firmó un contrato de adhesión con una Agrupación Empresarial de Agencias de Viaje con objeto de que se pudieran solicitar y emitir los certificados de residencia a través de sus Agencias. Para la obtención del certificado el interesado debería teclear el número de DNI o el Número de Tarjeta de residencia visualizándose los nombres, DNI o número de residencia y fecha de nacimiento (en el caso de menores), no sólo del interesado, sino también de todas las personas incluidas en una misma hoja padronal. En este procedimiento se resolvió declarar que el Ayuntamiento ha infringido el articulo 11 de la LORTAD.

* En relación al artículo 10 de la LORTAD, la Agencia de Protección de Datos dictó una resolución de infracción grave por vulneración del deber de secreto al Ayuntamiento de Puente Genil (Cordoba) responsable de la gestión, liquidación e inspección tributaria referente al Impuesto de Actividades Económicas por emitir, a través de la empresa encargada de la recaudación, un informe sobre la liquidación de I.A.E. de un ciudadano, que fue entregado a tercera persona sin conocimiento ni consentimiento del titular.
* Finalmente, cabe destacar la Resolución por infracción del articulo 4.2. de la Ley Orgánica 5/1992 en la que incurre el Ayuntamiento de Sancti-Spiritus (Badajoz) por la utilización del Censo Electoral y de las renovaciones del Documento Nacional de Identidad, para una finalidad distinta de aquella para la que fue recogida. En este sentido, tanto la LOREG como la LORTAD inhabilitan al Censo Electoral como fuente de acceso público. Así la propia Ley Orgánica del Régimen Electoral General establece en su párrafo 2 que "*queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial".* Este mismo criterio mantiene la Sección Novena de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, en la sentencia del recurso número 1421/95, en cuyo Fundamento de Derecho Sexto señala: *"Resulta en definitiva que se encuentra prohibida la información particularizada sobre los datos censales pues aunque el destinatario de tal prohibición sea la Oficina del Censo Electoral pone de manifiesto la voluntad del legislador de excluir del carácter de accesible al público tal información y que la exposición al público tiene como destinatario al interesado a los solos efectos de formular reclamaciones y asimismo que cuando se permite la obtención de copia de los datos resulta restringido el destinatario a los mismos y la finalidad de la de la utilización."*

3.3.2. Resoluciones de archivo.

* La mayor parte de las Resoluciones de Archivo derivan de expedientes incoados por cesión de datos personales a entidades públicas o privadas. En estos casos, la cesión se había producido en forma no automatizada. Así, la Diputación Provincial de León, con motivo de la acogida temporal de niños saharauis, envió un listado con datos personales de las familias de acogida a la delegación del Pueblo Saharaui en Castilla-León, que a su vez lo remitió a dos O.N.G. En todos los casos, se comprobó por parte de la Inspección de la Agencia que esta información no estaba contenida en ningún fichero automatizado, por lo que no se apreció en estos casos ninguna vulneración de la Ley Orgánica 5/1992, de 29 de octubre, Ley vigente en el momento en que se produjeron los hechos.
* Una situación similar se produjo con la cesión de los datos personales de un afectado que el Ayuntamiento de Barberá del Vallés (Barcelona) proporcionó a una asociación teatral, sin el consentimiento de aquél. Dicha comunicación se realizó de forma manual sin utilización o tratamiento con medios informáticos, por lo que la cuestión quedaba también fuera del ámbito de aplicación de la LORTAD.
* Otro de los Archivos de Actuaciones se realizó sobre una denuncia de un ciudadano que ponía de manifiesto que el Departamento de Hacienda y Finanzas de la Diputación Foral de Bizkaia había dado traslado de sus datos a la Agencia Estatal de Administración Tributaria,, existiendo entre dichos datos, datos especialmente protegidos relativos a la creencia religiosa y datos de salud. Sin embargo, no se apreció vulneración a la Ley Orgánica 5/1992, ya que al no quedar suficientemente acreditada la residencia fiscal del afectado en el territorio histórico de Bizkaia se había remitido su declaración a la Agencia Estatal de Administración Tributaria, situación prevista en el articulo 113 de la Ley General Tributaria.
* Otra de las resoluciones guarda relación con la denominada tarjeta ciudadana. La Agencia ha procedido al archivo de estas actuaciones en el caso del Ayuntamiento de Palma de Mallorca, denunciado por cesión de los datos de los solicitantes a dos entidades bancarias con las que había suscrito un Convenio, toda vez que el consentimiento se deriva de la solicitud del propio interesado. Sin embargo, entre las funciones establecidas en el citado Convenio estaba la emisión de las tarjetas por tales entidades bancarias, las cuales procedían a la destrucción del fichero enviado por el Ayuntamiento una vez realizada la estampación. Asimismo, no se hallaron evidencias de que los datos personales de los solicitantes de la citada tarjeta se hubieran utilizado por parte de las entidades financieras emisoras de la misma para finalidades distintas de las especificadas en el Convenio, por lo que también se decretó el archivo de actuaciones.
* Otra de las actuaciones que también finalizó con un archivo se refiere a la vulneración de deber de secreto por parte del Ayuntamiento de Sevilla, el cual fue denunciado al aparecer en diversos diarios datos sobre contribuyentes que mantenían impagos de distintos tributos. La inspección comprobó que los datos personales aparecidos en los medios de comunición habían sido publicados en diferentes Boletines Oficiales (fuente de acceso público) a excepción de uno de los afectados que no aparecía en dichos boletines. Sin embargo, respecto a este último (al igual que los demás), no se pudo acreditar en la inspección practicada que la publicación de los datos en los medios de comunicación se debiera al citado Ayuntamiento.
* Por último, una denuncia que culminó también en el archivo de actuaciones fue debida a la remisión, por parte del Ayuntamiento de Coslada (Madrid), de un certificado de empadronamiento a otra persona utilizando para ello una autorización supuestamente firmada por la denunciante. En este caso el Ayuntamiento acreditó que la emisión del certificado de empadronamiento fue conforme a las normas establecidas al efecto.

4. ACTUACIONES MÁS RELEVANTES EN EL ÁMBITO DE LOS FICHEROS DE TITULARIDAD PRIVADA

En el ámbito de los ficheros de titularidad privada las más significativas Resoluciones dictadas durante el año 2000 afectan a los siguientes sectores:

4.1. TRATAMIENTOS DE DATOS PERSONALES EN LOS SERVICIOS DE TELECOMUNICACIONES.

La Agencia de Protección de Datos ha seguido recibiendo durante el año 2000 diversas denuncias acerca de tratamientos realizados por operadores de telecomunicaciones con los datos de sus clientes. A continuación se destacan las más significativas indicando las materias a las que afectan y resumiento algunas de las conclusiones dictadas: 4.1.1. Tratamiento de datos sin consentimiento.

* Un ciudadano formuló una denuncia contra una entidad bancaria por remitirle esta última un envío publicitario con objeto de captarle como cliente sin disponer del consentimiento del afectado .
* Un expediente se origina como consecuencia de una denuncia en la que la persona afectada se queja de que tras haber solicitado la rescisión del contrato de abono que mantenía con un operador de telecomunicaciones y la cancelación de sus datos personales, recibió, con posterioridad a dicha solicitud, un envío publicitario remitido por el mencionado operador.

Este hecho dio lugar a las correspondientes actuaciones en las que se constató que efectivamente la persona afectada había solicitado la baja del servicio. De hecho, la baja fue solicitada por dos vías diferentes, una a través del distribuidor con quien el afectado contrató el servicio y otra directamente con el operador de telecomunicaciones, siendo únicamente en ésta última en la que se solicitaba la cancelación de los datos personales.

También se constató que efectivamente el operador remitió publicidad al denunciante con posterioridad a la recepción de la solicitud de cancelación

La LORTAD, en su articulo 6 " Consentimiento del afectado", dispone que:

"1.El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado salvo que la Ley disponga otra cosa.

2. *No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al publico, cuando se recojan para el ejercicio de las funciones propias de las Administraciones publicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato"*

En el presente caso, el operador no contaba con el consentimiento para tratar los datos del denunciante, después de que éste haya pedido la cancelación de los mismos, y es evidente que dichos datos no proceden de una fuente accesible al publico sino que provienen de la relación contractual con su cliente.

Por lo anteriormente expuesto se sancionó al operador por una infracción del artículo 6.1 de la Ley Orgánica 5/1992 tipificada como grave en dicha Ley. 4.1.2. Calidad de datos.

* Un cliente de un operador de telefonía móvil disponía de un plan de precios que consistía en un prepago de una serie de minutos de consumo, de tal forma que, nada más producirse el alta, se cargaba en la cuenta del cliente un importe fijo del que se iba detrayendo el consumo, repitiéndose la recarga por el importe fijo cada seis meses. Si llegados los seis meses el cliente no había agotado el crédito, el importe fijo de la recarga se acumulaba al crédito no consumido. Si, por el contrario, el cliente consumía el crédito con anterioridad al transcurso de los seis meses, se le facturaban los minutos de consumo de acuerdo con las tarifas aplicables en el plan de precios preestablecido.

En el caso del denunciado, en uno de los periodos de facturación el importe consumido excedió del importe de crédito por lo que la factura correspondiente incluyó además del importe fijo del crédito correspondiente al periodo de facturación siguiente, el importe de las llamadas realizadas en exceso. Esta factura no fue pagada por el cliente ya que discrepaba con la misma, lo que provocó que el operador incluyera el importe global de la factura como una incidencia de impago del cliente en un fichero de incumplimiento de obligaciones dinerarias.

Posteriormente, el operador emite una nueva factura en sustitución de la anterior, en la que descuenta el importe de la recarga automática, manteniendo únicamente el importe del exceso de consumo. Sin embargo, no actualiza el valor de la deuda que dio de alta en el fichero de incumplimiento de obligaciones dinerarias, que permanece por valor del importe de la primera factura hasta que el cliente abona la segunda factura, momento en el cual se modifica el valor de la deuda a cero pesetas.

Según resuelve el Director de la Agencia, el valor de la deuda comunicada al fichero de incumplimiento de obligaciones dinerarias debería haber sido actualizado al valor por el que se emite la segunda factura. Este hecho vulnera el artículo 4.3 de la Ley Orgánica 5/1992 que establece los datos de carácter personal *"...*

serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado", por lo que fue sancionado con una falta leve según el artículo 43.2 c) de la misma Ley. 4.1.3. Cumplimiento de la normativa específica de protección de datos en el sector de las telecomunicaciones.

En la memoria de 1999 se informó acerca de las actuaciones iniciadas como consecuencia de una denuncia que hacía referencia al cumplimiento de diferentes artículos del Real Decreto 1736/98, por el que se regulan diversos aspectos de

la protección de datos en el sector de las telecomunicaciones. En concreto, se denunciaban los siguientes aspectos:

* Que el operador no haya accedido a su petición consistente en la presentación de la identificación de la línea llamante (la denunciante se apoya en la Directiva 97/66/CE y en la Disposición Transitoria Novena del RD 1736/98).
* Que el operador no ha accedido a su petición consistente en rechazar las llamadas procedentes de usuarios o abonados que hayan suprimido la presentación de la línea llamante (art. 74 RD 1736/98 y Directiva 97/66/CE).
* Que el operador tampoco ha accedido a su petición consistente en rechazar las llamadas no solicitadas con fines de venta directa (art.68 RD 1736/98 y art. 12 de la Directiva 97/66/CE).
* Que el operador no le ha proporcionado el servicio consistente en la facilidad de identificación de la línea llamante en los mensajes de depósito del servicio contestador, del cual la denunciante es una abonada.
* Que el operador no le ha proporcionado el servicio consistente en establecer un procedimiento para poner fin al desvío automático de llamadas a su terminal por parte de un tercero (art. 10 de la Directiva 97/66/CE y art. 80 del RD 1736/1998).

A la vista de esta denuncia se iniciaron actuaciones previas al objeto de estudiar el alcance de los hechos denunciados, actuaciones que culminaron en el año 2000 con el archivo de las actuaciones por parte del Director de la Agencia por las siguientes razones:

De las actuaciones practicadas se ha constatado que el operador no cumple con el deber de prestar determinados servicios a que está obligado conforme a los arts. 62 a 80 del mencionado Real Decreto 1736/1998. Ello supone la infracción de una disposición reglamentaria cuya tipificación está prevista genéricamente en el art. 43.3.d) de la Ley Orgánica 15/1999 (vertiente material del principio de legalidad). Sin embargo, para que pueda apreciarse una infracción será preciso que concurra, además, el elemento formal del principio de legalidad (reserva de ley). Es decir, será preciso que se produzca una conducta concreta del operador que suponiendo un incumplimiento de los preceptos de protección de datos contemplados en el Real Decreto 1736/1998, implique, además, una vulneración de los principios o derechos reconocidos en la LOPD, incurriendo así en alguna de las infracciones tipificadas en dicha norma.

Así resultaría, por ejemplo, si solicitado por un abonado la prestación de un determinado servicio a que el operador viene obligado por el mencionado R.D. 1736/1998, éste no lo prestase. Produciéndose en este caso un tratamiento de datos por la operadora, conforme a la definición que de tratamiento da el art. 3.c) de la Ley Orgánica 15/1999, y no contando dicho tratamiento con el consentimiento del afectado por la evidente manifestación de éste contraria a dicho tratamiento, se estaría conculcando su derecho a la autodeterminación informativa, lo que daría lugar a la correspondiente sanción al concurrir en este caso la doble vertiente de la legalidad formal y material. Lo mismo sucedería si el afectado/abonado ejercitara alguno de los derechos que le atribuye la Ley Orgánica 15/1999, y en particular el derecho de oposición, en cualquiera de las formulaciones que de tales derechos contempla el Título V del Real Decreto 1736/1998, y el operador no garantizara o no permitiera su ejercicio, pues también en este caso concurriría la doble vertiente del principio de legalidad al incurrir en una infracción de la propia Ley Orgánica 15/1999, cuya modulación en el sector de las telecomunicaciones ha sido desarrollada en el Título V del citado Real Decreto.

En los escritos de la denunciante se solicita al operador la prestación de determinados servicios previstos en el Real Decreto 1736/98. Respecto a algunos de ellos la denunciante ya ha obtenido el servicio solicitado; respecto a otros existe una imposibilidad presente de prestación del servicio (sujeción a un calendario que ha de establecer el Ministerio de Fomento); y en otro se hace referencia a la prestación de un servicio no recogido en la normativa de protección de datos. Los hechos denunciados tuvieron lugar durante la vigencia de la derogada Ley Orgánica 5/1992, de 29 de octubre, donde no se regulaba el derecho de oposición, a diferencia de la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no precediendo estimar la reclamación de la denunciante.

4.2 TRATAMIENTO DE DATOS PERSONALES EN EL ENTORNO DE INTERNET

Durante el año 2000 fueron muy numerosas las actuaciones de inspección realizadas en relación con actividades desarrolladas en el seno de Internet, que en muchos casos se iniciaron como consecuencia de las denuncias presentadas por los ciudadanos, cada vez más preocupados por la incidencia que la Red puede tener en la protección de su propia intimidad. En este sentido, el objeto de las denuncias versaba sobre la publicación indebida de datos personales, la remisión de mensajes a través del correo electrónico o la utilización de los datos recabados por Internet para finalidades distintas a la que ocasionó su recogida.

A continuación, se destacan por su relevancia algunos de los procedimientos tramitados que, aunque de carácter bien distinto, tienen en común la plataforma a través de la cual se realiza la actividad que dio lugar a su inicio: internet.

4.2.1.Participantes en el casting del programa televisivo "*Gran Hermano* " En el verano de 2000 el Director de la Agencia ordenó a la Subdirección General de Inspección de Datos la realización de diligencias para el esclarecimiento de ciertos hechos divulgados por los medios de comunicación, relativos a la publicación a través de Internet de un fichero con datos sobre personas que habían participado en el casting del programa de televisión "*Gran Hermano* ". Una vez realizadas las pertinentes actuaciones previas en averiguación de los hechos, el Director de la Agencia acordó incoar Procedimiento Sancionador a la productora del programa.

Durante la tramitación de este procedimiento quedó acreditado que en el proceso de selección de participantes en el programa televisivo una entidad especializada en labores de atención telefónica se había encargado de recoger en un fichero datos identificativos de los interesados. Al ser la productora del programa la beneficiaria de dicho fichero y teniendo en cuenta que la recogida de los datos se había realizado por encargo de la misma, se la consideró como

responsable del fichero o tratamiento, de conformidad con el artículo 3 d) de la Ley Orgánica 15/1999, incumbiéndole también en consecuencia el cumplimiento de la obligación establecida en el artículo 5 de la citada Ley.

Teniendo como base el fichero elaborado por esa compañía colaboradora, la productora llamaba telefónicamente a los participantes para convocarles a un casting, que se realizó en diversas poblaciones del territorio español en función de la localización geográfica del participante. En este casting se les sometió a una prueba de cámara/imagen y a una serie de tests sobre *Hábitos y Preferencias, Personalidad Propia* y *de la Personalidad de la Pareja Ideal* , incluyendo algunos de ellos una hoja de respuestas para su lectura mecánica. La productora tampoco proporcionó a los afectados, en ese momento, ninguna información de la prevista en el artículo 5 de la LOPD.

Igualmente, a partir de los resultados obtenidos en la fase anterior, la productora y un gabinete de psicólogos convocaron nuevamente a unos 200 seleccionados con objeto de someterles a una nueva prueba de cámara/imagen y a un nuevo test de inteligencia y psicopatías, que contenía también dos hojas de respuestas para lectura mecánica. En esta fase posterior, tampoco se informó a los afectados de los requisitos exigidos legalmente.

Finalmente, la productora sometió a las últimas 17 personas finalistas a un test de 100 preguntas diversas, sin proporcionar tampoco la información a que estaba obligada conforme a lo previsto en el precitado artículo 5 de la Ley.

La productora manifestó en su descargo que se le imputaba la falta de información en la recogida de los datos, cuando realmente la entidad que recogió los datos había sido otra, por lo que no podía imputársele esta infracción dado que en caso contrario se vulneraría el principio de responsabilidad y el de exigibilidad de culpa, añadiendo además que durante la celebración del casting fueron los propios concursantes los que ofrecieron voluntariamente sus datos personales y conocían la finalidad del mismo. Sin embargo, como se ha señalado antes, no sólo se le imputaba la falta de información en la primera recogida de datos, sino también en las posteriores recogidas, en las que precisamente se recababan los datos más sensibles de todo el proceso de selección. No basta con que los concursantes sepan la finalidad de la recogida, puesto que la información que debe proporcionárseles es mucho más amplia: derechos de acceso, rectificación y cancelación, responsable del fichero y cesionarios de los datos. Cualquier desconocimiento o incumplimiento por parte del responsable del fichero de estos aspectos esenciales de la posición jurídica del afectado constituye una clara infracción de un derecho fundamental, y lo cierto es que ninguna de estas informaciones le fue facilitada a los concursantes, de manera que poco o nada sabían sobre el tratamiento posterior de sus datos o sobre las conclusiones que se iban a extraer de las respuestas proporcionadas como consecuencia de las preguntas formuladas o sobre los perfiles de personalidad que se iban a realizar sobre ellos. En cualquier caso, lo previsto en los apartados a) y e) del transcrito art. 5 son siempre de obligada información a los interesados de conformidad con lo dispuesto en el apartado 3 de dicho artículo, sin que quepa su exclusión por el hecho de que los datos sean dados voluntariamente por los interesados y conociendo su finalidad.

En consecuencia, se consideró acreditada la comisión de la infracción prevista en el artículo 5 de la LOPD por parte de la productora, en la que interviene el elemento subjetivo de la culpabilidad al ser responsable directo del fichero creado al efecto y al haber participado directamente en la recogida de los datos en diversas fases del proceso de selección, sin vulnerarse, en consecuencia, el principio de responsabilidad consagrado en el art. 130 de la Ley 30/1992, de 26 de noviembre, por el hecho de imputarle la tantas veces citada infracción.

La segunda imputación fue la relativa al tratamiento de datos sensibles sin consentimiento.

En el momento de la primera Inspección realizada en sus locales, la productora tenía en su poder en formato automatizado las respuestas de los concursantes correspondientes a algunos de los cuestionarios. En uno de ellos se hace constar los siguientes datos: *apellidos y nombre, sexo, provincia, DNI, cuestiones relacionadas con la familia y relaciones de amistad, aspecto físico, procedencia, aficiones y costumbres propias y de la pareja ideal*, *incluyendo orientación política y personalidad religiosa* . Y en una segunda Inspección, se encontraron en poder de la productora, además de los cuestionarios precitados otros incluyendo: *cuestionarios de hábitos y preferencias, cuestionario de personalidad propia, cuestionario de personalidad de la pareja ideal y cuestionario para foto y vídeo* , todos ellos cumplimentados con datos de carácter personal y con un apartado para *observaciones del redactor* , rellenado a mano, conteniendo comentarios subjetivos, sobre la apariencia física, psíquica o de comportamiento de quien rellenaba los cuestionarios. Por otra parte, resultó acreditado también que la productora había tratado datos especialmente protegidos, como son los datos de salud mental de los participantes en el proceso de selección. Cabe resaltar en este punto, que el contrato suscrito entre dicha entidad y el gabinete de psicólogos con el que colaboró disponía en su clausulado que no se procederá al tratamiento de datos especialmente sensibles relativos al origen racial, las creencias religiosas, la vida sexual, afiliación sindical o ideología, y sin embargo se omitía la referencia a los datos de salud, que precisamente han sido los datos tratados, independientemente de que también se han tratado datos de orientación política y personalidad religiosa.

A este respecto la productora alegó que los interesados habían llamado voluntariamente a un número de teléfono en el que se les informó de que se les iba a realizar un casting y unos test y que rellenaron personalmente los cuestionarios que contenían datos, por lo que tienen su consentimiento para el tratamiento de los mismos. Sin embargo, no es suficiente que los interesados sepan que van a rellenar un test sobre psicopatías o hábitos de consumo. Es necesario que al solicitar y tratar automatizadamente datos especialmente protegidos, como son los datos de salud mental, los afectados consientan expresamente el tratamiento de los mismos, tal y como exige el artículo 7.3 de la Ley Orgánica 15/1999. No es válido el mero supuesto consentimiento tácito para el tratamiento de este tipo de datos. La productora no aportó al procedimiento, a pesar de las numerosas ocasiones que tuvo para ello, los consentimientos expresos de los afectados para ese tipo de tratamientos. Tampoco se les había explicado a los concursantes que esos tratamientos de datos fueran necesarios para participar en el concurso. Es evidente que los concursantes habían rellenado volunta-

riamente los test y cuestionarios que se les habían presentado. Pero ello no exime a la productora de cumplir con la obligaciones que la normativa sobre protección de datos personales le impone, pues una cosa es dar el consentimiento para concurrir a un concurso y otra es dar el consentimiento para que sus datos sean tratados automatizadamente. De aquí que la Ley Orgánica 15/1999 defina el "consentimiento del interesado" en su art. 3 h) como: "*Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen* ", lo que supone que no cabe el consentimiento "presunto".

Por todo ello, los concursantes debían estar suficientemente informados de que sus datos personales iban a ser objeto de tratamiento automatizado, del destino final de sus datos, y de los perfiles a todos los niveles que se han hecho de sus respectivas personalidades. Sólo así podría considerarse que han dado su consentimiento informado de manera inequívoca y específica para que sus datos personales fueran objeto de tratamiento y ello con independencia de que hayan rellenado los cuestionarios voluntariamente.

Este criterio ya había sido confirmado por la Audiencia Nacional en su Sentencia de 14 de abril de 2000 que señala: " *Tampoco puede admitirse (...) la existencia de un consentimiento tácito o un impropiamente llamado silencio positivo del afectado para admitir la cesión de sus datos, pues tal forma de obtener el consentimiento requeriría, en la mejor de las hipótesis, una rigurosa constancia documental de que la entidad cedente había informado y conservaba el escrito, con constancia de la recepción por el interesado, en el que tales extremos quedaban claramente expuestos* ". (F.D. SEXTO *in fine*).

Por todo lo anterior, se consideró cometida la infracción del articulo 6, en relación con el 7.3, de la Ley Orgánica 15/1999, por parte de la productora.

Se le imputó, igualmente, a la precitada entidad la comisión de la infracción del artículo 11 de la Ley Orgánica 15/1999. En este sentido, se comprobó durante la tramitación del procedimiento sancionador que, haciendo uso del fichero elaborado a partir de las respuestas telefónicas recabadas por la primera compañía colaboradora, un gabinete de psicólogos se encargó de seleccionar 2.681 personas. Sin embargo, en realidad estas personas fueron tipificadas por otro psicólogo ajeno a ambas entidades, a partir de los datos que le fueron remitidos por la productora. Igualmente, se acreditó que los tests sobre los diversos *Cuestionarios,* también fueron entregados por la productora a un sociólogo para su lectura mecánica.

Estas dos cesiones de datos, contrastadas durante el procedimiento sancionador, no contaban con el consentimiento de los afectados, entre otras razones porque incluso éstos desconocían que se iban a producir. A la vista de lo anterior, y dado que no era aplicable ninguna de las excepciones previstas legalmente en el art. 11.2 de la LOPD para considerar validas las cesiones de datos producidas, se entendió que la productora había cometido la infracción del citado artículo.

Alegaba en su descargo la productora que no existía cesión de datos, ya que había un contrato de prestación de servicios con el gabinete de psicólogos, amparada en el artículo 12 de la Ley Orgánica 15/1999. Adicionalmente argumentó que el artículo 11 del mismo texto legal prevé como cesiones legales las que cuenten con el consentimiento de los afectados y, según la productora, éstos rellenaron voluntariamente los cuestionarios formulados por el gabinete de psicólogos. Igualmente, alegaba que la remisión de datos al psicólogo y sociólogo anteriormente citados se había hecho teniendo en cuenta que eran miembros del gabinete de psicólogos, no teniendo conocimiento de que existieran facturas por servicios prestados giradas por el gabinete a dichas personas.

Según la Resolución, para que exista una prestación de servicios - encuadrable dentro del actual artículo 12 de la LOPD - deben darse los siguientes requisitos: la existencia de un contrato por escrito, o en alguna otra forma que permita tener constancia de su celebración y contenido; la constatación en el mismo de que el encargado del tratamiento no utilizará los datos para otras finalidades distintas a las que figuren en el contrato ni los comunicará a otras personas; y las estipulaciones contractuales sobre las medidas de seguridad que el encargado del tratamiento está obligado a implementar. En el presente caso existía, como alegó la productora, un contrato suscrito entre dicha entidad y el gabinete de psicólogos. Analizado detenidamente dicho contrato se observa que es un contrato mercantil de arrendamiento de servicios y que el gabinete de psicólogos asume la responsabilidad de selección, monitorización e intervención en el programa de televisión *BIG BROTHER* , durante un período de 180 días dividido en dos fases diferenciadas, cada una siguiendo su propia metodología. Sin embargo, dicho contrato no contenía estipulación alguna sobre las medidas de seguridad que se deberán adoptar para la protección de los datos personales de los concursantes. Tampoco contenía ninguna cláusula acerca de que el encargado del tratamiento no utilizará los datos para otras finalidades distintas a las que figuren en el contrato, ni los comunicará a otras personas. Por tanto, no podía considerarse un contrato válido encuadrable dentro de los contratos de prestación de servicios que prevé el artículo 12 de la Ley Orgánica 15/1999.

Pero, a mayor abundamiento, las cesiones o comunicaciones de los datos de los concursantes efectuadas al psicólogo y al sociólogo anteriormente citados ni siquiera estaban regidas por un contrato escrito, ni existían suficientes elementos que permitiesen presumir su existencia. Simplemente se había producido la entrega de datos sin ningún tipo de garantía respecto a su tratamiento, o a posibles cesiones posteriores o a su confidencialidad. No existiendo contrato, no es aplicable pues el artículo 12 de la LOPD, por lo que no se podía admitir que existiese un contrato de prestación de servicios válido, habiéndose producido en consecuencia una cesión de datos inconsentida.

Finalmente, alegaba también la imputada que el art. 12 de la nueva Ley Orgánica 15/1999 viene a contemplar dos tipos de contratos distintos: Uno, en el apartado 1 del art. 12, consistente en la prestación por un tercero de un servicio, cualquiera que sea la naturaleza de éste; y otro, en el apartado 2 del mismo art. 12, que es el que se circunscribe a la

prestación del servicio de realización de "tratamientos" por cuenta de terceros (o contrato de "outsourcing"). Con base en esta distinción alegaba la imputada que el legislador con el apartado 1 del susodicho art. 12 pretende excluir de la figura de la comunicación de datos el supuesto de que un tercero tenga acceso a los datos, por ser dicho acceso necesario para la prestación de un servicio - sea cualquiera la naturaleza de éste - al responsable del tratamiento. Con base en esta distinción y argumento, la alegante manifestaba que el contrato entre la productora y el gabinete de psicólogos se incardinaba en cualquier caso en dicho apartado 1 y, por lo tanto, amparaba la cesión o comunicación de datos que la primera entidad hace a la segunda.

Esta alegación tampoco puede admitirse por carecer de una fundamentación jurídica mínimamente coherente con la naturaleza de la protección otorgada por el art. 18.4 CE y, en su desarrollo, por la Ley Orgánica 15/1999, al tratamiento y cesión de los datos personales, en definitiva, a la protección de un derecho fundamental. En efecto, el art. 12 de la Ley regula un único contrato de prestación de servicios de tratamiento de datos por cuenta de terceros (el responsable del fichero o tratamiento) y para ello la Ley exige un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido, así como el cumplimiento de los demás requisitos especificados en su apartado 2; y en ningún caso está regulando dos contratos distintos, uno de los cuales (el del apartado 1 del art. 12) permitiría la comunicación de datos *inter partes* sin cumplir necesariamente con todos los requisitos del apartado 2 del mismo artículo, como pretende la alegante.

Igualmente, se imputaba a la productora la infracción consistente en no haber adoptado las medidas de seguridad pertinentes y suficientes respecto a los ficheros automatizados creados conteniendo datos de carácter personal. Estas medidas consisten, de conformidad con lo dispuesto en los artículos 8 a 14 del Reglamento de Medidas de Seguridad, aprobado mediante Real Decreto 994/1999, de 11 de junio, en la elaboración de un Documento de Seguridad que especifique el ámbito de aplicación del mismo, las medidas y procedimientos encaminados a garantizar el nivel de seguridad exigido, las funciones y obligaciones del personal, el registro de incidencias, la identificación y autenticación de usuarios, el control de acceso de usuarios, la gestión de soportes o identificación de la información que contiene y la posibilidad de crear copias de respaldo y de recuperación.

La productora no había firmado ningún contrato específico de confidencialidad con ninguna de las entidades participantes en el proceso de selección de concursantes, en el que pudiesen establecerse las medidas de seguridad a adoptar por estas compañías respecto del tratamiento de los datos personales relacionados con los servicios prestados.

Manifestó en su descargo la entidad imputada que existía un Documento de Seguridad que se adjuntó al Acta de Inspección y, además, se constató en la Inspección que los ficheros de la productora se hallaban ubicados en una planta con dispositivo electrónico de control de acceso, por lo que se cumplían las medidas de seguridad exigibles.

Hay que decir que el aludido Documento de Seguridad adjunto al Acta de Inspección, era en realidad un documento elaborado por una empresa participada por la productora el 7 de diciembre de 1999, que consta de seis puntos: Ambito de aplicación, Normas y Procedimientos de seguridad, Funciones y Obligaciones del personal, Procedimiento de Notificación, Gestión y Respuesta ante incidencias y Copias de Seguridad. Asimismo, existe un *Código Ético de Confidencialidad de Datos* , también elaborado por la citada compañía, que afecta al personal que trabaja a su cargo con Bases de Datos de información personal. El propio documento de seguridad delimita su ámbito de aplicación circunscribiéndolo, exclusivamente, al personal de la compañía participada. El personal de la productora ha tenido acceso a los datos tratados automatizadamente de los participantes en el proceso de selección. Por tanto, aun en el caso de que las medidas de seguridad incorporadas a dicho documento fueran correctas, no son exigibles a los empleados de la productora, de forma que el acceso a los datos que realizan estos últimos no se encuentra sujeto a las medidas de seguridad que exigen la Ley Orgánica 15/1999 y el Reglamento que, en esta materia, la desarrolla. Por lo tanto, la productora, como responsable del fichero en el que finalmente fueron incluidos los datos personales de los participantes en el proceso de selección del programa GRAN HERMANO y como responsable de su propio personal, que accedió a los datos tratados automatizadamente, debió elaborar su propio documento de seguridad, del que no dispone o, alternativamente, debió modificarse el documento de seguridad de la otra compañía para que le fuera aplicable.

En consecuencia, el Director de la Agencia de Protección de Datos resolvió imponer a la entidad imputada sendas multas por la infracción de los artículos 5, 6 (en relación con el 7.3), 11 y 9 (éste en relación con el Reglamento de Medidas de Seguridad) de la Ley Orgánica 15/1999. Así mismo, acordó requerir a esta compañía para que en lo sucesivo se abstuviese de efectuar cesiones de datos personales no permitidas, como las constatadas durante la tramitación del presente procedimiento sancionador, pudiéndose proceder en caso contrario a la inmovilización de sus ficheros, de conformidad con lo dispuesto en el artículo 49 de la Ley Orgánica 15/1999.

Como consecuencia de este procedimiento también se incoaron procedimientos sancionadores al resto de las empresas participantes en el mencionado concurso, procedimientos que a final de año aún no se había dictado resolución.

4.2.2 Asociación Contra la Tortura

En el mes de marzo de 2000, tras la recepción de una denuncia, la Agencia inició un Procedimiento Sancionador en el que se imputaba a la ASOCIACIÓN CONTRA LA TORTURA (ACT) una infracción de los artículos 6.1 y 7.5 de la Ley Orgánica 15/1999, después de haberse verificado que esta organización distribuía, a través de un servidor *web* ubicado en España, un fichero conteniendo los nombres y apellidos de funcionarios de las Fuerzas y Cuerpos de Seguridad y de Prisiones, así como de responsables políticos, que habían sido denunciados por la comisión de delitos de maltrato, vejaciones o tortura. También se incluía en la citada web información acerca de la denuncia y del resultado del proceso judicial, detallándose en cada caso si el acusado había sido condenado, absuelto o si dicho proceso estaba todavía en fase de instrucción.

Durante la tramitación del procedimiento sancionador, la Agencia adoptó como medida de carácter provisional que la ACT cesara, de manera inmediata, en el tratamiento de datos de carácter personal de las personas afectadas, suprimiendo dicha información del servidor web utilizado. La misma medida cautelar se adoptó contra el elemento instrumental (servidor). Tanto la ACT como el servidor donde se alojaba la mencionada página web cesaron inmediatamente en el tratamiento de los datos cumpliendo así lo dispuesto en la medida cautelar, cuya legalidad fue confirmada por la Audiencia Nacional.

Durante la fase de alegaciones, la ACT manifestó que debía aplicarse la excepción del consentimiento para el tratamiento de los datos personales establecida en el artículo 6.2 de la LOPD, no teniendo la Asociación bases de datos ni ficheros, toda vez que sus informes anuales se elaboran con datos obtenidos a través de noticias publicadas en medios de comunicación así como de copias de sentencias facilitadas por los Tribunales de Justicia. Los datos que aparecen en la página web corresponden a informes del año 1997 sin que hayan sido actualizados ni modificados con datos nuevos. Añaden que los datos personales que constan en dichos informes no afectan a los derechos fundamentales reconocidos en la C.E. objeto de la protección de la LOPD

La ACT se cuestiona el concepto de dato personal considerando que los que incumben a la intimidad personal y familiar del individuo serían los que reflejasen su ideología, religión, creencias, raza, salud y tendencias sexuales, es decir los denominados "datos sensibles". Por otra parte, estarían aquellos datos que aun formando parte del individuo tienen una relevancia pública por razón de su cargo o profesión y, por lo tanto, no forman parte de la intimidad del individuo y están supeditados a los derechos de expresión y de información. Asimismo, declaran que no son titulares de ningún fichero ni base de datos, ni ha existido tratamiento, sino que los datos que aparecen publicados en la página web son los correspondientes al informe bienal de la Asociación correspondiente a los años 1996/1997, sin que el mismo haya sido actualizado con nuevos datos desde su publicación en soporte electrónico.

A este respecto la Resolución señala que los datos que constaban en la dirección de Internet, formaban un conjunto ordenado de nombres y apellidos de funcionarios, organizados por Cuerpos de pertenencia, completados con datos relativos a la situación en la que se encuentran por las denuncias recibidas, lugar y fecha donde ocurrieron los hechos y referencia numérica del caso concreto. Por tanto, esta información concerniente a personas físicas conformaba un conjunto organizado de datos, por lo que se entendió que es un fichero de datos de carácter personal de los mencionados en el artículo 3 de la LOPD. Los datos de carácter personal habían sido obtenidos y organizados, primero en soporte papel y posteriormente mediante procedimiento técnico automatizado para su conservación y comunicación a terceros a través de la citada página web de Internet. Comparando este hecho con la definición de tratamiento, nos encontramos ante un tratamiento de datos de carácter personal. En consecuencia, al existir un conjunto de datos personales registrados en un fichero y ser objeto de tratamiento, es de aplicación la LOPD en virtud del ámbito de la misma concretado en su artículo 2.1.

Respecto a la imputación de proceder al tratamiento de datos de carácter personal sin consentimiento de los afectados, la ACT alega que los datos de funcionarios de prisiones y de las Fuerzas y Cuerpos de Seguridad, así como de responsables políticos que constan en su memoria, la cual ha sido objeto de publicación en la página web, se han obtenido de fuentes accesibles al público y se persigue un interés legítimo que forma parte de los fines de la propia asociación. Concretamente, manifiestan que los datos se han obtenido de las publicaciones en diarios y de las sentencias que han sido facilitadas por los propios Tribunales de Justicia.

Para demostrar la alegación relativa a que el origen de los datos de los funcionarios y políticos se obtuvo de publicaciones en diarios de ámbito nacional y provincial, la ACT presenta listado con los nombres de 258 personas cuyos datos aparecen en la mencionada página web y las fechas de publicación en diversos diarios. Sin embargo, la propia Asociación enumera en dicho listado un número inferior de datos de funcionarios que los publicados vía Internet, que superaban los 400.

Tras las pruebas practicadas quedó acreditado que no todos los datos publicados en Internet por la ACT habían sido obtenidos de una de las fuentes de acceso público que, como los medios de comunicación, son admitidas por la LOPD.

La ACT también declara como origen de los datos las sentencias de los Tribunales de Justicia, por considerarlas fuentes públicas. Sin embargo, debe aclararse que una cosa es fuente pública y otra fuentes accesibles al público a los efectos de la LOPD. Las sentencias judiciales son efectivamente fuente pública, o, dicho de otro modo, gozan del efecto de publicidad procesal general en los términos reconocidos en la Ley Orgánica del Poder Judicial, pero ello no quiere decir que sean "*fuentes accesibles al público* " en el sentido reconocido por la LOPD a los efectos de su tratamiento automatizado, pues es evidente que las sentencias judiciales no se encuentran entre las fuentes accesibles al público que taxativamente enumera el artículo 3 j) de la citada Ley.

A este respecto, el Consejo General del Poder Judicial, tras analizar el alcance de los artículos 120 de la Constitución y 235 y 266 de la Ley Orgánica del Poder Judicial ha establecido criterios sobre la noción de publicidad e interés a los efectos del artículo 235 citado. Así, el Acuerdo del Consejo de 6/3/1991 señala que "*El acceso al texto de las sentencias y demás resoluciones judiciales debe ser permitido en tanto en cuanto guarde relación con la finalidad del derecho al proceso público, teniendo en cuenta los límites de este derecho, en especial los derivados de otros derechos fundamentales como el derecho a la intimidad personal y familiar y en este sentido debe interpretarse la expresión "interesado" de los arts. 236 y 266.1 de la Ley Orgánica del Poder Judicial* ".

Conforme a esta interpretación, cuando el "*interés* " consista en la obtención de datos personales que no guardan relación ni con el fin general de la publicidad procesal, ni con la función de la jurisprudencia, debe entenderse excluido del

concepto de interesado a que se refieren los artículos antes citados, por lesionar derechos de los afectados. En consecuencia, la utilización de los datos de carácter personal que figuran en sentencias judiciales por persona o entidad distinta a los interesados, en cualquier caso necesitaría para su tratamiento el consentimiento previo de los mismos, no pudiendo considerarse fuente de acceso público general. Por esta causa, debe entenderse que existe una norma limitativa al tratamiento automatizado de dichos datos que impide que cualquiera que no sea interesado pueda tratar los datos recogidos en las sentencias y cederlos posteriormente, pues dicha información se está no sólo compilando sino proporcionando a personas físicas o jurídicas a las que en un principio no iba destinada, por no ser interesados en esas causas judiciales.

Por otra parte, no se debe obviar que algunos de los datos divulgados hacen referencia a que el asunto está aún en vías de investigación. Lógicamente, estos datos no han podido ser obtenidos de resoluciones judiciales y se ha comprobado (comparando la información que figuraba en la página web con el listado facilitado por la ACT respecto a datos obtenidos de publicaciones de diarios) que muchos de estos datos tampoco se han obtenido de los medios de comunicación. La inclusión de los nombres, apellidos y categoría profesional (guardia civil, policía nacional, funcionario de prisiones, etc) de los sujetos que participan en dicha investigación con anterioridad a que los Jueces y Tribunales competentes decidan sobre la veracidad de las denuncias presentadas contra los mismos, estaría vulnerando el derecho fundamental reconocido en el artículo 18.4 de la C.E.

El artículo 7 de la LOPD establece un régimen especial y más riguroso para el tratamiento de determinados datos personales a los que denomina genéricamente como "datos especialmente protegidos". En el citado precepto se aprecian tres grupos de estos datos para cada uno de los cuales se concretan unas específicas exigencias de protección.

Así un primer grupo viene integrado por los datos de carácter personal que revelan ideología, afiliación sindical, religión y creencias, en cuyo supuesto al recabarse el consentimiento del afectado se le deberá advertir de su derecho a no prestarlo y si hecha la advertencia decide prestar el consentimiento deberá ser éste necesariamente expreso y por escrito. Un segundo grupo de datos especialmente protegidos lo constituyen aquéllos que hagan referencia al origen racial, a la salud y a la vida sexual, para cuyo tratamiento y cesión se requiere que por razones de interés general así lo disponga una Ley o que el afectado consienta expresamente. Finalmente, el tercer grupo de datos especialmente protegidos lo integran los relativos a la comisión de infracciones penales y administrativas para los que el legislador establece que su inclusión en ficheros sólo pueda hacerse por las Administraciones Públicas competentes y sólo en los supuestos previstos en las respectivas normas reguladoras. La infracción de esta norma es lo que se imputa en el presente procedimiento a la ACT. Al no ser una Administración Pública, sino una asociación de carácter privado es evidente que no puede crear un fichero en el que se incluyan datos relativos a la comisión de delitos o procesamientos por hechos delictivos de diversos funcionarios, miembros de cuerpos y fuerzas de seguridad y políticos. Y ello con independencia de que tales datos procedan o no de fuentes accesibles al público o de que se fundamenten o no en sentencias judiciales, incluso en el supuesto de que hubiesen ganado firmeza.

La imputación de esta infracción a la ACT nada tiene que ver con su libertad de expresión, ni con el derecho a la información, que se manifestará en todo caso en su informe sobre la tortura, sobre el que la Agencia de Protección de Datos nada tiene que decir por no ser de su competencia. Por ello, la medida cautelar decretada previa audiencia de los afectados por la misma se concretó en el borrado del fichero, que venía establecido y difundido a terceros a través de una página web en Internet, sin ninguna extensión ni alusión al informe de aquella Asociación. De igual forma, la iniciación simultánea del procedimiento por infracción del art. 7.5 de la LOPD se circunscribió la creación del mencionado fichero y no a la elaboración del informe.

La publicación en Internet de un fichero con los nombres y apellidos de funcionarios de prisiones y de las Fuerzas y Cuerpos de Seguridad, así como de responsables políticos, que han sido denunciados por la comisión de delitos de maltrato, vejaciones o tortura es, obviamente, una comunicación de datos a terceros, si se quiere incluso agravada dada la facilidad de difusión que lleva aparejado el medio empleado, lo que determinó la adopción de medidas cautelares por parte de la Agencia. No consta el consentimiento previo de los interesados para proceder a dicha comunicación ni se ha acreditado la existencia de alguna de las excepciones previstas en el artículo 11.2 LOPD al requisito del consentimiento para la cesión o comunicación de datos personales. Por tanto, la ACT ha infringido también el art. 11 de la Ley.

Teniendo como base todas estas argumentaciones, el Director de la Agencia de Protección de Datos resolvió imponer a la ACT dos multas: por infracción de los artículos 6.1 y 7.5 de la LOPD, por una parte, y por infracción del artículo 11 de la misma Ley, por otra.

Además, como los datos personales habían sido replicados en otros servidores con sede fuera del territorio español (Canadá, Dinamarca, Ecuador, Estados Unidos, Francia, Holanda, Italia, Nueva Zelanda y República Checa), el Director de la Agencia de Protección de Datos informó a las autoridades extranjeras competentes en materia de protección de datos de la Medida Cautelar adoptada, solicitando su auxilio para que cesase el tratamiento de los datos de las personas afectadas en los servidores web de sus respectivos territorios.

4.2.3. Difusión de claves de usuarios para acceso a un portal de internet.

También en el verano de 2000, tuvo entrada en la Agencia un soporte informático conteniendo más de doce mil códigos de usuario y contraseñas correspondientes supuestamente a *usuarios de Internet que tienen contratados sus servicios con la compañía propietaria del portal referido.*

Se iniciaron las correspondientes actuaciones de inspección, con objeto de determinar una posible vulneración de la

Ley en relación con la pérdida de confidencialidad de estos datos.

Como resultado de estas actuaciones, la Agencia inició un Procedimiento Sancionador que aún no ha concluido y del que se informará en la Memoria del próximo ejercicio.

4.2.4 Difusión de datos personales de abonados telefónicos a través de internet.

A finales de febrero de 2000 diversos medios de comunicación informaron que a través de Internet se podía acceder a los datos personales de los abonados de un importante operador de telefonía. Dicha información dio lugar al inicio de actuaciones previas de investigación en las que se constataron los siguientes hechos:

El operador se encontraba en fase de desarrollo de un sistema informático que permitiría acceder a los datos reales de facturación y tráfico de los abonados al personal de la compañía encargado de atender las consultas y reclamaciones al respecto. Por diversas circunstancias, el sistema en pruebas quedó como si de un sistema ya operativo se tratase, accesible además desde Internet.

Esta circunstancia permitió que cualquier usuario de Internet, fuese o no cliente del operador en cuestión, tuviese acceso a datos de tráfico y facturación de cualquier abonado del operador. Los datos personales que se pudieron consultar eran los que figuraban en la última factura emitida en ese momento (nombre del titular del servicio, domicilio, importe, domiciliación bancaria y detalle de las llamadas efectuadas con las tres últimas cifras ocultas de los números a los que se realizaron las llamadas), así como los de las seis facturas anteriores, sin detalle de llamada, y el importe acumulado de la factura que en ese momento se encontraba en curso.

Estos hechos dieron lugar a la apertura de un procedimiento sancionador que concluyó con una resolución sancionadora por infracción del operador del artículo 9 de la LOPD en relación con diversos artículos del Reglamento de Seguridad.

Es interesante destacar la disquisición que se produjo durante la tramitación del procedimiento sancionador acerca de la aplicabilidad del Reglamento de Medidas de Seguridad sobre ficheros que, a la fecha de entrada en vigor del citado Reglamento, se encontraban ya constituidos.

Según el operador, los ficheros afectados por los accesos no autorizados existían ya a la fecha de entrada en vigor del citado Reglamento por lo que, a su criterio, les era de aplicación el período transitorio que establece el propio Reglamento de Medidas de Seguridad, dentro del cual se produjeron los hechos objeto de la infracción.

La Resolución contradice dicho criterio. En efecto, la Disposición Transitoria única del citado Real Decreto fija los plazos en que deberán ser implantadas las medidas de seguridad en los sistemas de información que se encuentren en funcionamiento a la entrada en vigor del Reglamento, que han sido prorrogados para las de nivel básico hasta el 26 de marzo de 2000 por el Real Decreto 195/2000, de 11 de febrero. La mencionada Disposición Transitoria determina en su párrafo primero: "*En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años".*

Por su parte, el artículo 2.1 del Real Decreto 994/1999 define los sistemas de información como: "*conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal*", de lo que se desprende que el concepto de sistema de información es más amplio que el de fichero, debiendo entenderse que un sistema de información lo constituye el conjunto de ficheros automatizados, programas, soportes y equipos empleados no sólo para el almacenamiento de los datos sino también para el tratamiento de los mismos. En este sentido, el artículo 3 de la Ley Orgánica 15/1999 define en su apartado c) el concepto de tratamiento de datos como: *Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias* .

Para determinar si existe o no un nuevo sistema de información no es suficiente con considerar si la información a la que se accede procede de un fichero preexistente. Es necesario, además, tener en cuenta si, para llevar a cabo dicho acceso, se han diseñado nuevos programas o utilizado nuevos soportes o equipos que permitan llevar a cabo nuevos tratamientos de los datos que no existían respecto del fichero preexistente.

Si con las actuaciones realizadas por el operador se permiten accesos y tratamientos de datos que antes no estaban permitidos, debe afirmarse, a los efectos de la exigencia de medidas de seguridad, que existe un nuevo sistema de información.

Esta interpretación no sólo es conforme con la literalidad y finalidad del artículo 9 de la Ley y del Reglamento que lo desarrolla, sino también con lo previsto en la Directiva 95/46/CE cuyo Considerando 46, al tratar de las medidas de seguridad, las refiere tanto al momento de la concepción del sistema de tratamiento como al de la aplicación del mismo.

En este sentido, la finalidad de la Disposición Transitoria única antes transcrita es la de que los sistemas existentes gocen de un periodo de adaptación para la incorporación de las medidas de seguridad. Pero en casos como el presente en el que se habilitan nuevos accesos (materia incardinada en el artículo 9 de la Ley y en su Reglamento), configurando programas específicos para permitirlos, aquéllas deben ser adoptadas desde el primer momento para

evitar las nuevas situaciones de riesgo que van a producir los nuevos tratamientos automatizados de datos, lo que se evitará mediante la adopción de las oportunas medidas de seguridad. Especialmente si estos nuevos accesos y tratamientos se encuentran en una fase de prueba que se realiza con datos reales.

En este caso, de acuerdo con las definiciones transcritas, debe concluirse que el operador, al diseñar y crear en octubre de 1999 una nueva forma de acceso a los datos de sus ficheros de facturación, destinada a facilitar el acceso a nuevos usuarios (los empleados de la empresa) a través de una red de comunicación distinta de Infovía e Internet (la Intranet del operador), creó realmente un nuevo sistema de información, por cuanto ello supuso la creación de nuevos tratamientos de la información .

Por ello, al realizarse pruebas con datos reales para la realización del nuevo sistema de información, eran exigibles al operador, desde el primer momento, las medidas de seguridad establecidas en el Real Decreto 994/1999, de conformidad con lo previsto en su Disposición Transitoria Única en concordancia con los artículos 22, 4, 8, 11 y 12 del mismo.

4.3 PUBLICIDAD Y MARKETING DIRECTO

El envío de publicidad no deseada y el marketing directo constituyen, como viene siendo reflejado habitualmente en la Memorias de la Agencia, una de las actividades comerciales que más denuncias ocasionan.

Considerando el número de procedimientos sancionadores iniciados durante el año 2000, se observa que **24** de ellos corresponden a actividades relacionadas con el envío postal de publicidad, lo que supone el 17% de todos los correspondientes al sector privado, porcentaje muy similar al del ejercicio anterior. En cuanto a las infracciones detectadas, se puede reseñar que 4 fueron muy graves por cesión de datos, 20 graves por tratamiento sin consentimiento y no cancelación de datos, y 3 leves.

Es también reseñable que del total de resoluciones sancionadoras, un gran porcentaje ha recaído sobre dos compañías (5 en un caso y 4 en el otro) especializadas en el alquiler o venta de direcciones para campañas de marketing directo, cuyo origen la imputada no pudo acreditar durante la tramitación de los correspondientes procedimientos, aunque en algún caso se constató que los datos personales tratados o cedidos habían sido obtenidos del Censo Electoral, que no tiene la consideración de fuente accesible al público. Por otra parte, son también varias las sanciones impuestas a empresas que, a pesar de haber recibido expresas solicitudes de cancelación por parte de los interesados, no procedieron a su cancelación y continuaron tratando sus datos con fines publicitarios.

4.4 PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO

Siguiendo la tendencia de los años anteriores, las reclamaciones dirigidas contra entidades responsables de ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito han originado gran parte de la actividad desarrollada por la Agencia de Protección de Datos durante el año 2000. La experiencia constata la gran repercusión que tiene el uso de los datos de carácter personal tratados en estos ficheros entre las personas que desean contratar productos crediticios y de financiación, lo que justifica la tendencia de que durante el año 2000 se haya producido un ligero aumento con respecto al año 1999, tanto en lo referente al número de reclamaciones presentadas por los ciudadanos como al número de sanciones impuestas.

Las actividades realizadas por la Agencia durante el año 2000 en relación con los ficheros a los que se refiere el artículo 29 de la Ley Orgánica 15/1999, se han centrado fundamentalmente en atender las reclamaciones y denuncias presentadas por los ciudadanos, toda vez que durante años anteriores estos ficheros ya fueron objeto de un profundo análisis en el ámbito del Plan de Oficio Sectorial, abordado como consecuencia de la constante preocupación que la Agencia de Protección de Datos ha mantenido en todo momento por el funcionamiento de los denominados ficheros de morosidad.

* Merece destacarse que la entrada en vigor el 14 de enero de 2000 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, así como la reciente Sentencia del Tribunal Constitucional n§ 292/2000, de 30 de noviembre de 2000, han introducido novedades en cuanto al funcionamiento de estos ficheros que pueden establecer cambios en los criterios fundamentales que rigen la línea de actuación de la Agencia en relación con los mismos.

En el caso del sector que nos ocupa, los ciudadanos, a través de sus reclamaciones, han planteado una cuestión sobre la validez de la restricción temporal de seis años establecida en el artículo 29.4 de la LOPD de los datos adversos registrados en los ficheros de información sobre solvencia patrimonial y crédito una vez que la deuda ha sido cancelada, momento en el cual pasa a figurar en el fichero la deuda regularizada bajo la denominación "saldo 0", situación ésta que había sido considerada lícita en aplicación de la derogada LORTAD y durante su vigencia.

Como consecuencia de este cambio legal producido en el art. 29.4 LOPD, respecto de lo dispuesto en el anterior art. 28. 4 de la derogada LORTAD, durante el año 2000 se han tramitado varias denuncias sobre el denominado "saldo 0" que han dado lugar a la incoación de procedimientos sancionadores por infracción del artículo 29.4 de la LOPD, en relación con el articulo 4.3 de la misma Ley. Al terminar el año dichos procedimientos aún no han finalizado, por lo que se informará de ello en la próxima Memoria.

* Al margen de lo anterior, entre las resoluciones dictadas por el Director de la Agencia de Protección de Datos durante el año 2000 en relación con ficheros de información sobre solvencia patrimonial y crédito, cabe destacar el incoado a

una entidad financiera que incluyó en el fichero ASNEF los datos personales de un denunciante a causa del incumplimiento de un contrato de financiación firmado para la adquisición de un vehículo, contrato que el denunciante manifiesta no haber firmado.

Los indicios aportados durante la investigación previa ponen de manifiesto que el citado contrato no fue firmado por el afectado, lo que motiva la apertura de un procedimiento sancionador que concluye mediante la resolución del Director de la Agencia de Protección de Datos que impone una sanción a la entidad financiera por infracción del artículo 6 LOPD (tratamiento de datos del afectado sin consentimiento), tipificada como grave.

La entidad financiera alegó que se hicieron todos los controles de seguridad, tales como comprobar las firmas, solicitar fotocopia del DNI, verificar la operación, etc..., y que la entidad no puede comprobar el original del DNI del prestatario puesto que se trata de una forma de contrato prevista en nuestro ordenamiento como "venta entre ausentes" o "contrato por correspondencia".

Sin embargo, la resolución establece que los sistemas de seguridad implementados por la entidad no cumplieron su objetivo puesto que el contrato del préstamo no fue firmado por el denunciante, a pesar de lo cual se le incluyó en un fichero de morosidad.

Así mismo, durante la investigación previa el denunciante manifestó su deseo de renunciar a cualquier acción que pudiera derivarse de la presentación de la denuncia. Sin embargo, dicha renuncia no impidió la continuación del procedimiento con base en el artículo 68 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y el artículo 18.1 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, conforme al cual el procedimiento sancionador se iniciará siempre de oficio. Así, el hecho de que el denunciante renuncie a los derechos dimanantes de su denuncia, no implica el archivo del procedimiento sancionador incoado si se aprecia vulneración de la LOPD, toda vez que el mismo se inicia y se tramita en todas sus fases de oficio.

4.5 ENTIDADES FINANCIERAS

Entre las actuaciones practicadas en el mismo año 2000 acerca de las entidades financieras, cabe destacar la motivada por la aparición en los medios de comunicación de una noticia relativa a la aparición de diversa documentación que contenía datos de carácter personal en los contenedores de basura depositados en la vía pública de cuatro entidades bancarias.

A la vista de estos hechos, el Director de la Agencia acuerda iniciar una inspección de oficio a las citadas entidades bancarias a fin de esclarecer los hechos. Los objetivos de dichas actuaciones de inspección se concretaron en:

Conocer los Sistemas de Información y procedimientos utilizados por dichas entidades para el cumplimiento de las funciones desarrolladas por las mismas en relación a los datos de carácter personal.

Comprobar el grado de cumplimiento de la Ley Orgánica 15/1999 y del Real Decreto 994/1999 respecto de los ficheros automatizados de los que son responsables las entidades inspeccionadas y detectar las posibles deficiencias existentes en cuanto a las medidas de seguridad adoptadas por dichas entidades.

Tras las actuaciones llevadas a cabo por la Inspección de Datos en relación con los objetivos citados anteriormente, y a la vista de los resultados obtenidos, el Director de la Agencia acuerda iniciar un procedimiento sancionador a tres de las cuatro entidades bancarias investigadas por presunta vulneración de los arts. 9 (relativo a las medidas de seguridad) y 10 (deber de secreto) de la LOPD, y el archivo de la cuarta entidad inspeccionada por no haberse encontrado indicios de vulneración de la LOPD.

Los citados Procedimientos Sancionadores se encuentran actualmente en fase de tramitación y pendientes de dictar Resolución de la que se informará en la próxima Memoria.

4.6 SANIDAD

* El tratamiento de los datos de salud es objeto de especial protección por el legislador y tema de especial sensibilidad para la generalidad de la colectividad. De ahí la vigilante y constante preocupación de la APD por su adecuación a las prescripciones legales. Habiéndose expuesto anteriormente las actuaciones más relevantes de este sector en el ámbito sanitario público, corresponde ahora referirse a las más significativas habidas en el sector privado.
* Una de las denuncias recibidas se refería a la recepción por parte de la denunciante de un escrito remitido por una Clínica de cirugía estética, ofreciéndola sus servicios de tratamiento.
* Según manifestaciones de la denunciante, ello es consecuencia de la cesión de datos realizada a la clínica de cirugía estética por la familia del médico en cuya clínica fue tratada la denunciante con anterioridad, dado que ella recibió un escrito de la familia del citado médico en la que le indicaban que ante el fallecimiento del mismo, *todos los archivos relativos a la relación de tratamientos realizados en la clínica, así como todos los datos de carácter privado de la clientela, a los que hemos podido tener acceso, han sido destruidos,* habiéndose facilitado los nombres de los clientes, a la Clínica de cirugía estética mencionada, *con el único fin de que, cuantos de ellos estuviesen interesados en seguir o comenzar algún tratamiento, pudiesen ser atendidos en todo momento por personal acreditadamente cualificado.*
* La denunciante manifestaba su disconformidad en la cesión de dichos datos.

Tras la realización de las oportunas actuaciones de inspección, se obtuvieron las siguientes conclusiones:

La Clínica de cirugía estética, por encargo de la familia del médico fallecido, al carecer éstos de medios para ello, realizó un mailing a los pacientes de dicho doctor.

Los datos facilitados consistían en una relación manual con los nombres, apellidos y direcciones de los pacientes, cuyos datos procedían de una agenda personal del citado doctor.

En el fichero que utilizaba la Clínica de cirugía estética para la gestión de sus clientes, no se encontraron datos de la denunciante, no habiéndose podido acreditar la existencia de algún fichero en dicha Clínica, que contuviera datos de los pacientes del médico fallecido.

A la vista de los hechos, el Director de la Agencia resolvió *archivar* estas actuaciones de inspección dado que en el supuesto presente quedó acreditado que la Clínica de cirugía estética obtuvo los datos de la denunciante a través de la familia del médico fallecido, si bien datos de los pacientes del mismo procedían de su agenda personal no automatizada, quedando estos hechos fuera del ámbito de aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal.

* Otra de las denuncias recibidas ha sido presentada por el Presidente del Ilustre Colegio Oficial de Farmacéuticos de Valencia contra la Consellería de Sanitat de la Generalitat Valenciana, en la que manifiesta que en virtud del tradicional Convenio entre los Colegios de Farmacéuticos de la Comunidad Valenciana y la Consellería, a través de cada uno de los tres Colegios de la Comunidad se presentan mensualmente a la Consellería las facturas correspondientes a todas las recetas dispensadas por las farmacias, a cargo del Servicio Valenciano de la Salud. A dicha factura se acompañan los originales de las recetas a modo de albarán que acredita que la dispensación de cada medicamento se ha hecho conforme a la prescripción del médico y que el precio que se carga es el correcto, puesto que a cada receta se adhiere el cupón precinto en el que consta el precio de venta al público. Sin embargo, la Consellería utiliza las recetas para un segundo uso, distinto del que queda reseñado y motiva su entrega, puesto que sus Servicios de Inspección Farmacéutica, en lugar de acudir a la farmacia y en su caso levantar un acta de infracción al farmacéutico, toma las recetas, las saca de su contexto de instrumento de facturación y pago y las utiliza para iniciar con ellas expedientes sancionadores por el hecho de que el farmacéutico no haya consignado, al dorso de las recetas de medicamentos psicotrópicos, el DNI del usuario.
* El denunciante considera que con tal actividad la Consellería rompe el principio de confidencialidad que protege el uso de los datos que el ciudadano le facilita a la Administración y estima que si bien es legítima la obligación de entregar los originales de las recetas, es ilegítimo el uso de las mismas para fines distintos de los que motivaron su entrega.
* De las actuaciones practicadas a consecuencia de la denuncia, se ha comprobado que la relación entre la Consellería de Sanitat y los Colegios Oficiales Farmacéuticos viene determinada por las cláusulas y anexos que constituyen el cuerpo del Concierto en el que se fijan las condiciones para la prestación farmacéutica a través de las oficinas de farmacia. La Consellería de Sanidad, en el ámbito de sus atribuciones, cuenta con la Inspección Farmacéutica con competencias para supervisar y controlar el cumplimiento de la normativa farmacéutica y, concretamente, para velar por el uso racional del medicamento y comprobar que el paciente recibe el producto prescrito o en su caso uno sustituible, así como que en la dispensación se han cumplido las reglas establecidas.
* Este procedimiento de revisión es generalmente de forma manual y las recetas médicas se encuentran en soporte papel, siendo sobre éstas sobre las que la Inspección Farmacéutica realiza el muestreo al objeto de comprobar la correcta dispensación y facturación.
* En el Concierto entre la Consellería de Sanitat y los Colegios Oficiales Farmacéuticos se fijan las condiciones para la prestación farmacéutica a través de las oficinas de farmacia. La prestación de estos servicios profesionales se ve compensada con unas condiciones económicas que se regulan en la Cláusula Cuarta, de la que es necesario destacar su primer párrafo: *"La Administración suscribiente abonará a las oficinas de farmacia las recetas* **correctamente dispensadas y facturadas** en las condiciones económicas" que se especifican. Ante esto se presupone el control por la Administración de la correcta dispensación.
* Existe una responsabilidad de la Administración como órgano administrador, toda vez que en el Anexo al Concierto, así como en el Acta 1/98 de la Reunión de la Comisión Central encargada de velar por el cumplimiento y aplicación del Concierto en el que se fijan las condiciones para la ejecución de la prestación farmacéutica a través de las oficinas de farmacia, en el apartado *Subsanables 1 (S1)* , se dice **"Recetas en las que falta alguno de los datos de identificación, correspondiente a los datos del paciente"**. En estos casos se firman las causas de devolución, que se detectan mediante muestreo de las recetas, siendo las incidencias que se encuentran remitidas a la Inspección para su valoración.
* Es función de la Administración velar por el Uso Racional del Medicamento y comprobar que el paciente recibe el producto prescrito o en su caso uno sustituible, y que en la dispensación se han cumplido las reglas establecidas. También ha de comprobar que la receta dispensada y facturada reunía los requisitos de validez para su dispensación (plazo de validez, visado, DNI para psicótropos, etc.). La exigencia del DNI se establece por primera vez en 1994, para exigir un mayor y necesario control con el fin de evitar una indebida utilización de esta medicación (estupefacientes y psicótropos) susceptible de tráfico ilícito.
* Esta exigencia se establece para el modelo de receta del Sistema Nacional de Salud, que es precisamente la que se utiliza para la provisión de servicios y medicamentos en las oficinas de farmacia (Orden de 25 de abril de 1994, Ministerio de Sanidad y Consumo, por la que se regulan las recetas y los requisitos especiales de prescripción y dispensación de estupefacientes para uso humano).
* Por otro lado, el mismo Concierto prevé un plazo de tiempo de custodia de estos documentos oficiales, precisamente para realizar los controles pertinentes desde el punto de vista administrativo y sanitario. Estos controles afectan exclu-

sivamente a lo referente a la prescripción y dispensación (actuación profesional del farmacéutico y no sobre el paciente).
* La Consellería de Sanidad en el ámbito de sus competencias cuenta con la Inspección Farmacéutica, constituida por Inspectores del Cuerpo Sanitario, Escala de Inspectores Farmacéuticos. Estos funcionarios al amparo del art. 124 del Decreto 2065/74, Texto refundido de la Ley General de la Seguridad Social, no derogado por el Real Decreto legislativo 1/1994, tienen reconocida la condición de autoridad pública, siendo por tanto plenamente competentes para realizar informaciones previas y expedientes disciplinarios ante situaciones de incumplimiento de la normativa sanitaria por la que están obligados a velar. Las competencias de la Inspección Farmacéutica son precisamente las de supervisar y controlar el cumplimiento de la normativa farmacéutica.
* En virtud de los preceptos expuestos y atendiendo a que los hechos denunciados se refieren a datos que se encuentran en soporte papel, la Agencia de Protección de Datos no es competente, en la actualidad, para conocer del asunto, por lo que procede archivar las actuaciones iniciadas a consecuencia ecepción de la denuncia.
* Por lo tanto, por el Director de la Agencia de Protección de Datos se acuerda proceder al *archivo* de las presentes actuaciones.

* En el año 1999 se iniciaron diversas actuaciones de inspección que fueron concluidas en el año 2000, motivadas por varias denuncias relacionadas con la cesión por parte de la Entidad Pública Empresarial Correos y Telégrafos, el Departamento de Medio Ambiente de la Generalitat de Cataluña y una Caja de Ahorros (en adelante, las entidades) de datos de identificación, domicilio y salud de los trabajadores de las mismas, a tres empresas médicas privadas, alegando algunos de los denunciantes haber recibido visitas de facultativos de estas empresas en su domicilio particular, los cuales disponían, entre otros datos personales suyos, los relativos a su historial médico.

* El objeto de los contratos suscritos entre las citadas entidades y las empresas médicas es la prestación de un servicio médico de apoyo para la mejora de la atención asistencial a los trabajadores de las entidades, así como para la gestión de las ausencias laborales por motivos de salud.
* Con base en dichos contratos, las mencionadas entidades facilitan a las empresas médicas una relación de bajas laborales y altas producidas, incluyendo los siguientes datos personales: fecha en que se produce la baja, motivo de la baja (enfermedad o accidente), nombre, apellidos, domicilio, población y - cuando es posible - teléfono. Los facultativos de las empresas citadas realizan visitas médicas a los trabajadores que se encuentran en situación de baja laboral, elaborando resúmenes que se remiten a los Servicios Médicos de las entidades.
* Posteriormente, los datos de los pacientes son introducidos en los ordenadores de las empresas médicas. Entre dichos datos se registran los datos de salud de los trabajadores visitados.
* A la vista de lo expuesto, hay una cesión de datos de las entidades citadas a las empresas médicas, que dio lugar a la incoación de los correspondientes procedimientos. El carácter de dichos datos es el de datos bentificación de empleados de la entidad, a excepción de los relativos a la fecha de alta o baja y al motivo de esta última (si es por causa de enfermedad o accidente), que dependiendo del contenido de la información suministrada pueden ser calificados o no como datos de salud.
* Sin embargo, independientemente de la calificación de dichos datos, la infracción imputada a las entidades es la cesión o comunicación de datos fuera de los casos permitidos, tipificada como *muy grave* en el artículo 43.4.b) de la Ley Orgánica 5/1992, de 29 de octubre, y en este sentido, para determinar si tal cesión es o no ajustada a la normativa sobre protección de datos personales, es preciso tener en cuenta no sólo lo específicamente previsto en su Ley reguladora, sino también lo dispuesto en el artículo 20.4 del Estatuto de los Trabajadores (Real Decreto Legislativo 1/1995, de 24 de marzo), que dispone que "*el empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones".*
* Este precepto habilita pues al empleador a controlar el absentismo laboral de sus trabajadores, permitiéndole comprobar la autenticidad de la baja médica mediante la verificación del estado de enfermedad o accidente del trabajador, encuadrando esta posibilidad como una de las competencias del empleador. La cuestión se reduce pues a determinar si dicha verificación del estado de enfermedad o accidente del trabajador ha de realizarla forzosamente por sí mismo el empresario/empleador o, por el contrario, puede encargar a un tercero la prestación de ese servicio. Y, en este sentido, ha de concluirse que tal encargo podrá realizarse siempre y cuando se prevean las garantías adecuadas, de conformidad con lo previsto en el artículo 27 de la LORTAD, hoy artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre.
* En el presente caso, dado que las entidades han demostrado fehacientemente que existen varios contratos escritos de prestación de servicios firmados con las empresas, debe entenderse que existe una prestación de servicios amparada por el artículo 27 de la LORTAD y por el actual artículo 12 de la LOPD y no una cesión ilegal de datos, habida cuenta de que no se han utilizado los datos para fines distintos de los estipulados en el contrato de servicios y que los datos no han sido cedidos a terceros, habiéndose previsto igualmente las garantías adecuadas al establecerse cláusulas de confidencialidad.
* En su virtud, se ha considerado que no existe infracción a la normativa sobre protección de datos en la actuación de las entidades, por lo que el Director de la Agencia ha resuelto declarar la ausencia de responsabilidad de las mismas respecto de los hechos imputados en los correspondientes procedimientos.
* Por su parte, en los correlativos procedimientos sancionadores abiertos a las empresas médicas por el tratamiento de datos relativos a la salud de los afectados sin disponer del consentimiento de los mismos, dichas empresas alegaron en su descargo no ser las responsables del fichero sino las encargadas del tratamiento de datos solicitado por las entidades. Sin embargo, ello no se corresponde con la realidad de los hechos que están acreditados en los correspondientes expedientes, ya que quienes obtienen los datos de salud de los afectados son las propias empresas médicas y son éstas quienes los incorporan a su propio fichero, lo que tratándose de datos de salud sólo puede realizarse con consentimiento expreso de aquéllos, que en el presente caso no se obtuvo; sin que pueda confundirse el supuesto consentimiento tácito para que alguien pueda ser examinado por un médico de dicha empresa, por el hecho de some-

terse al reconocimiento médico, con el consentimiento expreso que exigen tanto la Ley 5/1992, como la Ley 15/1999, para tratar datos de salud.
* Por estas razones el Director de la Agencia ha resuelto:
* Imponer a cada una de las tres empresas médicas, por una infracción del artículo 7.3 de la Ley Orgánica 15/1999, de 13 de diciembre, tipificada como *muy grave* en el artículo 44.4 c) de dicha norma, una multa de 10.000.000 (diez millones) de pesetas de conformidad con lo establecido en el artículo 45.2 de la citada Ley Orgánica, por aplicación de la previsión recogida en el artículo 45.5 de la misma.
* Requerir a cada una de las empresas médicas para que adopten las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 7.3 de la Ley Orgánica 15/1999, con indicación de que, de acuerdo con lo preceptuado en el artículo 49 de la citada Ley Orgánica, si el requerimiento fuera desatendido la Agencia de Protección de Datos podrá inmovilizar los ficheros.

4.7. COLEGIOS PROFESIONALES

Como en años anteriores, la tipología de las infracciones en este sector se centra en la cesión de datos personales por parte de los Colegios Profesionales a otras entidades y el tratamiento sin consentimiento por parte de estas últimas. De entre las resoluciones más importantes o significativas dictadas durante el año 2000 cabe destacar las siguientes:

* Se presentaron tres denuncias relacionadas con este sector por posible infracción de la Ley Orgánica 15/1999. Las tres denuncias están relacionadas con los artículos 6 y 11 de la Ley Orgánica 15/1999, es decir, con el consentimiento del afectado y la comunicación o cesión de datos a terceros. Realizadas las inspecciones a las entidades involucradas, el Director de la Agencia de Protección de Datos dictó resolución de archivo de actuaciones en los tres casos, al no apreciarse infracciones a la normativa sobre protección de datos personales en la actuación de estas entidades.

De las tres denuncias mencionadas, la más destacable corresponde a la suscrita por seis profesionales de la enfermería, que manifestaban en su escrito de denuncia la utilización del soporte informático del Colegio de Enfermería de A Coruña y del Consello Galego de Enfermería para hacerles llegar a todos los colegiados la propaganda del Sindicato Unión Profesional de la Enfermería, sin su consentimiento.

Considerando que el artículo 5 apartado j) de la Ley de Colegios Profesionales permite a éstos "*organizar actividades y servicios comunes de interés para los colegiados, de carácter profesional, formativo, cultural, asistencial y de previsión y otros análogos, proveyendo al sostenimiento económico mediante los medios necesarios"* y que el apartado u) del mismo artículo prevé también que pueden realizar*" cuantas funciones redunden en beneficio de los intereses profesionales de los colegiados* ", se concluyó a la vista de los hechos constatados por los Servicios de Inspección que fueron los propios Colegios Provinciales de la Comunidad Autónoma Gallega y el Consejo Galego de Enfermería los que, usando sus ficheros automatizados, remitieron directamente la propaganda a sus colegiados en una publicación con contenido propio de la actividad colegial, con independencia de cual fuera su contenido ideológico. Existiendo, por tanto, una norma con rango de Ley, como la citada Ley de Colegios Profesionales, que permite este tratamiento y no existiendo cesiones entre las entidades involucradas, se concluyó que no existió vulneración de la LOPD.

* Aparte de estas tres denuncias aludidas, cabe destacar en este sector la incoación durante el año 2000 de diez procedimientos sancionadores a otros tantos Colegios Oficiales de Aparejadores y Arquitectos de diferentes regiones del territorio español. Dichos procedimientos corresponden a actuaciones previas efectuadas por la Inspección de Datos durante el año 1999, con relación a la obtención, tratamiento y cesión por parte de una empresa privada, de datos personales de los profesionales que intervienen en obras de la construcción, tales como los nombres del arquitecto, aparejador, promotor e incluso del propietario de la obra, con la finalidad de editar publicaciones relativas al sector de la construcción.

En la inspección practicada a la citada empresa se comprobó la existencia en poder de la misma de listados de profesionales de la construcción y propietarios de las obras que le habían sido cedidos por los diferentes Colegios Profesionales de Aparejadores y Arquitectos. En dichos listados se especificaban, entre otros, los datos personales de la naturaleza mencionada. De los diez procedimientos sancionadores iniciados a las entidades cedentes de los datos, seis de ellos fueron resueltos con la imposición de sanción por infracción del artículo 11 de la Ley Orgánica 5/1992, tipificada como muy grave, siendo los otros cuatro archivados, bien por aportar la entidad el consentimiento de los afectados, bien por no existir pruebas suficientes de las que pudiera deducirse que los correspondientes listados de datos personales habían sido facilitados a la entidad editora de la publicación sobre la construcción por los respectivos Colegios Profesionales.

* Además de estas diez resoluciones mencionadas, el Director de la Agencia de Protección de Datos dictó durante el año 2000 la resolución del procedimiento sancionador iniciado en diciembre de 1999 a la propia empresa privada que obtenía y trataba los datos. Además de la edición de revistas relativas al sector de la construcción, esta empresa privada cedía a su vez los datos publicados en distintos soportes (papel, disquete, fax y correo electrónico) a diversos clientes.

En dicha resolución se impusieron sanciones por tratamiento automatizado (art. 6.1. LOPD) y comunicación de datos de carácter personal (art. 11.1. LOPD) sin el consentimiento de los afectados, tipificadas como grave la primera y muy grave la segunda en los artículos 43.3 y 43.4 de la citada Ley Orgánica. El consentimiento para el tratamiento automatizado de los datos de carácter personal es uno de los principios de la Ley Orgánica 5/1992 y puesto que dicho consentimiento no fue acreditado por parte de la empresa privada, se consideró que había incurrido en la citada infracción grave. Dado además que la empresa no acreditó el consentimiento previo de los afectados para que sus datos consta-

ran publicados y fueran comunicados a terceros por medio de cualquier otro soporte, se estimó también que había incurrido en la infracción muy grave mencionada.

4.8. PARTIDOS POLÍTICOS

Durante el año 2000 sólo se ha iniciado un procedimiento sancionador referido a un Partido Político.

En septiembre de 1999, tuvo entrada en la Agencia de Protección de Datos un escrito en el que el denunciante manifiesta que durante la campaña electoral de las elecciones del 13 de junio de 1999, fueron enviados a su domicilio particular impresos de propaganda electoral de un determinado partido político. Habiendo solicitado a dicha formación política el origen de sus datos fue contestado que seguramente habían sido facilitados por algún familiar o amigo durante encuentros y reuniones electorales previas.

Tras las actuaciones de inspección, quedó acreditado que los datos utilizados para la realización de la citada campaña electoral, tenían su origen en una empresa privada a la que fueron alquilados dichos datos por mediación de otra empresa privada, que manipuló y distribuyó la citada propaganda electoral, sin contar ninguna de ellas con el consentimiento del afectado.

Por todo lo expuesto, se procedió al inicio del correspondiente procedimiento sancionador al partido político y a las dos empresas privadas. Al partido político por posible incumplimiento del artículo 14 de la Ley Orgánica 5/1992, que regula el derecho de acceso y cuya infracción es tipificada como grave. A la empresa privada origen de los datos por posible vulneración del artículo 11 de la misma Ley Orgánica al haber comunicado los datos a la empresa mediadora, y cuya infracción está tipificada como muy grave. Y a la empresa privada manipuladora de los datos por posible incumplimiento del artículo 6 de la citada Ley Orgánica 5/1992, el cual regula el consentimiento del afectado, y cuya infracción está tipificada como grave. Al finalizar el año 2000, dicho procedimiento se encuentra aún en fase de tramitación, por lo que de su resolución se dará cuenta en la próxima Memoria.

4.9. SINDICATOS

* Durante el año 2000 sólo se ha realizado una actuación de investigación ante un sindicato, la cual se inició tras recibirse un escrito de denuncia en la Agencia. Durante las actuaciones quedó acreditado que el sindicato denunciado había publicado en una revista propia los complementos de productividad percibidos por una serie de funcionarios de un organismo público, información que había sido facilitada por ese mismo organismo; también que la revista figuró expuesta en el propio tablón de anuncios de este último. Dichas actuaciones fueron finalmente archivadas por el Director de la Agencia, en cuya Resolución se tuvo en consideración el artículo 23.3.c) in fine de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública que establece en cuanto al complemento de productividad: "*En todo caso, las cantidades que perciba cada funcionario por este concepto serán de conocimiento público de los demás funcionarios del departamento u Organismo interesado así como de los representantes sindicales* "; y también el artículo 8.2.a) de la Ley Orgánica de Libertad Sindical, de 2 de agosto de 1985, que preceptúa: "*Con la finalidad de facilitar la difusión de aquellos avisos que puedan interesar a los afiliados al sindicato y a los trabajadores en general, la empresa pondrá a su disposición un tablón de anuncios que deberá situarse en el centro de trabajo y en lugar donde se garantice un adecuado acceso al mismo de los trabajadores".*

Por ello, teniendo en cuenta que en este caso concreto la cesión de datos no requería el consentimiento del afectado por encontrarse autorizada en una Ley, tal y como preceptúa el artículo 11.2.a) de la Ley Orgánica 15/1999, la difusión de la revista del sindicato con los datos indicados entre el colectivo del organismo público, sin que se pudiera constatar su distribución entre personas ajenas a ese colectivo, lo que hubiera supuesto contravenir el principio de finalidad consagrado en la Ley Orgánica 15/1999, no suponía vulneración de lo dispuesto en esta Ley.

* También se archivó un procedimiento sancionador que se había iniciado en el año 1999, tras recibirse la denuncia de diferentes personas que habían recibido en sus domicilios particulares cartas remitidas por un sindicato con motivo de un acto sindical, sin que dichas personas hubieran facilitado al sindicato sus datos personales. Durante la tramitación del procedimiento se acreditó que los datos de algunos de los denunciantes constaban en los repertorios de abonados telefónicos, así como que algunos otros habían recibido en anteriores ocasiones envíos del mismo sindicato. Por ello, se aplicó para los primeros la excepción prevista en el artículo 6.2 de la Ley Orgánica 5/1992 respecto al requisito del consentimiento para aquellos datos que se habían recogido de fuentes accesibles al público. Y en cuanto al segundo grupo de denunciantes, se tuvo en consideración que los mismos, ya habían recibido un anterior envío y no habían mostrado su disconformidad con dicho tratamiento, lo que suponía un indicio de haber facilitado un consentimiento tácito al sindicato para el tratamiento de sus datos personales, tal y como mantiene consolidada Jurisprudencia del Tribunal Supremo. Por estas razones del Director de la APD decretó el archivo del procedimiento.

IV. SECRETARIA GENERAL

El Real Decreto 428/93, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos atribuye a la Secretaría General las actividades encaminadas a dotar y administrar los medios personales, materiales y técnicos para posibilitar el buen funcionamiento del Ente. Asimismo le atribuye las competencias relativas a la atención al ciudadano.

1. PLANIFICACIÓN, ORGANIZACIÓN Y GESTIÓN DE RECURSOS HUMANOS.

La estructura orgánica de la Agencia de Protección de Datos se configura, de conformidad con lo dispuesto en el artículo 11 del citado Real Decreto 428/93, en los siguientes órganos:

- El Director de la Agencia, asistido por su Secretaría Particular, Unidad de Apoyo y el Jefe del Gabinete Jurídico, que suponen un total de 9 funcionarios.

- El Consejo Consultivo

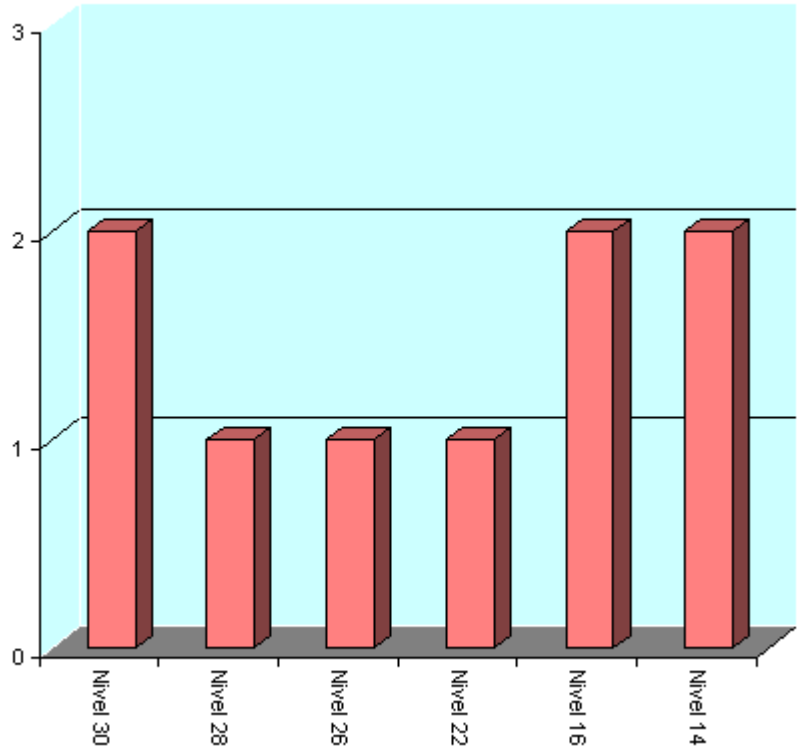
- El Registro General de Protección de Datos, integrado por 12 funcionarios.

- La Inspección de Datos, constituida por 27 funcionarios.

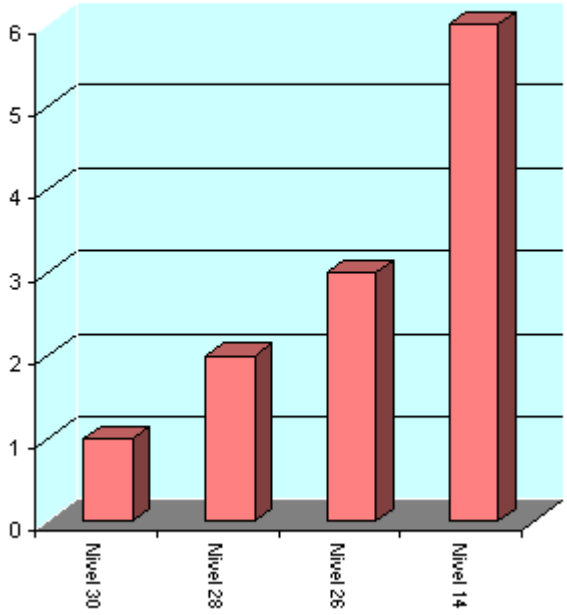
- La Secretaría General, integrada por 14 funcionarios y 2 laborales.

El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General se constituyen como órganos jerárquicamente dependientes del Director de la Agencia.

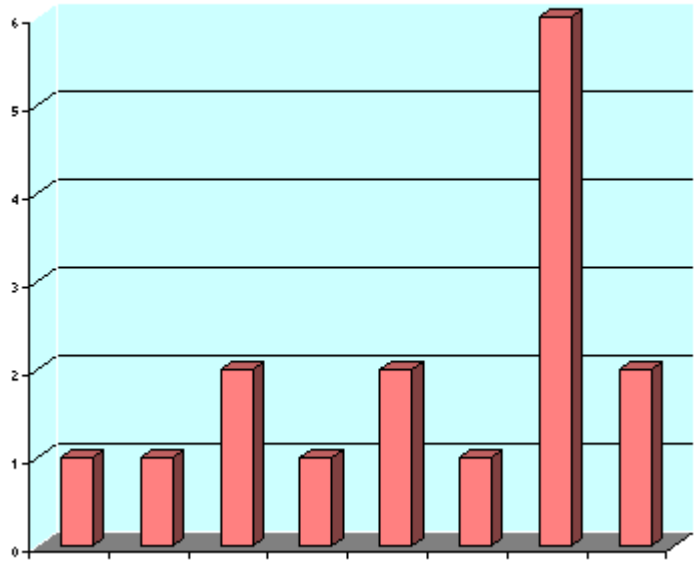
UNIDAD DE APOYO
Gráfico Secretaría General nº 1



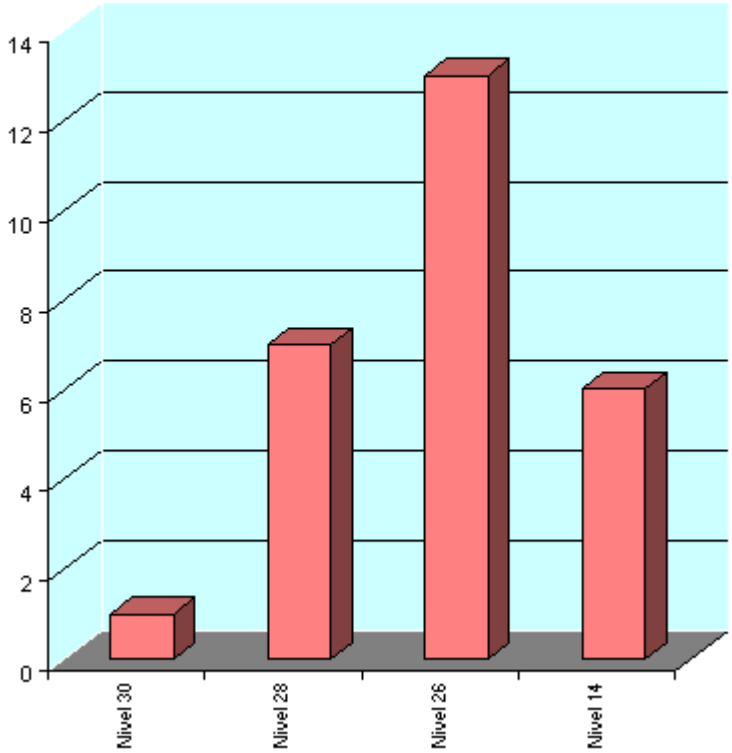
REGISTRO GENERAL DE PROTECCIÓN DE DATOS
Gráfico Secretaría General nº 2



SECRETARIA GENERAL
GRÁFICO SECRETARIA GENERAL Nº 3



INSPECCIÓN DE DATOS
Gráfico Secretaría General nº 4



En materia de Planificación, Organización y Gestión de Recursos Humanos se han realizado las siguientes actuaciones:

* Gestión y administración del personal funcionario y laboral destinado en la Agencia, y gestión de retribuciones y habilitación. Entre las actividades realizadas durante el año destaca, además de la gestión y administración ordinaria para el normal funcionamiento, la tramitación de un expediente de incremento de puestos de trabajo del Ente Público ante la Comisión Ejecutiva de la Comisión Interministerial de Retribuciones . Se ha puesto de manifiesto durante el 2000 la insuficiencia de la actual dotación de personal para el desarrollo de competencias propias de este Ente Público dado el gran volumen de actividad actual con perspectiva de constante crecimiento. Se ha considerado por ello indispensable acometer un incremento de la Relación de Puestos de Trabajo que permita atender las ascendentes necesidades de la Agencia. Al finalizar el año la indicada solicitud de aumento del número de funcionarios de la Agencia se encuentra en tramitación.

* Con fecha 4 de enero de 2000 se comunicó a la Agencia de Protección de Datos **la modificación de la Relación de Puestos de Trabajo,** tramitada el año anterior, **con un aumento** en los mismos en el sentido de aprobar los siguientes puestos:

1 Jefe de Servicio N. 26, para la Unidad de Apoyo

1 Instructor, para la Subdirección General del Registro General de Protección de Datos.

2 Inspectores Instructores

2 Jefes de Negociado N. 14, para la Subdirección General de la Inspección de Datos.

1 Jefe de Servicio de Sistemas Informáticos para la Secretaría General.

* Como consecuencia de lo anterior y para cubrir las bajas que se han ido produciendo a lo largo del año se han realizado las convocatorias para la provisión de puestos de trabajo que a continuación se detallan:

* Resolución de 9 de octubre de 2000, por la que se convocó una plaza, de libre designación, (BOE 16 octubre) de Secretario General, Nivel 30, adjudicado por Resolución de 10 de noviembre de 2000.

* Resolución de 2000 (BOE 3 de octubre) por la que se convocó concurso específico para la cobertura de los siguientes puestos de trabajo, resuelto con fecha 7 de noviembre de 2000:

Jefe De Área De Ficheros Privados, Nivel 28

Jefe De Servicio De Sistemas Informáticos, Nivel 26

Técnico Superior De Sistemas Informáticos, Nivel 26

Secretaria Puesto De Trabajo N. 30, Nivel 14

Jefe De Negociado De Información, Nivel 14

Jefe De Negociado, Nivel 14

- Resolución de 25 de septiembre de 2000, por la que se convocó una plaza, de libre designación, (BOE 2 de octubre) de Secretaria Director, Nivel 16, adjudicado por Resolución de 17 de noviembre de 2000.

- Resolución de 18 de mayo de 2000 (BOE 7 de junio) por la que se anuncia concurso específico para la provisión de un puesto de trabajo Inspector De Datos, Nivel 28, resuelto con fecha 17 de julio de 2000 (BOE del 31).

- Resolución de 24 de abril de 2000 (BOE 11 de mayo) por la que se convocó concurso específico para la provisión de los puestos de trabajo siguientes, resuelto con fecha 10 de julio de 2000, BOE del 21:

Secretaria Subdirector General, Nivel 14

Auxiliar Informático, Nivel 14

* Resolución de 27 de enero de 2000 (BOE del 15 de febrero) por la que se convocó concurso específico para la provisión de los puestos de trabajo siguientes, resuelto con fecha 30 de mayo de 2000, BOE de 14 de junio:

Inspector De Datos, Nivel 28

Jefe De Servicio, Nivel 26 (Unidad De Apoyo)

Subinspector, Nivel 26

Inspector Instructor, Nivel 26 (2 Plazas)

Instructor, Nivel 26

Jefe Servicio Sistemas Informáticos, Nivel 26 (Desierto)

Jefe De Negociado, Nivel 14 (2 Plazas)

* Resolución de 19 de enero de 2000 (BOE 1 de febrero) por la que se convocó una plaza, de libre designación, Consejero Técnico, Nivel 28, adjudicado por Resolución de 25 de abril de 2000 (BOE 9 de mayo).

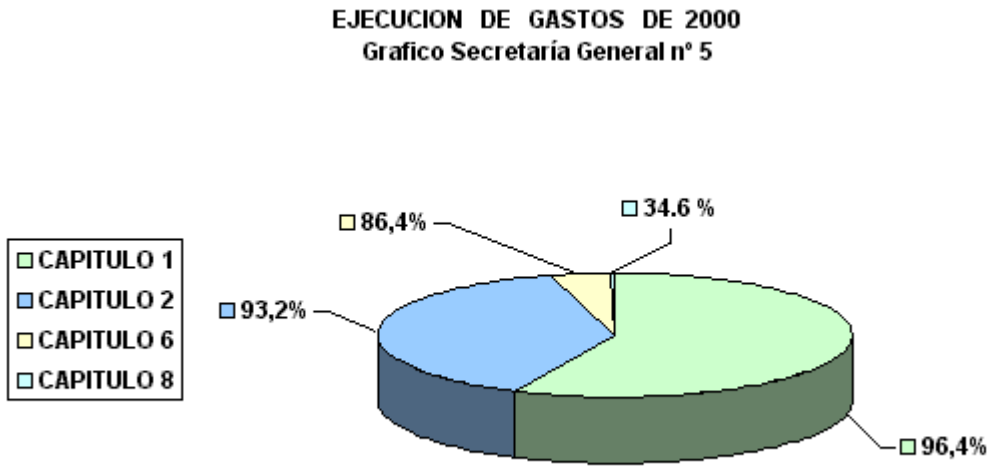
Para la provisión de todas las indicadas se han llevado a cabo las comisiones de valoración oportunas.

- Ejecución del Plan de Acción Social de la Agencia de Protección de Datos para 2000, siguiendo las recomendaciones previstas en el Acuerdo de Administración - Sindicatos sobre condiciones de trabajo en la Función Pública.

2. GESTIÓN ECONÓMICA Y PRESUPUESTARIA.

En cumplimento de lo dispuesto en el artículo 34 de la Ley Orgánica 15/99 y en los artículos 30 e), 32, 33, 34, 35 y 36 del Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia se han llevado a cabo las siguientes tareas y funciones:

- Ejecución y seguimiento presupuestario



- Modificaciones presupuestarias

- La contratación y la gestión presupuestaria y del gasto

- Gestión de los ingresos de la Agencia de Protección de Datos que han tenido su procedencia de transferencias establecidas en los Presupuestos Generales del Estado, intereses de cuentas corrientes, así como el pago de las sanciones impuestas por la Agencia en el ejercicio de la potestad sancionadora.

- Contrato de arrendamiento: Durante todo el año se ha mantenido un contrato de arrendamiento de las plantas 3ª, 4ª, y 5ª del edificio del Paseo de la Castellana nº 41, con una extensión de 1725 metros cuadrados. La duración de dicho contrato expiró el 31 de diciembre del año 2000. Con la finalidad de proporcionar un local a partir de la indicada fecha, acorde con las necesidades de la Agencia, y el de que dichos locales tengan una previsión de futuro con la que se pueda hacer frente a ampliaciones venideras, se llevó a cabo durante la primera parte del año acciones tendentes a la consecución de unos locales para lo que se estuvo en coordinación con la Dirección General de Patrimonio del Ministerio de Hacienda. Como consecuencia de lo anterior y tras las autorizaciones correspondientes, el 24 de julio de 2000 se firmó un contrato de arrendamiento del edificio Sagasta nº 22 de Madrid Plantas 1ª a 5ª y entreplanta. Dicho contrato de arrendamiento iba acompañado de uno de opción de compra que podía ser ejercitado a lo largo del año 2001. La propiedad el inmueble se comprometía a llevar a cabo las obras oportunas con objeto de que el mismo se acomodase a las necesidades de la Agencia. Dicho edificio debería ser entregado el 1 de enero del 2001.

- Asimismo se mantiene contrato de arrendamiento de un pequeño local destinado a almacén del Ente Público.

- Actualización permanente del inventario de los bienes y derechos que integran el patrimonio de la Agencia.

- Gestión de la Biblioteca de la Agencia: Ha continuado la adquisición de volúmenes y ejemplares para la formación de un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales.

3. OTRAS FUNCIONES Y TAREAS

- Notificación de las resoluciones del Director en cumplimiento de lo establecido en el artículo 30, b) del Real decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

- Total de Notificaciones efectuadas 1780

- De procedimientos a Administraciones Públicas 173

- De actuaciones previas 486

- De Procedimientos sancionadores 758

- De Tutela de Derechos 363

* Estas cifras no tienen porqué coincidir necesariamente con las de expedientes, procedimientos y actuaciones de la Inspección (ver el apartado de la Memoria dedicado a la Inspección de Datos), toda vez que una actuación inspectora habitualmente da lugar a diversas notificaciones por la existencia de una pluralidad de personas que legalmente deben

ser notificadas.

_ Registro de Entrada y Salida de documentos en la Agencia

Registros de Entrada 21.448 (incremento del 79,93% respecto 1999)

Registros de Salida 39.797 (incremento del 131,29% respecto 1999)

Estas cifras son reveladoras del notable auge de la actividad de la Agencia.

- En cumplimiento del mandato establecido en el artículo 22 del Estatuto de la Agencia la Secretaría General ha actuado como Secretaria del Consejo Consultivo en las 3 reuniones celebradas durante el año 2000. El contenido de las reuniones se concreta en el apartado de la memoria relativo al Consejo Consultivo.

- Ha sido también competencia de esta Secretaría General la organización en colaboración con la Universidad Pública de Navarra de unas Jornadas sobre "Protección de la Privacidad, Telecomunicaciones e Internet" en Pamplona durante los días 22 y 23 de junio de 2000.

Asimismo se ha llevado a cabo la convocatoria, fallo y entrega de la 4ª edición del Premio "Protección de Datos Personales" y del Primer Premio de Periodismo "Protección de Datos Personales.

De estas últimas actuaciones se da cumplida información en los puntos 3 y 4 del epígrafe de esta memoria "OTRAS ACTIVIDADES".

4. EL ÁREA DE ATENCIÓN AL CIUDADANO

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (en adelante LOPD) establece en su artículo 37, apartado e) la función de la Agencia de Protección de Datos de proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal. Esta función viene atribuida a la Secretaría General de la Agencia por el artículo 31 apartado d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, que la ejerce a través del Área de Atención al Ciudadano, siendo pues ésta la puerta de acceso con la que los ciudadanos se encuentran cuando vienen a plantear sus consultas o dudas ante la APD respecto al tratamiento que con sus datos personales pueden realizar terceros ajenos a ellos mismos y que por lo tanto pueden escapar de su control.

Es por ello, que una de las funciones primordiales de esta Unidad, es la de tratar de informar a los ciudadanos de la forma más sencilla posible sobre aquellas cuestiones que les preocupan directamente, facilitándoles la orientación y ayuda que precisen para una mejor defensa de sus derechos, e indicándoles los diferentes aspectos que se regulan en la LOPD y en el resto del ordenamiento jurídico de aplicación en esta materia.

La atención que se presta por el Área, se puede dividir básicamente en dos partes. De un lado, la atención personalizada al ciudadano, y de otro, la información a través de la página Web de la Agencia: www.agenciaprotecciondatos.org

La atención personalizada se realiza directamente por el personal adscrito al Área y se materializa de tres formas, como son: la atención telefónica, la atención presencial y la atención por escrito.

Seguidamente, se pasa a detallar el número de consultas atendidas a lo largo del año 2000, reflejándolas en el siguiente cuadro:

Atención telefónica	Atención presencial	Atenciónpor escrito	Total
14420	1878	2964	19262

Comparativamente y tal y como se reflejó en la memoria del año 1999 el número de consultas atendidas fue de:

Atención telefónica	**Atención presencial**	**Atenciónpor escrito**	**Total**
11500	1150	1739	14389

Un primer análisis de estas cifras implica que se ha producido un aumento considerable en las tres formas de atención, que se corresponden con un **25% en la atención telefónica**, un **63% en la atención presencial** y destacando, un incremento del **70% en las consultas escritas**. Como se observa, el incremento mas importante lo experimentan las consultas escritas y ello es debido a la posibilidad inmediata de formalizarlas a través de la página Web. Esta posibilidad, que ya fue objeto de mención en la memoria de 1999, se ha confirmado y consolidado a lo largo del año 2000,

siendo la tendencia más habitual del ciudadano el utilizar la página Web para formalizar sus consultas.

En efecto, si se compara el número de consultas presentadas a través de la página Web durante los años 1999 y 2000, se desprende que éstas han pasado de 654 a 1700, lo que supone un **160% de incremento**, que confirma, que efectivamente se ha invertido la forma de consultar por parte de los ciudadanos.

Por otro lado, es importante señalar que el acceso al resto de la información contenida en la página Web de la Agencia, ha aumentado en proporciones igual de considerables con respecto al año 1999, pasando de un total de 506.362 accesos a un total de 1.173.056 accesos, lo que supone un **132 % de incremento**.

Número total de accesos a la página Web durante el año 2000

enero	61599
febrero	86697
marzo	136004
abril	96429
mayo	62020
junio	101569
julio	96194
agosto	77362
septiembre	99939
octubre	119169
noviembre	130167
diciembre	105907
total	**1173056**

En dicha página se contiene una guía informativa, los modelos para ejercer los derechos de acceso, rectificación y cancelación, las recomendaciones a usuarios de Internet, legislación en la materia de protección de datos, los modelos de cuestionarios para notificar la inscripción de ficheros tanto de titularidad pública como privada al Registro General de Protección de Datos, así como el catálogo actualizado de ficheros inscritos en la Agencia. Como novedad con respecto al año 1999 se destaca que en el año 2000 y dentro de los contenidos de la página se han incorporado a la misma un apartado con las consultas más frecuentes, así como el programa informático para la declaración de los ficheros a través de Internet.

Con respecto al apartado de consultas más frecuentes hay que señalar que, la inclusión del mismo dentro de la página Web era uno de los objetivos de esta Unidad, dado, que tal y como se ha ido reflejando a lo largo de las sucesivas memorias de la Agencia, existe un gran número de consultas que inciden sobre los mismos temas, y por ello se consideró que, en aras de facilitar una mayor y mejor información al ciudadano, se incluyese dentro de la información general facilitada a través de la página, este apartado.

Dentro de este apartado, se han incluido un total de 16 contestaciones a los temas más frecuentes, poniendo la advertencia de que la información que se contiene en las mismas es aquella que, con carácter general, se está facilitando, careciendo dicha información de efectos vinculantes para la Agencia de Protección de Datos.

La relación de consultas más frecuentes es la siguiente:

1.- Envíos publicitarios

2.- Datos de facturación telefónica

3.- Datos de las Guías Telefónicas

4.- Ámbito de aplicación de la ley

5.- Acceso ante responsable conocido

6.- Acceso ante la Agencia de Protección de Datos sobre datos personales

7.- Ficheros de información de solvencia patrimonial y crédito (Ficheros de morosos)

8.- Ficheros de información de solvencia patrimonial y crédito que incluyan datos de fuentes accesibles al público

9.- Direcciones de ficheros de información de solvencia patrimonial

10.- Inscripción de ficheros

11.- ¿¡Cómo se deben declarar los ficheros de datos?

12.- Presentación del documento de seguridad

13.- Medidas seguridad (Fichero de nóminas)

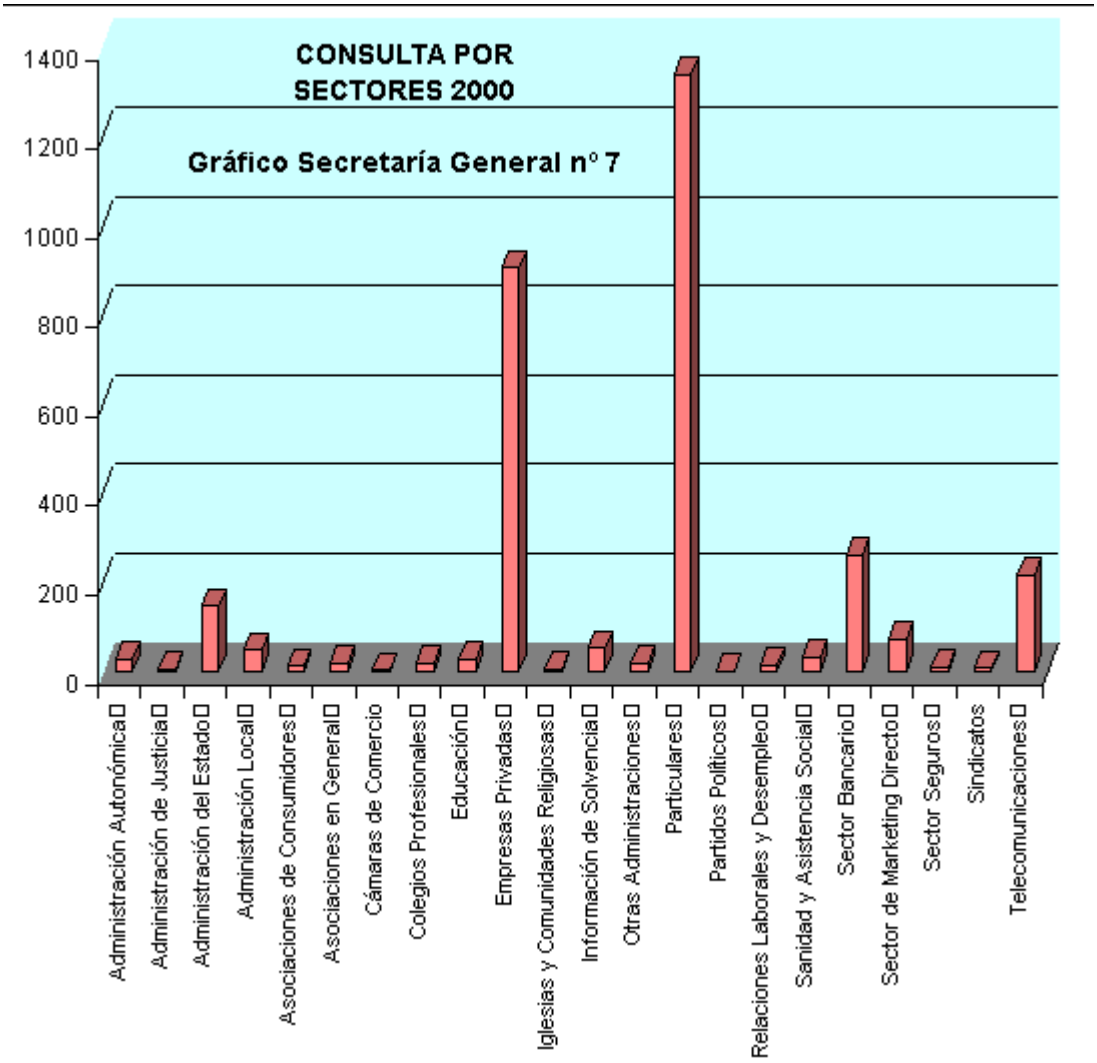
14.- Medidas seguridad (Datos de Hacienda Pública)

15.- Medidas seguridad (Servicios financieros)

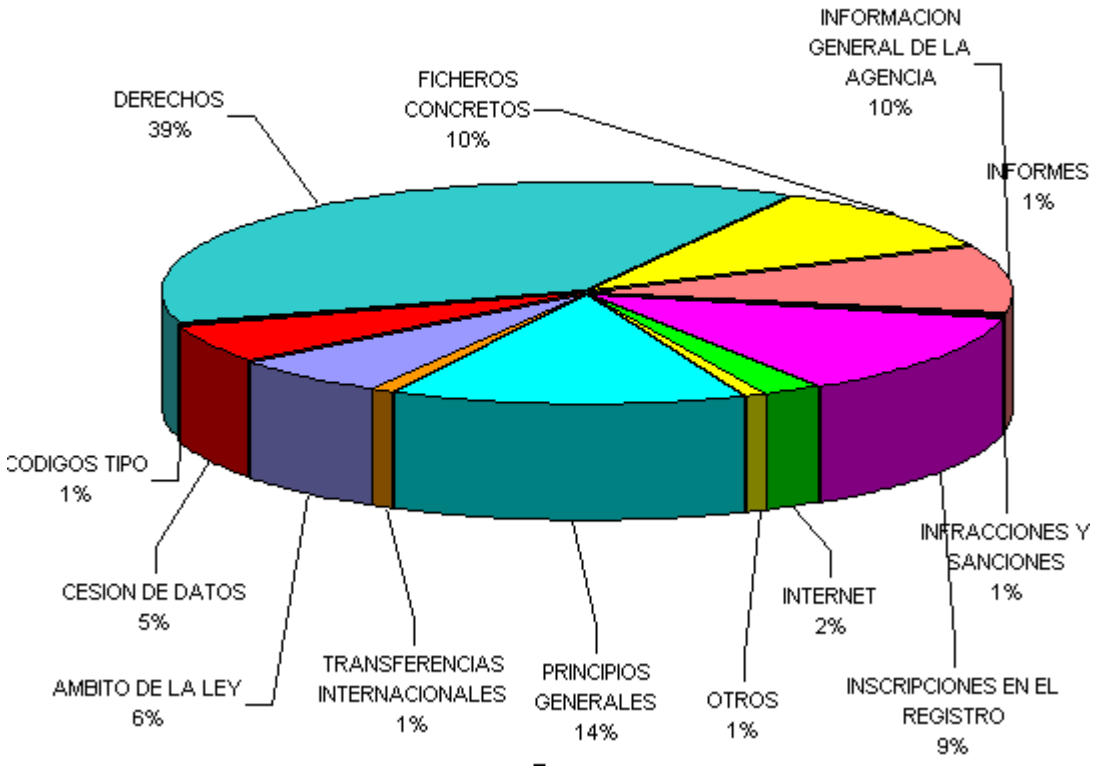
16.- Implantación de medidas de seguridad nivel medio

La importancia de este apartado queda reflejada en el número de accesos que ha tenido y así, según los informes habilitados a partir del mes de noviembre de 2000 por el proveedor de servicios, en los que se detallan aquellos apartados de la Web más consultados, es significativo que en concreto, al apartado de consultas más frecuentes, se haya accedido en el mes de noviembre en 2.122 ocasiones, y en el mes de diciembre en 1.572 ocasiones.

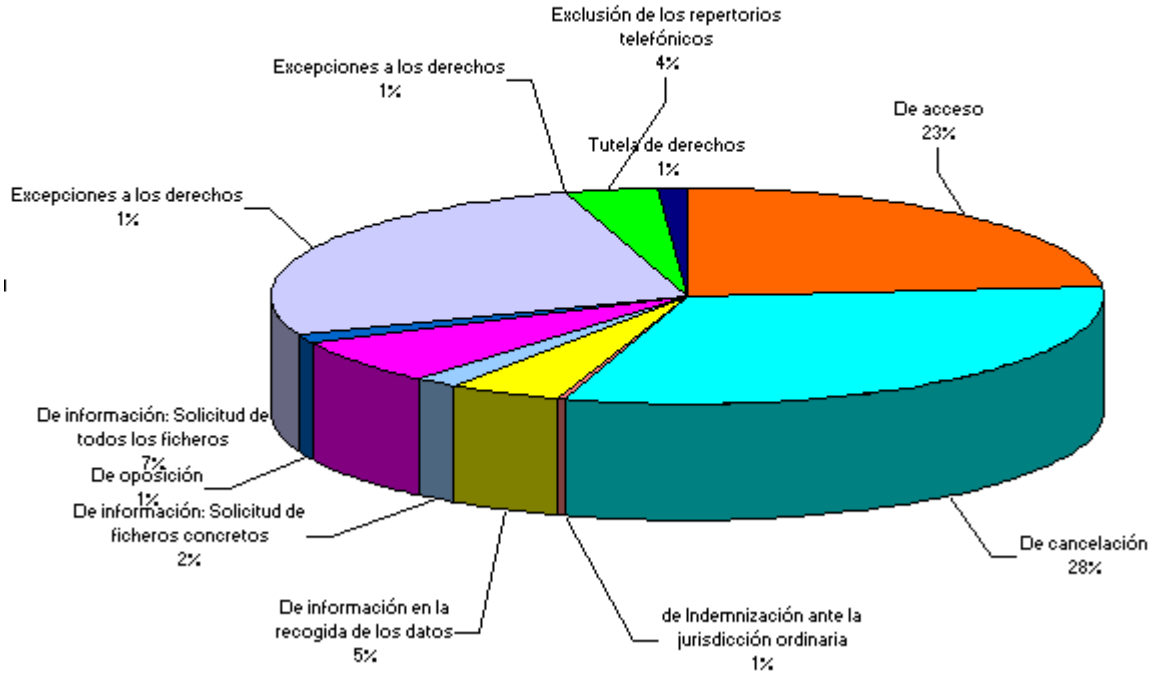
Seguidamente, y antes de entrar a exponer aquellas consultas de mayor interés, se procede a insertar una serie de gráficos, en donde queda reflejada la distribución por sectores y temas del global de las consultas planteadas durante el año 2000.



CONSULTAS POR TEMAS 2000
Gráfico Secretaría General nº 8

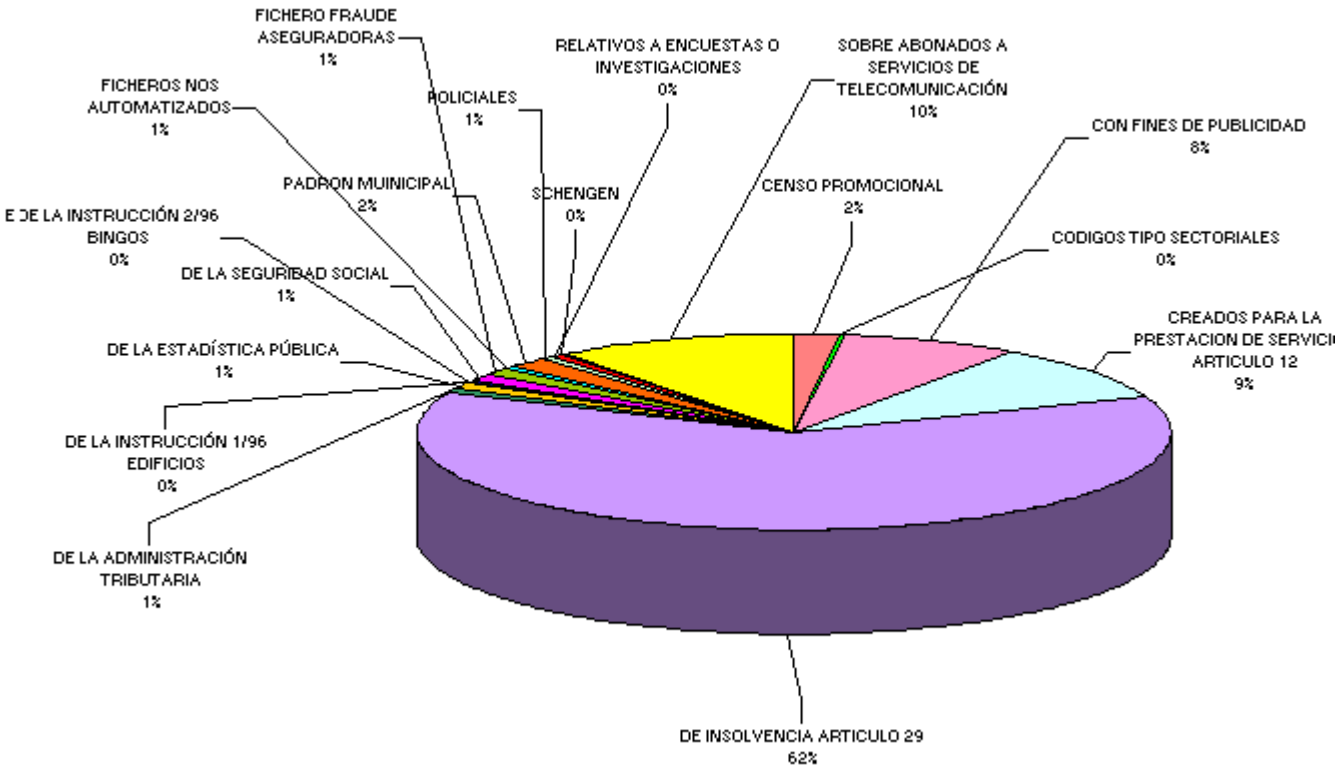


TIPOS DE CONSULTAS SOBRE DERECHOS 2000
Gráfico Secretaría General nº 9

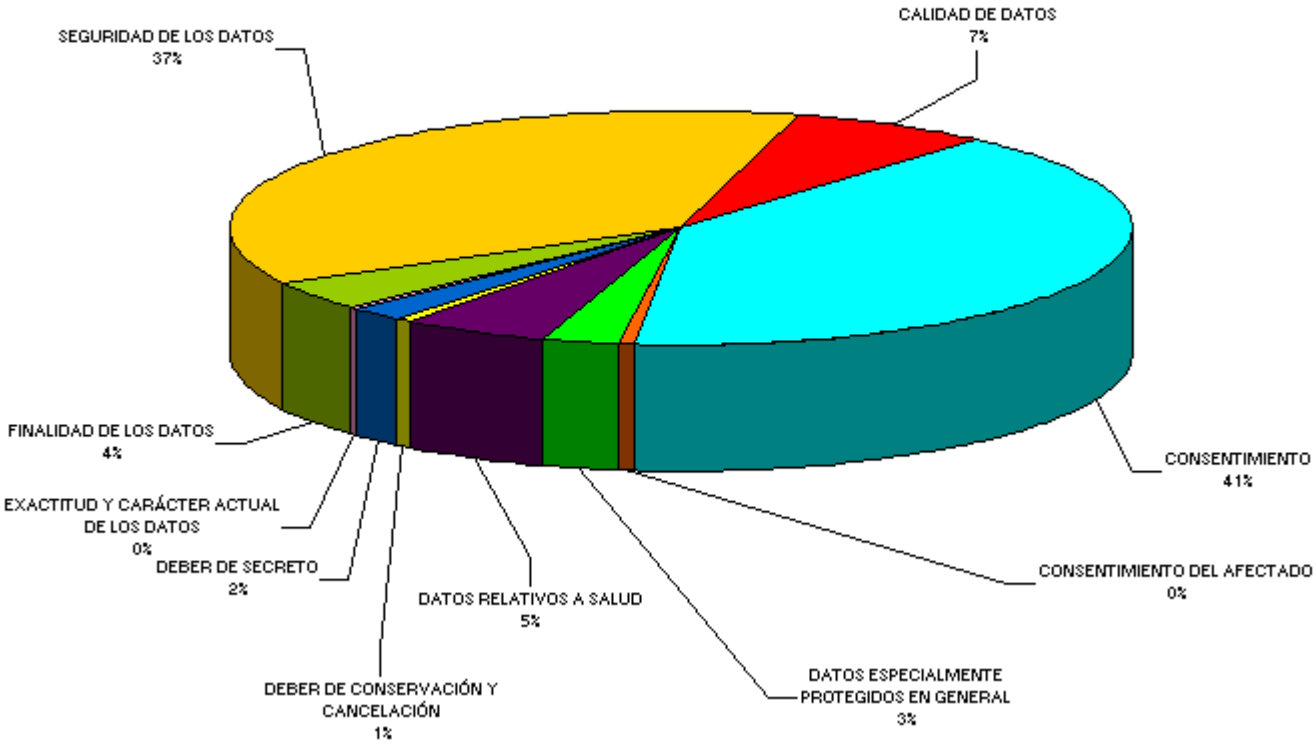


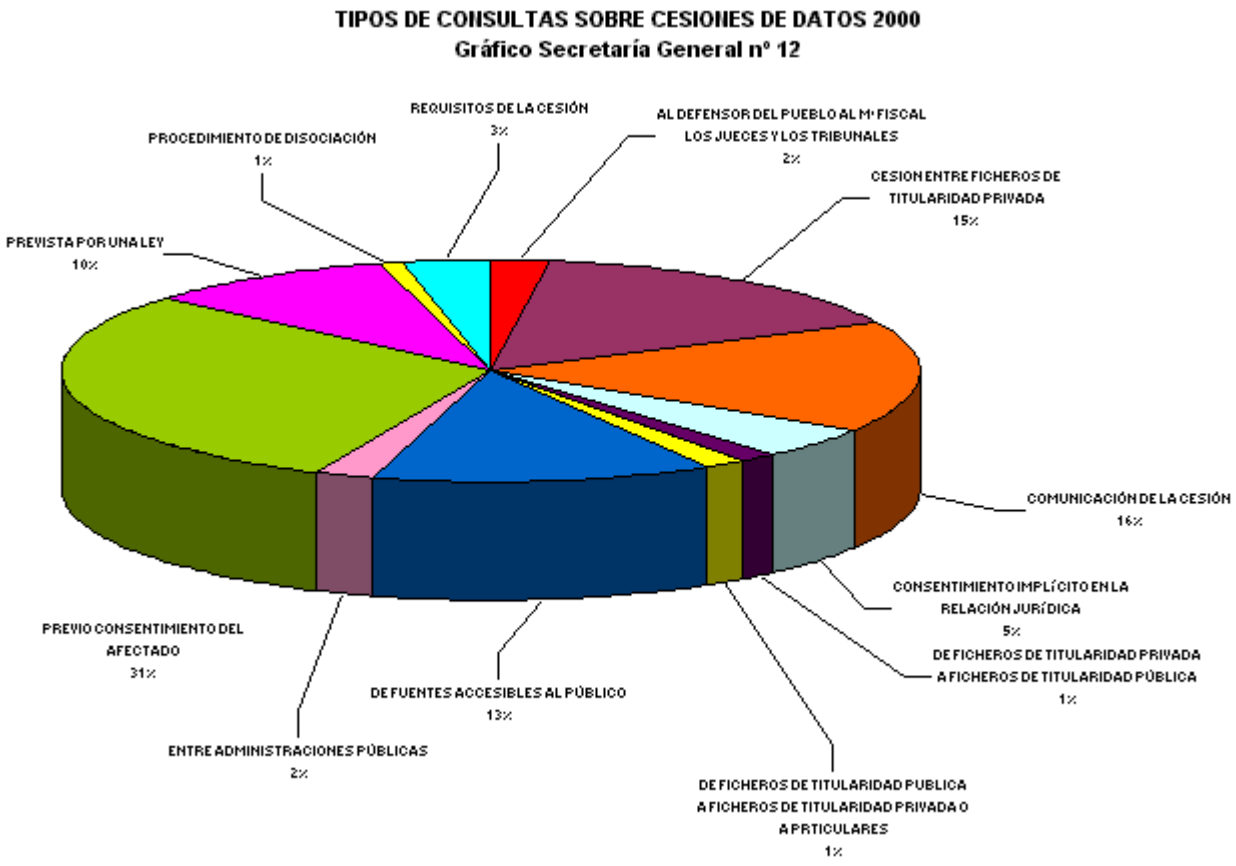
FICHEROS CONCRETOS 2000

Gráfico Secretaria General nº 10



CONSULTAS SOBRE PRINCIPIOS GENERALES 2000
Gráfico Secretaría General nº 11





A continuación, y de la misma forma que en las memorias de los años anteriores dado el interés que las consultas de los ciudadanos pueden despertar, se procede a publicar en esta memoria aquellas consultas que se ha considerado de mayor importancia por la cuestión planteada, distribuyéndolas en los siguientes apartados:

* RELACIONES LABORALES

* CESION DE DATOS

* DATOS DE SALUD

* DERECHOS DE ACCESO, RECTIFICACION, CANCELACION Y OPOSICION

* INTERNET Y PAGINAS WEB

* REGLAMENTO DE SEGURIDAD

* SECTOR DE TELECOMUNICACIONES

* SECTOR SEGUROS

* RELACIONES LABORALES

Dentro de este apartado, en primer lugar se incluye la posibilidad planteada de crear una base de datos con trabajadores conflictivos, así como la de si los Comités de Empresa pueden dar publicidad a los datos de cotización de la seguridad social de los trabajadores de la empresa, y, también, en que medida están protegidos los datos de las retribuciones de los trabajadores facilitados al Comité de Empresa. También se expone otra consulta relativa a si se puede publicar en una página Web de una empresa el censo electoral de los trabajadores y por último, se incluye la consulta planteada por un miembro de la policía respecto a si existe el derecho al borrado físico de los datos que sobre sanciones disciplinarias figuren en el expediente personal.

- *Creación de una base de datos con trabajadores conflictivos*

Se plantea una consulta sobre si es legal la existencia de una base de datos compuesta por los datos de trabajadores

que han tenido problemas en empresas, para que pueda ser consultada por terceros.

En esta consulta se informó en primer término que la creación de un fichero común de datos de trabajadores conflictivos suministrado por las empresas que hayan tenido problemas con estos trabajadores, para así dar a conocer estos datos a terceras empresas que pretendan contratar con ellos, no está previsto en la LOPD como una situación especial y excepcional a la regla general del consentimiento prevista en el artículo 11.

Los únicos ficheros comunes que se regulan en la Ley Orgánica son los ficheros de información de solvencia patrimonial y crédito regulados en el artículo 29, conocidos popularmente como ficheros de morosos, así como los ficheros comunes para la liquidación de siniestros y prevención del fraude creados por las Compañías Aseguradoras previstos en la disposición adicional sexta de la Ley.

A la vista por tanto de lo anteriormente señalado, se indica que la existencia de un fichero común de las características indicadas implicaría, de un lado, el que dicho fichero debería ser declarado al Registro General de Protección de Datos para su inscripción, o no, en función de que cumpliera con los principio de la LOPD, y de otro, el que para la cesión de los datos por parte de las empresas a dicho fichero se necesitaría el consentimiento de los trabajadores afectados, dado que dicha información excedería del ámbito de cada una de las empresas y sería de aplicación la regla general prevista en el artículo 11.1 de la Ley Orgánica que expresamente establece que: "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."

Finalmente se informó que una actuación contraria a lo previsto en el referido artículo 11 podría ser constitutiva de una infracción muy grave.

- ¿¡Los Comités de Empresa pueden dar publicidad a los datos de cotización de los trabajadores?

Se plantea esta consulta sobre la posibilidad de que se hagan públicos por el Comité de Empresa dentro del ámbito de la propia empresa los datos de cotización a la seguridad social de los trabajadores.

En primer término se indicó que hay que atender a las competencias que el artículo 64 del Estatuto de los Trabajadores reconoce a los Comités de Empresa y en ese sentido se establece en el apartado 9º, la de vigilancia en el cumplimiento de la normas laborales, de seguridad social y empleo, así como el resto de los pactos, condiciones y usos de la empresa en vigor.

En función de esta competencia, en principio, podría estar justificado que el Comité de Empresa tenga acceso a la información contenida en los formularios TC-2 de la empresa, pero sin embargo no parece que dicha competencia habilite a hacer públicos dichos datos dentro del seno de la empresa, dado que, ello podría contravenir el principio de calidad de datos contenidos en el artículo 4 de la LOPD y en concreto lo dispuesto en su apartado 1 que expresamente establece:

"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

- ¿¡Cómo están protegidos los datos de retribuciones de los trabajadores facilitados a los Comités de Empresa?

En esta consulta se puso de manifiesto que los Comités de Empresa deberán tener acceso a la información salarial de los trabajadores al objeto de poder negociar el Convenio Colectivo. Partiendo de esta premisa y de la necesidad de facilitar dicha información, lo que si es evidente, es que dichos datos se deberían de facilitar de forma disociada, dado que los únicos datos personales de los trabajadores a los que puede tener acceso el Comité de empresa, son aquellos que formen parte de la copia básica de los contratos y aunque en ellos figuren las retribuciones iniciales, no así, figuran las sucesivas revisiones salariales que se hayan podido aplicar a cada uno de los trabajadores.

Respecto a la obligación de guardar secreto por parte de dicho Comité, se le indica que dicha obligación les viene impuesta por el artículo 65 del Estatuto de los Trabajadores, donde se regula la capacidad y el sigilo profesional de estos Comités.

- Publicación del censo electoral de trabajadores en una página Web de la empresa

En esta consulta se interesaba conocer la posibilidad de publicación en una página Web del censo electoral de trabajadores de la empresa, como consecuencia de la celebración de elecciones sindicales.

Se informó que con carácter general la regulación del procedimiento electoral en el ámbito de las empresas viene regulada en los artículos 69 y siguientes del Estatuto de los Trabajadores.

En concreto, la publicación del censo electoral es una de las funciones conferidas a la mesa electoral por el artículo 74. 3 ET, estableciendo expresamente que la mesa electoral, una vez constituida, solicitará al empresario el censo laboral y confeccionará, con los medios que le habrá de facilitar éste, la lista de electores. Esta se hará pública en los tablones de anuncios mediante su exposición durante un tiempo no inferior a setenta y dos horas.

La LOPD regula dentro de su artículo 4 el principio de calidad de datos, por el que se establece que sólo se podrán

recoger datos personales para su tratamiento, así como someterlos al mismo, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

El procedimiento de elecciones sindicales dentro de las empresas está limitado al ámbito de las mismas, independientemente de que con posterioridad el resultado final deba ser comunicado al Ministerio de Trabajo. Es por ello que, en principio, parece que la publicación del censo electoral de los trabajadores de la empresa, únicamente se podrá realizar dentro de su ámbito y ese es el sentido de la publicación en los tablones de anuncios y no en una página Web, dado que estaría transcendiendo al ámbito de la empresa y no sería esa la finalidad de dicha publicación. Cosa distinta es que se publicase en una red interna de la propia empresa.

- ¿¡Existe la posibilidad del borrado físico de los datos que sobre sanciones disciplinarias a la policía consten en sus expedientes personales?

Se informó que los datos que figuran en el fichero de personal de la Dirección General de la Policía están bajo el ámbito de aplicación de la LOPD en virtud de lo establecido con carácter general en el artículo 2 de dicho texto legal.

Por lo que se refiere al borrado físico de los datos se señaló que la LOPD establece en su artículo 4.1, al regular el principio de calidad de datos, el que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos al mismo, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Igualmente, el apartado 5 de dicho artículo establece que los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

También se indicó, que con carácter general está reconocido en el artículo 16 de la LOPD el derecho de rectificación y cancelación.

Finalmente y por lo que se refiere al supuesto concreto se indicó la regulación específica que podría ser de aplicación y que está recogida en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado, estableciendo en su artículo 28.2 que:

" ....Las sanciones disciplinarias se anotarán en los respectivos expedientes personales con indicación de las faltas que las motivaron.

Transcurridos dos o seis años desde el cumplimiento de la sanción, según se trate de faltas graves o muy graves no sancionadas con la separación del servicio, podrá acordarse la cancelación de aquellas anotaciones a instancia del interesado que acredite buena conducta desde que se le impuso la sanción. La cancelación de anotaciones por faltas leves se realizará a petición del interesado, a los seis meses de la fecha de su cumplimiento. La cancelación producirá el efecto de anular la anotación sin que pueda certificarse de ella, salvo cuando lo soliciten las Autoridades competentes para ello y a los exclusivos efectos de su expediente personal."

El principio general de calidad de datos obligaría a cancelar los datos cuando hayan dejado de ser necesarios para la finalidad para la que se recogieron, pero en este caso concreto la propia finalidad viene establecida en la Ley Orgánica 2/1986, señalando que la cancelación anulará la anotación y no podrá certificarse sobre ella, salvo cuando lo soliciten las Autoridades competentes, por lo que ello llevaría a concluir, en principio, que el borrado físico de los datos no puede producirse, dado que en ese caso no se podría cumplir con lo dispuesto en el referido artículo 28.2 al no poder emitir la certificación cuando sea requerida por la Autoridad competente.

CESION DE DATOS

Las consultas sobre cesión de datos han sido también bastante frecuentes, pero únicamente se van a reflejar aquellas que han tenido una especial incidencia. Así, se pone de manifiesto que han sido varias las quejas sobre la carta enviada a sus abonados, por empresas pertenecientes a un grupo del sector eléctrico, solicitándoles el consentimiento para la cesión de sus datos al grupo. De otra parte, también en varias ocasiones se ha consultado sobre si una entidad bancaria estaba actuando de acuerdo con la LOPD al pedir el consentimiento para la cesión de los datos de sus clientes. También se ha consultado si la obtención fraudulenta de datos pudiese ser motivo de infracción penal.

- Encarte de las empresas de un grupo del sector eléctrico

Se ha planteado en varias ocasiones si la carta enviada a los abonados por las empresas asociadas a un determinado grupo del sector eléctrico solicitándoles el consentimiento para proceder a comunicar sus datos personales al resto de empresas del Grupo, era correcto

Se indicó que, si del contenido de la carta enviada por la empresa se puede apreciar por los abonados del servicio eléctrico que presta dicha empresa, la finalidad explícita, determinada y legítima a la que se van a destinar los datos, la carta en principio sería conforme a la LOPD, dado que en cualquier caso se está comunicando al propio grupo.

Finalmente y respecto de la forma de solicitar el consentimiento se ha señalado que la LOPD solo habla de necesidad de consentimiento expreso y por escrito en el artículo 7 que regula los datos especialmente protegidos, es decir aquellos datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, o bien aquellos que

hagan referencia al origen racial, a la salud y a la vida sexual.

Es por ello, que si el legislador hubiera considerado que el consentimiento hubiera de ser siempre expreso no habría distinguido entre diversas clases de supuestos o modalidades para prestarlo. En este sentido se informó que el Tribunal Supremo, en varias sentencias, interpreta que: **Fuera de los casos en que la Ley exige una declaración expresa, el consentimiento en los negocios jurídicos puede ser prestado en forma tácita**

Por tanto, el consentimiento tácito para la cesión de datos, puede ser válido, siempre que no se trate de datos especialmente protegidos.

No obstante, correspondería a la entidad que ha solicitado su consentimiento, la prueba de que lo ha obtenido en cada caso concreto.

Finalmente también se indica que, aunque el consentimiento se haya prestado en algún momento para la cesión de datos, este siempre tendrá el carácter de revocable como establece el artículo 11.4 LOPD.

* *Cambio de finalidad en el tratamiento y cesión de datos a las empresas participadas dentro de un grupo bancario*

Esta consulta ponía de manifiesto la disconformidad con la comunicación cursada por una entidad bancaria a sus clientes, en la que se informaba del nuevo tratamiento que se iba a realizar con sus datos personales, así como de la posibilidad de cesión de los mismos a las entidades del grupo o a entidades participadas.

Se indicó respecto del cambio de finalidad y del nuevo uso que van a realizar con los datos, que la LOPD regula dentro de su artículo 4, apartados 1 y 2, que:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos....."

Asimismo en el artículo 6.1 se establece que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa."

A la vista de las disposiciones anteriores se desprende que la actuación de la entidad bancaria respecto del nuevo tratamiento, podría ser conforme a derecho, dado que al variar la finalidad del tratamiento de los datos de sus clientes con el objeto de mejorar la promoción comercial de sus propios servicios, les está solicitando a cada uno de ellos el consentimiento para poder realizar dicho tratamiento, situación acorde con lo que establecen dichos preceptos.

Respecto de la cesión de sus datos se le señaló, al igual que en el caso del grupo eléctrico anteriormente expuesto, que la LOPD dentro de su artículo 11 regula la comunicación de datos, estableciendo el principio de que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

No obstante, el propio artículo 11 establece que, será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar. En este sentido se le señala que la finalidad deberá ser determinada, explícita y legitima.

Del contenido de la carta enviada por la entidad bancaria, no se podía apreciar por los clientes, la finalidad explícita, determinada y legítima a la que se iban a destinar los datos, ni tampoco quedaban determinados los destinatarios de la cesión, por lo que en principio, dicha comunicación no tendría validez.

A estos efectos y dado que la carta anterior carecería de validez en la parte de la cesión, se informó que si con posterioridad al envío de estas comunicaciones se hubiera procedido por las empresas pertenecientes al Grupo a tratar los datos de aquellas personas que no se han opuesto a la cesión, dicho tratamiento podría ser denunciado a la Agencia.

Se terminó poniendo de manifiesto, al igual que en la consulta anterior, que la forma tácita de solicitar el consentimiento es lícita, siempre que no se trate de datos especialmente protegidos, correspondiendo a la entidad que lo ha solicitado la prueba de que lo ha obtenido en cada caso concreto y señalando que dicho consentimiento tiene el carácter de revocable (art.11.4 LOPD).

- *Obtención de datos de forma fraudulenta*

En este caso se solicitaba información sobre si el comprar o conseguir de forma fraudulenta información reservada sobre datos personales, revelando la misma a terceras personas ajenas a dicha información sin permiso o autorización de los titulares, puede ser causa de infracción penal

En primer lugar se indicó que la LOPD prevé como una infracción administrativa muy grave la obtención de datos de forma engañosa y fraudulenta (art. 44.4.a).

Asimismo, también prevé como infracción muy grave la comunicación o cesión de datos de carácter personal fuera de los casos en que estén permitidas (art. 44.4.b). En este sentido se le señala que según lo previsto en el artículo 11.2 de la LOPD no será preciso el consentimiento de las personas afectadas para la cesión o comunicación de datos en los siguientes supuestos:

- *Cuando la cesión está autorizada en una Ley.*

- *Cuando se trate de datos recogidos de fuentes accesibles al público.*

- *Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique*

- *Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.*

- *Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*

Finalmente también se le informó, aunque no es materia de conocimiento de la Agencia de Protección de Datos, que el Código Penal tipifica dentro del Título X los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y en concreto en su artículo 197 los delitos del descubrimiento y revelación de secretos.

DATOS DE SALUD

Dentro de este apartado se recogen dos consultas que van referidas, la primera, a cesión de datos de salud de los trabajadores de una empresa a una compañía de seguros para contratar un seguro de riesgo. La segunda plantea la posibilidad de si desde un Colegio Oficial de Farmacéuticos se puede transmitir a terceros ajenos al INSALUD información de la farmacia donde se dispensó una receta médica.

- *Cesión de datos de salud con el objeto de contratar por la empresa un seguro de riesgo*

En este caso se solicitó información sobre el cuestionario que había envia sus trabajadores la dirección de Recursos Humanos de una empresa del sector de los medios de comunicación, cuestionario que debían de rellenar al objeto de que se contratase un Seguro de Riesgo con una entidad aseguradora.

Se puso de relieve la existencia en la LOPD de dos principios básicos de la protección de datos y que se refieren al principio de calidad de datos y al principio del consentimiento para poder ceder los datos a un tercero.

El artículo 4 de la LOPD regula el principio de calidad de datos y establece básicamente que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Por otra parte el artículo 11.1 establece que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

A la vista de la regulación anterior se le informó que, para la suscripción voluntaria de un seguro de riesgo ofrecido por la empresa donde trabaja, el hecho de que se faciliten una serie de datos de salud como los incluidos en el cuestionario no contravendría el principio de calidad, siempre que dichos datos sean adecuados, pertinentes y no excesivos en relación precisamente con la contratación del seguro.

No obstante sí se resaltó que, respecto de la petición del consentimiento para poder ceder los datos recogidos en el cuestionario a la entidad aseguradora y empresas de su grupo, el propio artículo 11 establece que, será nulo dicho consentimiento cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar. En este sentido se le señala que la finalidad deberá ser determinada, explícita y legitima.

De acuerdo con la regulación anterior se desprende que, del contenido de la cláusula de cesión que figura en el Boletín de Adhesión del Seguro, no se aprecia la finalidad explícita, determinada y legítima a la que se van a destinar los datos, ni tampoco quedan determinados los destinatarios de la cesión, por lo que dicha comunicación no tendría validez.

Igualmente, y por lo que se refiere a la forma de solicitarle el consentimiento, tanto para el tratamiento de sus datos como para la cesión de los mismos, se le indica que no valdría el consentimiento tácito, dado que la LOPD cuando se trata de datos de salud requiere la necesidad del consentimiento expreso, regulándolo así en el artículo 7.3.

Por tanto, el consentimiento tácito para el tratamiento y la cesión de datos, tal y como viene previsto en el Boletín de Adhesión no podría ser valido dado que se trata de datos especialmente protegidos.

A la vista de lo anteriormente señalado se concluyó señalando que, o se acredita la concurrencia de los dos requisitos indicados para así poder excepcionar la necesidad del consentimiento expreso de cada uno de los empleados en situación de incapacidad laboral, o el tratamiento de los datos de salud por parte de su empresa no se podría realizar sin la manifestación expresa de dicho consentimiento, o cuando por razones de interés general lo dispusiese una Ley.

- *Cesión de datos por parte de un Colegio Oficial de Farmacéuticos a terceros que no sea el INSALUD.*

Esta consulta fue planteada por una farmacéutica y preguntaba si desde un Colegio Oficial de Farmacéuticos se puede transmitir a terceros (no al INSALUD) información de la farmacia donde se dispensó una receta médica, en base a los datos de esos archivos.

Se le señaló que en esta materia la actuación de los Colegios Farmacéuticos, se rige por el Concierto firmado con fecha 17/11/98, entre el Presidente Ejecutivo del INSALUD y el Director General de la Tesorería de la Seguridad Social, por una parte, y el Presidente del Consejo General de Colegios Oficiales de Farmacéuticos, por otra, Concierto por el que se fijan las condiciones para la ejecución de la prestación farmacéutica a través de las oficinas de farmacia.

Dicho Concierto tiene por objeto la fijación de las condiciones en que las Oficinas de Farmacia colaborarán profesionalmente con el INSALUD en lo referente al control de la dispensación de las especialidades farmacéuticas, fórmulas magistrales y preparados oficiales que estén incluidos en la prestación farmacéutica de la Seguridad Social, de acuerdo con la legislación vigente y las especificaciones señaladas en este Concierto.

En la cláusula 2 se establece que el Concierto se regulará por sus condiciones particulares, siendo de aplicación directa la normativa sanitaria por la que se regula la prestación farmacéutica en general y, en su caso la de Seguridad Social en particular, así como la Ley Orgánica 5/1992, de 29 de octubre de Regulación de Tratamiento Automatizado de Datos de Carácter Personal (LORTAD) hoy derogada y sustituida por la LOPD, resultando aplicable subsidiariamente la legislación reguladora de Contratación del Estado.

Por otra parte, en la cláusula 6 se establece que al objeto de garantizar la confidencialidad de los datos de carácter personal, con estricto cumplimiento de lo dispuesto en la LORTAD, la Organización Farmacéutica Colegial solamente podrá disponer y utilizar la información procedente de la mecanización de las recetas del Sistema Nacional de Salud para permitir la facturación de las recetas en términos del Anexo C que forma parte del Concierto. Cualquier otro uso deberá ser autorizado por el INSALUD.

DERECHOS DE ACCESO, RECTIFICACION, CANCELACION Y OPOSICION.

Este tipo de consultas siguen siendo las que con mayor frecuencia se plantean a la Agencia dado que son los derechos básicos que la LOPD reconoce al Ciudadano.

En este sentido y en computo global se indica que durante el año 2000 se han presentado 441 consultas sobre derecho de acceso, 588 sobre derecho de cancelación, 489 sobre derecho de rectificación y 27 sobre derecho de oposición.

La información que con carácter general se facilita es la ya recogida en Memorias anteriores sobre la forma del ejercicio de dichos derechos y que se tiene incluida dentro del apartado consultas más frecuentes, por lo que se da aquí por reproducida.

Sobre el ejercicio de estos derechos únicamente se van a reflejar aquí tres consultas que, al igual que en los apartados anteriores, se ha considerado que por su especialidad puede ser de interés el resaltarlas sobre el resto. Así, en primer término, se refleja una consulta en la que se quiere conocer el porqué del carácter personalísimo de estos derechos. La siguiente hace referencia a cómo se puede ejercitar dichos derechos en nombre de personas fallecidas. Finalmente la tercera se refiere al ejercicio del derecho de oposición.

- *Ejercicio personalísimo de los derechos de acceso, rectificación, cancelación y oposición* .

Se puso de relieve que de conformidad con lo que dispone el artículo 11 del Real Decreto 1392/1999 que desarrollaba la hoy derogada Ley Orgánica 5/1992, pero que es una norma que continua vigente de conformidad con la disposición transitoria tercera de la LOPD, se dispone que los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, pudiendo no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

A la vista de esta disposición se señala que el criterio de la Agencia en cuanto a la interpretación que debe darse a este precepto y que se ha contenido en otras Memorias (véase la correspondiente al año 1999, pag. 427 a 430), es que deben quedar perfectamente conciliados los derechos de los afectados a que su ejercicio se produzca de la forma que les resulte menos gravosa (lo que resulta conforme con las garantías atribuidas por nuestro texto constitucional) con la seguridad de que sólo el interesado podrá ostentar la voluntad adecuada para decidir dicho ejercicio, dado el carácter personalísimo del derecho.

Tomando en cuenta lo establecido en este precepto, resulta evidente que sólo el interesado podrá efectuar la manifestación de su voluntad consistente en la emisión de una declaración por la que pretenda el ejercicio de los derechos de acceso, rectificación o cancelación, a menos que se trate de una persona que carezca de la suficiente capacidad de obrar, en cuyo supuesto su voluntad podrá resultar suplida por la de su representante legítimo (tal y como prevé el párrafo segundo). Ahora bien, lo establecido en el citado artículo 11 no obsta a que la declaración de voluntad que inequívoca y específicamente haya de efectuar el interesado pueda ponerse en conocimiento de su último destinatario (el responsable del fichero) a través de la persona a la que aquél haya legítimamente otorgado su representación.

En consecuencia, el artículo 11 del Real Decreto 1332/1994 pretende que nadie, salvo el propio interesado, pueda decidir si quiere ejercitar los derechos que la ley le atribuye, ante quién desea ejercitar esos derechos, a qué ficheros se refiere tal ejercicio y en qué condiciones habrá de producirse el mismo pero, una vez efectuada por el interesado una declaración clara, inequívoca y suficientemente explícita en ese sentido, la transmisión al responsable del fichero de esa declaración de voluntad, en los estrictos términos en que aquélla se haya manifestado, podrá encomendarse a un representante voluntario o mandatario, que actuará (dentro de esos límites) ante el responsable del fichero.

Por tanto, se le informa que del artículo 11 del Real Decreto 1332/1994 no se desprende una prohibición del ejercicio de los derechos de acceso, rectificación y cancelación por un representante voluntario o mandatario del propio afectado, por cuanto ese ejercicio se producirá siempre en nombre y por cuenta del propio afectado, considerándose el ejercicio del derecho por el mandatario como efectuado por el propio interesado que le confiere la representación (tal y como se desprende *a sensu contrario* de lo dispuesto en el artículo 1717 del Código Civil). Por ello, el apoderamiento deberá ser expreso y referido al concreto derecho que se pretende ejercitar, con expresa mención del fichero ante el que tal derecho pretende ejercitarse, así como del objeto de cada actuación concreta. Sólo un apoderamiento otorgado en esos términos podrá haber sido precedido de una concreta declaración de voluntad del afectado, que permita concebir que el ejercicio del derecho se efectúa por él.

En consecuencia, no serán admisibles apoderamiento genéricos, sino aquéllos que se refieran concretamente al ejercicio de alguno de los derechos consagrados por la ley indicando los términos en que el apoderamiento se realiza, sin que el mandatario pueda, en modo alguno, exceder de lo dispuesto en esos términos y sin que quepa atribuir al mismo una potestad genérica de actuación. Esta atribución genérica desvirtuaría la exigencia contenida en el artículo 11 del Real Decreto 1332/1994, por cuanto no supondría una concreta manifestación de la voluntad del interesado de ejercitar los derechos, toda vez que éstos serían ejercidos únicamente si el apoderado lo considerase oportuno y en los términos en que el mismo estimase adecuados. Resta, por último, hacer referencia, una vez precisado el contenido que habrá de tener el apoderamiento que se efectúe, a los requisitos formales que deberá ostentar el mismo.

Partiendo de lo anteriormente expuesto, resulta evidente que no será posible un mandato verbal, puesto que sólo mediante un apoderamiento escrito podrá conocer el responsable del fichero la concreta voluntad de ejercicio del derecho por el afectado.

Por otra parte, si el apoderamiento fuera efectuado mediante documento privado sería preciso, a fin de que el mismo pudiera dar fe ante el responsable del fichero, que dicho apoderamiento derive directa e inequívocamente del interesado, titular del derecho protegido, que la firma de éste último apareciera autenticada mediante medio que permitiese a aquél tener perfecto conocimiento de que la declaración de voluntad procede inequívocamente del propio afectado, aportándose por el representante el original de dicho apoderamiento.

Del mismo modo, será posible el ejercicio del derecho por apoderado cuyo poder aparezca otorgado en escritura pública, siempre y cuando dicho apoderamiento cumpla los requisitos de contenido a los que nos hemos referido con anterioridad.

Se indicó, por último, que la información facilitada lo es con carácter general, por lo que en ningún caso puede entenderse como una valoración jurídica, quedando supeditada a las circunstancias que se puedan presentar en cada caso concreto.

- *Ejercicio de los derechos en nombre de una persona fallecida*

Han sido varias las consultas que se han planteado en términos similares referidos a como se puede ejercitar los derechos de acceso, rectificación o cancelación en nombre de un familiar (padre, madre etc.) fallecido .

En la contestación a estas consultas se ha expuesto el criterio que de forma muy detallada ha sido objeto de análisis por el Gabinete Jurídico de la Agencia.

Se comenzó poniendo de manifiesto que, de conformidad con lo establecido en la normativa de aplicación sobre protección de datos, básicamente contenida en la LOPD y en el Real Decreto 1332/1994 que sigue en vigor, los derechos de acceso rectificación y cancelación a los datos personales son derechos personalísimos que únicamente pueden ser ejercitados directamente por el propio afectado.

Según su artículo primero, la LOPD tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Sentados así los términos, se informó que en principio, la solución deberá estar en función de la naturaleza misma del derecho protegido por la norma, lo que conlleva a la necesidad de determinar si la muerte de las personas da lugar a la

extinción del derecho a la protección de la "privacidad", ya que el artículo 32 del Código Civil dispone que " la personalidad civil se extingue por la muerte de las personas", lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

Sin perjuicio de lo anteriormente expuesto, debe indicarse que la protección otorgada por la Ley frente a las intromisiones que supongan una vulneración de los derechos al honor y a la intimidad subsiste con posterioridad a la muerte de las personas. En ese sentido, cabe destacar que la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pone de manifiesto en sus artículos 4 a 6 que el fallecimiento no impide que por las personas que enumera el primero de los preceptos citados puedan ejercitarse las acciones correspondientes, siendo éstas la persona que el difunto haya designado a tal efecto en testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de las personas anteriormente citadas, el Ministerio Fiscal.

Como anteriormente se expuso, la LOPD tiene como objeto especial (por imperativo del artículo 18.4 de la Constitución) la protección del honor y la intimidad, estableciendo a lo largo de su articulado las medidas precisas para asegurar que dicha protección se lleva plenamente a efecto.

Del análisis conjunto de las disposiciones contenidas en ambas Leyes se desprende que la legitimación conferida para el ejercicio de las acciones reconocidas en la Ley Orgánica 1/1982 existirá, en el ámbito de la LOPD, cuando la actuación de las personas legitimadas tenga por directo y exclusivo objeto el ejercicio de las acciones tendentes a la protección del honor, la intimidad personal y familiar y la propia imagen de las personas fallecidas, no siendo posible la actuación de éstas en cualquier otro supuesto en que la finalidad de su actividad difiera de la antedicha protección.

Ello supone que, en principio las personas legitimadas por la Ley Orgánica 1/1982 carecerán de legitimación para el ejercicio de los derechos reconocidos por la LOPD, salvo en los supuestos en que esos derechos se ejerciten como instrumento para la realización de alguna de las finalidades protectoras indicadas que la Ley Orgánica 1/1982 les atribuye. Fuera de estos supuestos no será posible entender que la actividad de los herederos o personas referidas en el artículo 4 de la Ley Orgánica 1/1982 se encuentra amparada por la LOPD.

- *Ejercicio del derecho de oposición y diferencias con el derecho de cancelación*

En esta consulta se solicitaba información sobre el ejercicio del derecho de oposición que figura en el artículo 30.4 de la LOPD y se indico a este respecto lo siguiente:

El derecho de oposición no estaba regulado en la Ley Orgánica 5/1992 Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, siendo una de las modificaciones incluidas en la nueva Ley Orgánica 15/1999 por venir obligados a ello al figurar dicho derecho en la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

El derecho de oposición está previsto con carácter general en el artículo 6. 4 de la LOPD, y con carácter especial para ficheros de publicidad y prospección comercial en el artículo 30. 4 de la Ley.

Dicho derecho consiste básicamente en que, en aquellos supuestos en los que para el tratamiento de datos personales no sea necesario el consentimiento de las personas afectadas por los mismos y siempre que una ley no disponga lo contrario, estas podrán oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal, motivos estos que en el caso de tratarse de ficheros de publicidad y prospección comercial no serán necesarios y los afectados se podrán oponerse previa petición y sin gastos al tratamiento de sus datos dándoseles de baja del tratamiento a su simple solicitud.

INTERNET. PÁGINAS WEB

Bajo este epígrafe se van a incluir cuatro consultas que son significativas respecto a cómo está evolucionando o pretende evolucionar el tratamiento y uso de los datos a través de Internet. Se incluye una primera consulta que responde a una de las preguntas que van siendo cada vez más habituales por aquellas personas que pretenden crear una página Web y obtener datos de carácter personal a través de ella. La segunda, va referida a otro tipo de consultas que los ciudadanos demandan con mucha frecuencia y se refiere, a los envíos de publicidad a través de Internet. La tercera se ha considerado interesante incluirla pues en ella se pregunta si por parte de una Administración Local se puede dar la posibilidad de acceder a la información del padrón a través de una Web. Finalmente, se ha incluido una consulta en la que se preguntaba sobre si la dirección de correo electrónico se puede considerar como dato de carácter personal.

- *Recogida y tratamiento de datos personales a través de una página Web*

Como se ha indicado anteriormente, ha sido frecuente este tipo de consultas a lo largo del año 2000. En líneas generales se pregunta sobre la posibilidad de crear páginas Web, para, a través de ellas, poder realizar encuestas, suscripciones a revistas, etc., en definitiva proceder a recabar y tratar datos de personas físicas con una determinada finalidad.

Se ha puesto de relieve que el hecho de utilizar Internet para recabar datos personales, en nada difiere de cualquier otra forma más común o tradicional de obtener los mismos. Es por ello que, le será de aplicación igualmente lo previsto en la LOPD dado que los datos de carácter personal recogidos, se van a incorporar a un soporte físico y van a ser susceptibles de tratamiento.

Por otra parte, teniendo en cuenta que, de conformidad con lo previsto en el artículo 25 de la referida Ley Orgánica, se podrán crear ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y, se respeten las garantías que esta Ley establece para la protección de las personas, dichos datos se podrán recoger a través de una página Web y en la medida en que esos datos pertenezcan a personas físicas identificadas o se puedan identificar a través de dichos datos, el fichero que se cree quedará sometido a los principios y garantías que dicha Ley establece, tales como :

- El responsable de la página Web deberá proceder a notificar al Registro General de Protección de Datos la creación del fichero de datos que se cree a través de la página Web y el tratamiento informático posterior que va a realizar con los datos personales que recoja.

* Deberá informar a través de la página Web y previo a la recogida de los datos, del contenido básico del artículo 5.1 de la LOPD que señala que, los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

- Para el tratamiento posterior de los datos personales necesitara el consentimiento de las personas afectadas y no podrá comunicar estos datos a terceros sin su consentimiento.

- Por último, se le informa que de conformidad con el Reglamento aprobado por Real Decreto 994/1999, de 11 de junio (BOE 25-6-1999) deberá de adoptar en sus ficheros el nivel de seguridad básico, medio o alto, en función del tipo de datos que manejen (art. 4) y redactar el documento de seguridad regulado en el artículo 8 del referido Reglamento.

- *Envíos publicitarios a través de Internet*

En la contestación a estas consultas, y siguiendo la línea de las recomendaciones de Internet que tiene editadas esta Agencia desde el año 1997, se informa, sin pretender proporcionar una visión alarmista, sobre la necesidad de que todos los usuarios de Internet deben de concienciarse de que sus datos personales pueden ser utilizados de forma irregular y, de que está en su mano, el procurar que los mismos sean recogidos y tratados de manera leal y transparente.

Se informa que si están enviando publicidad a través de Internet, evidentemente es necesario para poder realizar dicho envío, el tener conocimiento de la dirección de correo electrónico del receptor del mensaje. Adicionalmente, una dirección de correo electrónico puede tener asociada información de carácter personal, tal como la organización donde trabaja o a la que pertenece una persona, lo que puede ser de gran interés para una empresa que se dedique a la publicidad directa. Las formas más habituales de obtener direcciones de correo sin el conocimiento del usuario son:

** Listas de distribución y grupos de news*

** Captura de direcciones en directorios de correo electrónico.*

** Venta, alquiler o intercambio de direcciones de correo por parte de los proveedores de acceso.*

** Entrega de la dirección de correo, por parte de los programas navegadores, al conectar a los servidores Web.*

En este sentido y desde la Agencia de Protección de Datos se hacen las siguientes recomendaciones:

**Cuando incluya su dirección de correo electrónico en un directorio o lista de distribución, considere la posibilidad de que la misma pueda ser recogida por terceros para enviarle mensajes no deseados.*

**Averigüe la política de alquiler, venta o intercambio de datos que han adoptado tanto su proveedor de acceso a Internet como los administradores de los directorios y listas de distribución donde esté incluido.*

**Si no quiere publicar su dirección de correo electrónico, configure su navegador para que no deje su dirección de correo en los servidores Web a los que accede.*

No obstante lo anterior, igualmente se le informa que se podrá dirigir al responsable del tratamiento, ejercitando el derecho de cancelación de sus datos personales, para lo que se le recomienda que se dirija directamente a dicho responsable, utilizando cualquier medio que permita acreditar el envío y la recogida de su solicitud, para el ejercicio de sus derechos, acompañando copia de su D.N.I.

Si en el plazo de los 10 días siguientes a la recepción de la solicitud en la oficina referida, ésta no ha sido atendida adecuadamente, podrá dirigirse a la Agencia de Protección de Datos con copia de la solicitud cursada, para que ésta a su vez se dirija a la oficina designada con el objeto de hacer efectivo el ejercicio de sus derechos.

También se le recomienda, que ponga en conocimiento del proveedor de servicios en Internet esta situación a los efectos de que se adopten las medidas necesarias de autorregulación.

- Publicación en Internet de datos del Padrón Municipal

La consulta se planteó por una persona que tenía interés en conocer si una Administración Local puede establecer un sistema de consulta de datos padronales a través de Internet.

En primer lugar se le indicó que la regulación del padrón municipal está contenida en la Ley 4/1996, que modifica la Ley 7/1985, de Bases de Régimen Local en relación con el Padrón Municipal, y en concreto el artículo 16 prevé lo siguiente:

"1. El Padrón municipal es el registro administrativo donde constan los vecinos de un municipio. Sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo. Las certificaciones que de dichos datos se expidan tendrán carácter de documento público y fehaciente para todos los efectos administrativos.

2. La inscripción en el Padrón municipal contendrá como obligatorios sólo los siguientes datos:

a) Nombre y apellidos.

b) Sexo.

c) Domicilio habitual.

d) Nacionalidad.

e) Lugar y fecha de nacimiento.

f) Número de documento nacional de identidad o, tratándose de extranjeros, del documento que lo sustituya.

g) Certificado o título escolar o académico que se posea.

h) Cuantos otros datos puedan ser necesarios para la elaboración del Censo Electoral, siempre que se garantice el respeto a los derechos fundamentales reconocidos en la Constitución.

3. Los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

Fuera de estos supuestos, los datos del Padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común."

En consecuencia y atendiendo a que los datos del Padrón Municipal son de carácter confidencial y que únicamente puede tener acceso a ellos cada uno de los vecinos empadronados en el municipio, y atendiendo a que su regulación está sometida a la LOPD, que ha venido a sustituir y derogar a la Ley Orgánica 5/1992 Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, en principio, está previsto que el derecho de acceso se ejercerá mediante petición o solicitud dirigida al responsable del fichero, por lo que la posibilidad planteada referida a acceder a sus datos de empadronamiento a través de Internet, parece que no se ajusta a las previsiones legales, salvo que se adopten medidas que eviten accesos no autorizados.

¿¡La Dirección de correo electrónico es dato de carácter personal?

La información que se facilitó a esta consulta partió básicamente de los criterios contenidos en una resolución de la Agencia, y en ese sentido se puso de relieve lo siguiente:

La dirección electrónica se forma por un conjunto de signos o palabras que la diferencian de las demás, siendo el titular de la misma quien generalmente decide y elige la dirección correspondiente, con el único límite de que no exista otra dirección idéntica correspondiente a otro titular.

En la selección de la dirección electrónica se pueden elegir combinaciones que no contengan significado alguno o, incluso, utilizar como combinación el nombre de la persona o algún otro dato identificativo.

El concepto de dato personal, según la definición de la LOPD comprende cualquier información concerniente a persona

física identificada o identificable, de donde se requiere la concurrencia de un doble elemento: por una parte la existencia de una información o dato y de otra, que dicho dato pueda vincularse a una persona física identificada o identificable. En el supuesto de direcciones electrónicas la información está constituida por un conjunto de signos que cuando permiten la vinculación directa o indirecta con una persona física la convierte en un dato de carácter personal.

El hecho de que una dirección electrónica se exteriorice de forma voluntaria por el afectado, no quiere decir que ese dato esté disponible para cualquiera, sino que únicamente, y por regla general, estará disponible y será conocido por aquellos a quienes voluntariamente se lo indique el titular de dicha dirección.

En consecuencia, las empresas o entidades públicas o privadas que obtienen direcciones electrónicas para enviar publicidad, o cualquier otro tipo de información, deben cerciorarse de que el afectado ha manifestado su consentimiento para que traten sus datos referidos a esa dirección.

Este es también el criterio general que sobre protección de datos mantiene la Directiva 95/46/CE, que hace referencia a cualquier tipo de tratamiento de datos personales con independencia de los medios técnicos utilizados. En este sentido, el tratamiento de los datos personales en Internet debe respetar los principios de protección de datos al igual que en el mundo habitual (off-line). Esto no constituye una limitación de la utilización de Internet, sino que, por el contrario, forma parte de los requisitos fundamentales destinados a garantizar la confianza de los usuarios en el funcionamiento de Internet y los servicios que se facilitan mediante esa red. Por consiguiente, el tratamiento de datos personales en Internet debe considerarse a la luz de la directiva.

- REGLAMENTO DE SEGURIDAD

Las preguntas relativas a la aplicación del Reglamento de Seguridad que en conjunto se han planteado durante el año 2000 han ascendido a 251. Sin embargo, se puede poner de relieve, que en la mayoría de ellas la información que se ha facilitado ha sido con carácter muy general y siempre como consecuencia de la solicitud de información sobre la inscripción de ficheros, en las que aprovechando la información sobre la forma en que se deben de declarar los ficheros, se facilitaba también información sobre la necesidad de adoptar en los mismos las medidas reguladas en el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal aprobado por Real Decreto 994/1999, de 11 de junio.

No obstante, y por su especialidad, se destacan dos consultas planteadas sobre este tema. Se ha preguntado en varias ocasiones sobre la aplicación del artículo 26 del Reglamento en cuanto al cifrado de los datos cuando se utilicen redes de telecomunicación para el envío de los mismos. De otro lado, respecto de la posibilidad de tratar los datos de salud fuera de los locales de un Hospital.

- *Aplicación del artículo 26 del Reglamento de Medidas de Seguridad*

Se ha vuelto a plantear el tema tratado en 1999 y, tal y como se expresó en la Memoria correspondiente a este año (página 421) se ha informado que:

En cuanto al ámbito de aplicación del artículo 26, aplicable únicamente a los ficheros que requieran medidas de seguridad de nivel alto, debe estarse al hecho de que en la transmisión de los datos se empleen redes de telecomunicaciones, definidas por el artículo 2. c) de la Directiva 97/66/CE, de 15 de diciembre, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, como "los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales entre puntos de terminación definidos por cable, por medios radioeléctricos, por medios ópticos o por otros medios electromagnéticos que se utilizan, total o parcialmente, para la prestación de servicios públicos de telecomunicaciones."

En consecuencia, las medidas a las que se refiere el artículo 26 del Reglamento serán de aplicación a la transmisión de datos entre distintas dependencias de la entidad cuando sea necesaria para dicha transmisión la utilización de redes de telecomunicaciones cuya titularidad sea ajena a la propia empresa, no siendo preciso el cifrado de los datos en caso de que las comunicaciones en ningún momento accedan a dicha red.

- *Utilización de datos de salud fuera de las dependencias hospitalarias*

Se plantearon en esta consulta una serie de cuestiones relacionadas con el acceso a datos de salud por parte de un directivo de un hospital que tiene autorización según el documento de seguridad y que procede a llevarse copia de algunos de los datos a su domicilio para poder terminar una serie de tareas.

La contestación que se dió a esta consulta fue una información de carácter muy general, y así se le indicó que las cuestiones planteadas deben ser resueltas directamente por el responsable del fichero, es decir por el Hospital en cuestión, dejándolas reflejadas en el documento de seguridad, debiendo ajustarse a lo dispuesto en el reglamento de Seguridad y en concreto a lo dispuesto en el artículo 9 *Funciones y obligaciones del personal;* artículo 11 *identificación y autenticación;* artículo 12 *control de acceso;* artículo 19 *control de acceso físico;* artículo 20 *gestión de soportes*; artículo 23 *distribución de soportes* y artículo 24 *Registro de accesos.*

Respecto de las responsabilidades que se pudieran derivar en el supuesto de un extravío, se le indica que el propio Reglamento en su artículo 28 y la LOPD en su artículo 44 establecen que el responsable será siempre la empresa o entidad que figura como responsable del fichero, independientemente de la responsabilidad disciplinaria de carácter interno que posteriormente se pueda adoptar contra el empleado o directivo de dicha empresa.

SECTOR DE TELECOMUNICACIONES

Dentro de este sector ha tenido durante el año 2000 una especial trascendencia el encarte que envió una empresa operadora de telecomunicaciones a todos sus abonados en el que se informaba del cambio de finalidad que se iba a dar a los datos de facturación telefónica, habiéndose recibido en la Agencia bastantes quejas sobre todo con la forma de solicitar el consentimiento para este nuevo uso. Igualmente ha habido también un número elevado de consultas al igual que en años anteriores sobre la utilización de los datos de los repertorios telefónicos. Finalmente se añade una consulta que fue planteada únicamente en dos ocasiones pero que se considera importante reflejarla en la memoria dado que se preguntó por la posibilidad de la realización de consultas inversas en los listines telefónicos.

- *Datos de facturación telefónica*

En esta consulta se solicitaba información acerca de si la petición del consentimiento por parte de un operador de telecomunicaciones a cada uno de sus abonados, con el objeto de utilizar sus datos de facturación telefónica era correcta o no, dado que en la carta se hacía la indicación de que si en el plazo de un mes no se oponían a dicho tratamiento se entendería concedido el consentimiento.

La LOPD regula dentro de su artículo 4, apartados 1 y 2, que:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos....."

Asimismo, en el artículo 6.1 se establece que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa."

La LOPD se complementa, en el sector de las telecomunicaciones, por lo dispuesto en la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que ha sido incorporada al ordenamiento jurídico español por la Ley 11/1998, de 24 de abril, General de Telecomunicaciones -LGT- (arts. 49 a 54) y el Título V del R.D. 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de la LGT en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones.

Las previsiones de la Directiva en lo relativo al tratamiento automatizado de datos de tráfico y facturación para fines comerciales, se incorporan al Derecho español a través del art. 65.3 del Reglamento, que además hace referencia a la definición de tratamiento de datos, en coincidencia con la contenida en el art. 3 de la LOPD.

Sin embargo, mientras la Directiva no distingue en su artículo 6 sobre la forma de prestar el consentimiento para tratar los datos de facturación del abonado, el legislador español ha admitido expresamente en el citado art. 65 del Reglamento, el consentimiento tácito del afectado para que los operadores puedan tratar sus datos de tráfico y facturación para la promoción comercial de sus propios servicios de telecomunicaciones.

El precepto mencionado establece, literalmente, en su apartado 3:

"*Asimismo, los operadores podrán tratar los datos a los que se refiere el apartado anterior para la promoción comercial de sus propios servicios de telecomunicaciones, siempre y cuando el abonado haya dado su consentimiento previo. A estos efectos, los operadores deberán dirigirse a los abonados, al menos con un mes de antelación al inicio de la promoción, requiriendo su consentimiento que, de producirse, será válido hasta que los abonados lo dejen sin efecto de modo expreso. Si en el plazo de un mes desde que el abonado reciba la solicitud, éste no se hubiese pronunciado al respecto, se entenderá que consiente, sin perjuicio de lo dispuesto en la disposición transitoria séptima* ".

A la vista de las disposiciones anteriores se desprende que la actuación del operador, es conforme a derecho, dado que al variar la finalidad del tratamiento de los datos de facturación para la promoción comercial de sus propios servicios de conformidad con el referido artículo 65.3, le está pidiendo a cada uno de sus abonados el consentimiento para poder realizar dicho tratamiento, situación acorde con lo que establecen dichos preceptos.

En efecto, en la carta recibida por cada uno de los abonados, se requiere el consentimiento para tratar automatizadamente los datos personales, se informa de que el consentimiento solicitado -facultativo y no obligatorio- es para ofrecer servicios de telecomunicaciones de la propia empresa, no de terceras compañías, así como de la norma que habilita para obtener el consentimiento tácito y, se incluye la referencia expresa a la posibilidad de ejercer los derechos de acceso, rectificación y cancelación y del lugar y responsable del fichero ante el que ejercitarlos.

Por ello, se indicó que, en tanto no se produzca una modificación normativa que cambie el art. 65.3 del Real Decreto 1736/1998, debe considerarse que la carta remitida se ajusta a sus exigencias, disponiendo el abonado de la opción de manifestar su consentimiento contrario al tratamiento de los datos, así como de la de revocarlo posteriormente.

Utilización de los datos de los repertorios telefónicos

Con carácter general, a estas consultas, se les ha informado en primer término que, de conformidad con el artículo 3.j) de la LOPD los datos telefónicos básicos que figuran en los repertorios telefónicos (tanto en papel como en soporte electrónico), constituyen una fuente que se considera como accesible al público, pudiéndose recabar tales datos sin el consentimiento expreso del interesado, regulándose por su normativa específica.

En consecuencia, en los repertorios de abonados de servicios telefónicos, ya sean impresos en papel o disponibles por otros medios (Infovía, Páginas blancas, CD-ROM, etc.) aparecen el nombre y apellidos así como la dirección, y, salvo que se manifieste en sentido contrario exigiendo su exclusión, sus datos pueden ser consultados y utilizados por el público en general.

Frente a esta situación, y para que estos datos no sean fuentes de acceso público, se debe proceder, a solicitar al operador de telecomunicaciones con carácter preventivo, que se proceda gratuitamente a la exclusión total o parcial de los datos relativos a su persona que se encuentren en los repertorios telefónicos de abonados de conformidad con lo establecido en su normativa especifica, contenida en el artículo 67 del Reglamento por el que se desarrolla el Titulo III de la Ley General de Telecomunicaciones (Real Decreto 1736/1998).

"Artículo 67. Guías de servicios de telecomunicaciones disponibles al público.

1. Los datos personales que figuren en las guías de abonados de los servicios a los que se refiere el artículo 62 que sean accesibles al público o que puedan obtenerse a través de servicios de información, ya sean impresas o electrónicas, deberán limitarse a los que sean estrictamente necesarios para identificar a un abonado concreto. Por Orden del Ministro de Fomento, se determinarán las condiciones para hacer constar dichos datos.

No obstante lo dispuesto en el párrafo anterior, los operadores encargados de la elaboración de las guías podrán publicar otros datos personales de los abonados siempre que éstos hayan dado su consentimiento inequívoco.

A estos efectos, se entenderá que existe consentimiento inequívoco de un abonado, cuando éste se dirija al operador por escrito solicitándole que amplíe sus datos personales que figuran en la guía. También se producirá cuando el operador solicite al abonado su consentimiento y éste le responda en el plazo de un mes dando su aceptación. Si en dicho plazo el abonado no hubiese dado su consentimiento expreso, se entenderá que no acepta que se publiquen en la guía correspondiente otros datos que no sean los que se establecen en el párrafo primero de este apartado.

2. Los abonados podrán exigir a los operadores que se les excluya de las guías, que se indique que sus datos personales no puedan utilizarse para fines de venta directa o que se omita parcialmente su dirección. Los operadores requeridos deberán cumplir lo dispuesto en este apartado, sin coste alguno para los abonados.

Los abonados que soliciten su exclusión de las guías, tendrán derecho a recibir la información adicional a la que se refiere el párrafo segundo del apartado 3 del artículo 69."

En el referido artículo 67 no está prevista la obligación de contestar por parte del operador, por lo que el hecho de que no le den respuesta a su solicitud no supone en principio ninguna infracción, no pudiendo iniciar por la Agencia de Protección de Datos ninguna actuación al respecto, sin perjuicio de la obligación del operador de excluirle de los referidos repertorios.

* *Posibilidad de realizar consultas inversas a las guías telefónicas*

Se informa que la finalidad de un repertorio con búsqueda inversa es diferente a la de un repertorio tradicional de abonados. Un directorio telefónico tal y como está concebido en nuestra legislación específica de telecomunicaciones permite obtener el número de teléfono de una persona conocida, a partir de su nombre y un criterio geográfico, mientras que la finalidad de una búsqueda inversa es la obtención de la identidad y la dirección de un abonado del que únicamente es necesario conocer su número de teléfono y aunque este recurso de los directorios inversos puede servir a los intereses legítimos en algunos casos especiales de emergencia y seguridad pública, el proporcionar los datos de un usuario a partir de su número de teléfono, sin disponer del consentimiento del afectado podría constituir un tratamiento desleal de la información que contravendría el principio de calidad de datos contemplado en el artículo 4 LOPD.

SECTOR SEGUROS

- **Corredurías de Seguros**

Se plantea una consulta sobre si lo dispuesto en la disposición adicional sexta de la LOPD es de aplicación a las corredurias de seguros.

Se informó que dicha disposición viene a modificar lo dispuesto en el artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados quedando redactado así:

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el

consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado".

A la vista de dicha disposición lo que se está regulando es la posibilidad legal de poder crear por las entidades aseguradoras ficheros comunes, en los que se van a poder introducir datos de los asegurados con las finalidades, o bien, de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora, o bien, de prevención del fraude en el seguro. La importancia de esta regulación es que para la introducción de los datos en el fichero común no va a ser necesario el consentimiento de los propios asegurados, aunque si deberán ser informados de ello en los términos previstos en dicha disposición.

De conformidad con la Ley de Ordenación y Supervisión de los Seguros Privados y atendiendo a lo dispuesto en su artículo 2, quedan sometidos a sus preceptos, entre otros, tanto las entidades que realicen las operaciones o actividades mencionadas en el artículo 3, como los profesionales y entidades que suscriban los documentos previstos en la presente Ley o en sus disposiciones complementarias de desarrollo.

De lo anteriormente señalado se desprende, por lo que se refiere a los términos de la consulta planteada, que aunque la Ley de Ordenación y Supervisión del Seguro incluye dentro de su ámbito de aplicación a las Corredurías de Seguro, sin embargo la posibilidad legal contemplada en la disposición adicional sexta de la LOPD, está fijando quienes son los que pueden crear los ficheros comunes previstos, y, en este sentido, señala única y exclusivamente a las entidades aseguradoras, por lo que las corredurías de seguro, en ningún caso, podrán crear este tipo de ficheros .

Fichero Histórico de Automóviles

Han sido varias las consultas, sobre todo a final de año, en que los ciudadanos han solicitado información o incluso han manifestado su queja, sobre la cesión de sus datos personales por parte de las compañías de seguros donde tienen el seguro de su automóvil, a un fichero común cuyo responsable es UNION ESPAÑOLA DE ENTIDADES ASEGURADORAS Y REASEGURADORAS (UNESPA).

Se ha informado en primer lugar que, en virtud de la disposición adicional sexta de la LOPD se ha modificado el articulo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados con la siguiente redacción:

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. **La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado,** pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado".

A la vista de lo previsto en esta disposición, la creación del fichero histórico de siniestros de UNESPA es acorde con la LOPD y, en principio, ningún tomador de la póliza de seguros mientras la mantenga en vigor, podría oponerse a la cesión de sus datos a este fichero por parte de su compañía de seguros, en el caso de que este adherida a UNESPA, siempre que de la información que se facilite se permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza por ley, o el tipo de actividad de aquél a quién se pretenden comunicar.

Se ha puesto de manifiesto que en el Registro General de Protección de Datos figura inscrito a nombre de UNESPA el Código Tipo "fichero histórico de seguros del automóvil" (véase el apartado Códigos Tipo de esta Memoria).

Como garantía de que los datos, una vez introducidos en el fichero histórico de UNESPA, no pueden ser consultados en cualquier momento, el propio Código Tipo prevé en su apartado 7.2 que las entidades adheridas podrán realizar consultas al fichero, según los modelos propuestos en la plataforma tecnológica, que no permite en ningún caso volcar el fichero en su base de datos. Para efectuar las consultas será necesario que se haya producido una solicitud de aseguramiento del interesado ante la entidad que consulta el fichero y, dicha entidad, deberá identificarle correctamente debiendo informar al Sistema mediante las claves necesarias.

Como respuesta a la consulta efectuada, el Sistema facilitará a la entidad la información que se encuentre en el fichero relativa a pólizas suscritas, sus correlativos períodos de cobertura, así como de los siniestros y de las garantías aceptadas. En la información que arroja el Sistema no aparecerán datos personales del tomador del seguro ni valoraciones personales de ningún tipo.

Por último se le indica que, el tomador del seguro tendrá la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en el apartado 8.2 del referido Código.

Dicho apartado establece lo siguiente:

"Si tras haber ejercitado el derecho de acceso, el afectado ejercita los derechos de rectificación, cancelación u oposición, deberá formular su solicitud con la indicación de los datos que, por considerar incorrectos o inexactos, quiere que sean modificados o cancelados y aportando cuantos documentos avalan su pretensión. Si lo que se ejercita es el derecho de oposición deberá fundamentar la causa por la cual considera que sus datos no deben ser objeto de tratamiento automatizado.

Si la rectificación o cancelación afecta a datos personales de identificación y con la documentación aportada por el afectado resultare suficientemente probado el error o la inexactitud, se procederá automáticamente a su modificación o cancelación, comunicándolo a la entidad aseguradora.

Cuando la solicitud verse sobre la existencia y/o cuantía de los siniestros, el responsable del fichero dará traslado de la solicitud a la entidad aseguradora que haya facilitado el dato, al objeto de que en el plazo de ocho días resuelva de forma motivada sobre su procedencia. La información que sobre el afectado contenga el fichero quedará bloqueada hasta que se resuelva la solicitud.

Si la entidad no se pronuncia, TIREA mantendrá el bloqueo cautelar del dato, y se comunicará tanto al afectado como a la entidad aseguradora que deberá proceder a su rectificación o cancelación, en los términos de la solicitud, en la primera actualización de información. Realizada la necesaria comprobación por TIREA, si la entidad no hubiera procedido a dicha rectificación o cancelación, el dato quedará definitivamente bloqueado.

Si la entidad aseguradora resuelve oponiéndose a la rectificación o cancelación solicitada, deberá motivar su posición ante UNESPA, como responsable del fichero. La respuesta de la entidad aseguradora será trasladada al afectado, indicándole que la misma puede ser recurrida ante la Comisión de Control en el plazo de quince días desde que recibió la comunicación, mediante presentación de escrito en que razone su petición y los documentos en que fundamenta la misma. Recibido el escrito de recurso, se resolverá por la Comisión de Control en el plazo de quince días".

Igualmente se ha indicado que también se podría utilizar la vía de plantear una tutela de derechos ante la Agencia de Protección de Datos ante la negativa de facilitarle el acceso, rectificación, cancelación u oposición al tratamiento de sus datos de conformidad con lo previsto en la LOPD.

MEMORIA DE 2000 - CÓDIGOS TIPO

En un "mundo sin fronteras" las políticas públicas encaminadas a proteger la privacidad personal se mueve entre dos amplias dinámicas. Unos países diseñan unas políticas basadas en los estándares mas restrictivos mientras que otros consideran que un clima menos normativo es mas atractivo para la creación de negocios globales por lo que eluden esas restricciones.

La Ley basada en un modelo de mandato y sanción, establece un marco de derechos y responsabilidades, intenta marcar una línea clara de "conducta aceptable". Las organizaciones cuyas prácticas caen por debajo de esas líneas están sujetas a unas sanciones, en función del contexto y la importancia de la infracción.

La autorregulación es inherentemente voluntaria, si una organización no se acoge no hay una penalización por ello. Este ambiente liberal forma parte de la naturaleza del sector privado.

Los instrumentos reguladores que se basan los códigos tipo que se utilizan en el marco de protección de la intimidad personal se categorizan en: acuerdos privados, códigos privados, estándares de privacidad y sellos de confidencialidad.

Estos instrumentos no son excluyentes pero mantienen claros rasgos que los diferencian.

Los acuerdos privados representan los primeros ejemplos de esta acción autorreguladora en el mundo de los negocios, consistiendo en pequeños acuerdos sobre algunos principios de confidencialidad. Surgieron en los Estados Unidos en los años 80 cuando empresas y asociaciones del sector privado fueron alentadas a adoptar las recomendaciones de la OCDE de 1981.

Estos acuerdos se desarrollaban de cara al exterior mas que para hacer efectivo un comportamiento interno correcto dentro de las organizaciones.

Los códigos tipo pueden representar funciones cruciales en el marco de regímenes de protección de datos como el de Holanda, Nueva Zelanda, Irlanda y el Reino Unido.

El artículo 27 de la Directiva del Parlamento europeo y del Consejo de 24 de octubre de 1995, requiere a la Comisión Europea y a los Estados Miembros a fomentar el desarrollo de códigos de conducta. Los códigos también pueden operar en ausencia de un entorno regulador, no únicamente para establecer acuerdos, sino para especificar más detalladamente como los empleados deberían o no tratar la información sobre datos personales. Dependiendo del ámbito de aplicación se incluyen los códigos organizacionales, sectoriales, funcionales, tecnológicos y profesionales.

Con los estándares de confidencialidad se amplían los códigos de autorregulación, ya que no solo suponen un estándar, sino que además implican un proceso a través del que se puede probar objetivamente la adherencia a un conjunto de normas. Una organización debe decir lo que hace, y también hacer lo que dice.

Los estándares técnicos han jugado un importante papel en la seguridad de los sistemas informatizados durante mucho tiempo. Sin embargo, es mas reciente la idea de que un estándar de privacidad pueda incorporar principios de protección de confidencialidad .

Este tipo de estándares ha sido utilizado en Canadá, publicando en 1996 un código para la protección de información personal, y recientemente en Australia y Japón.

Desde 1999 esta iniciativa se ha trasladado a Europa. El Centro Europeo de Normalización responsable de la negociación de estándares en Europa ha comenzado a estudiar la posibilidad de un estándar internacional de confidencialidad.

Los sellos de certificación surgen como la marca o símbolo otorgado a cualquier organización que satisface un certificado para su identificación en el uso común.

El sello de la Asociación Canadiense de Estándares está considerada como un símbolo de calidad en el mercado canadiense y su utilización está celosamente restringida a aquellas compañías que han realizado adecuadamente su proceso de registro o certificación.

El desarrollo de un sello o marca específica para la protección de la privacidad ha prosperado también en Internet, pueden mencionarse numerosos ejemplos. El mas destacado ha sido el desarrollado por la organización TRUSTe, por BBBOnline y por el Centro de Desarrollo de Procesamiento de Información Japonés. Esta propuesta permite a los editores de páginas Web desarrollar formas de confidencialidad sobre la información recogida y las prácticas de uso de sus páginas. Como resultado la marca TRUSTe rápidamente se ha convertido en la marca de protección de privacidad mas utilizada en la Red, aunque en la mayoría de los casos por parte de empresas americanas.

El programa se construyó bajo la premisa de que los consumidores deben conocer las prácticas y las medidas de privacidad llevadas a cabo por los "sitios" por los que navegan debiendo éstos revelar qué información personal se mantiene, cómo se utiliza y quién comparte la información.

En España la Ley establece la posibilidad de adoptar acuerdos sectoriales, mediante decisiones de empresa o conve-

nios administrativos, que pueden ser depositados en la Agencia para su inscripción en el RGPD. Dentro del marco expuesto anteriormente en el que se hace una revisión del estado del arte en esta materia, los códigos tipo españoles se corresponden a códigos privados en los que se incluyen algunos estándares de confidencialidad, y en el caso del Código Tipo sobre Marketing Directo y Comercio Electrónico, se adopta un sello de garantía que las empresas adheridas pueden mostrar en su página Web y que de cierta manera demuestra el compromiso de la entidad por el cumplimiento de la normativa legal y demás estándares de confidencialidad suscritos en el Código Tipo.

Durante el año 2000 se han depositado en el RGPD dos solicitudes de inscripción de Códigos Tipo, el denominado "Código Ético de Protección de Datos Personales de las Empresas del Sector de Gestión de Cobros" presentado por el Sector de Gestión de Cobros de la Asociación Multisectorial de la Información (ASEDIE), y el "Código Tipo del Fichero Histórico de Seguros del Automóvil" presentado por la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA).

El Código Ético de Protección de Datos Personales de las Empresas del Sector de Gestión de Cobros se presentó en el mes de marzo, teniendo por objeto establecer la política a seguir por las empresas del Sector de Gestión de Cobros en relación con el uso del tratamiento de datos de carácter personal en el desarrollo diario de sus actividades.

En el borrador presentado se observaron algunos aspectos que no eran suficientemente explícitos, y otros que no se ajustaban a las disposiciones legales sobre protección de datos, lo que se comunicó a ASEDIE para que procedieran a su subsanación. En el mes de junio se presentó por parte de esta Asociación un nuevo texto, que al no reunir las condiciones exigidas en el art. 32 de la Ley, por cuanto adolecía de aspectos fundamentales como: la descripción de los ficheros de datos personales tratados por las empresas del Sector de Gestión de Cobros de ASEDIE, la duración del tratamiento de los datos y las previsiones adoptadas para el mantenimiento de los ficheros o el nivel de medidas de seguridad que deben reunir los sistemas de información que dan soporte a estos ficheros, se procedió al archivo de dicha solicitud.

El Código Tipo del Fichero Histórico de Seguros del Automóvil fue presentado en el RGPD por UNESPA en el mes de mayo de 2000, siendo su objeto establecer la regulación del Fichero Histórico de Seguros del Automóvil.

La creación de este fichero estaba habilitada en el artículo 24.3 de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, párrafo segundo: *"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora"* , que se nutre de la información aportada por las entidades aseguradoras a partir de sus Registros de Pólizas y de Siniestros.

No obstante, UNESPA en vez de proceder a realizar una nueva declaración en los términos establecidos en el artículo 24.3 anteriormente mencionado, optó por realizar un Código Tipo, en el que se clarificasen las condiciones en las que se recogen datos relativos a los contratos y al historial de siniestros de cada tomador o contratante de seguros de automóviles durante los últimos 5 años de vigencia de su póliza, al objeto de facilitar al momento de la suscripción del contrato información rigurosa y contrastada de los datos de siniestralidad mediante la puesta en común de la información obtenida a través de pólizas y siniestros, completando la información facilitada por el propio tomador.

Las entidades adheridas al fichero únicamente lo pueden consultar en el momento de la solicitud de suscripción de una nueva póliza, realizando una valoración técnica y objetiva del riesgo, aplicando la tarifa de prima que tenga recogida en sus bases técnicas.

Una vez analizado el primer borrador, la Agencia observó que determinados aspectos del Código deben ser aclarados o modificados, poniéndolo en conocimiento de UNESPA para su subsanación.

En el mes de julio fue presentado por UNESPA un nuevo texto del Código así como los documentos solicitados, en el que se han tenido en cuenta las observaciones señaladas, y otras mejoras, que por su interés a continuación se detallan:

- Se define la finalidad del fichero, que tiene por objetivo, además de la tarificación, facilitar la selección de riesgos y la elaboración de estudios de técnica aseguradora, finalidades amparadas en el art. 24 de la Ley 30/95.

- Asimismo, se aclara que en ningún caso para la elaboración de estudios de técnica aseguradora se utilizan los datos personales. Los datos se extraen siempre del fichero de forma disociada.

- El fichero queda vinculado al tomador del seguro, por ser quien asume los derechos y obligaciones derivados del contrato.

- Se pone de manifiesto que en este fichero nunca se tratarán datos de salud, por ser un seguro de responsabilidad civil que cubre los daños que se acusan a terceros ajenos a la relación contractual. Si ha habido daños materiales y corporales el fichero sólo evidencia que hay un tercero perjudicado, que no está identificado en el contrato.

- El plazo de cinco años se fundamenta en este escrito en que es un plazo suficientemente amplio para conocer el historial de aseguramiento. Además, está aconsejado por los actuarios como resultado de estudios estadísico-actuariales basados en análisis multivariante de valoración del riesgo.

- Se especifica que únicamente podrá consultarse el fichero por las entidades a solicitud del tomador del seguro.

- Se recoge expresamente que el tomador del contrato pueda oponerse, por causa justificada, al tratamiento de los datos.

- Se aclara en el código Tipo cómo se realiza el acceso al fichero por parte de las aseguradoras y el procedimiento de funcionamiento.

- Se incorporan los modelos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

- Se establece un procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

- Se incorpora en el procedimiento la revisión, a instancia del afectado, por la Comisión de Control de las decisiones de las Aseguradoras respecto al ejercicio de estos derechos.

- Se incorpora también, a instancia de la Agencia de Protección de Datos, un régimen sancionador que tiene por objeto garantizar el debido respeto a la Legislación de Protección de Datos por las entidades adheridas al fichero.

Realizando el nuevo código, y comprobando sanado los extremos que se señalaban en el informe remitido a UNESPA respecto al primer borrador de Código presentado, se procede a su inscripción en el mes de julio, quedando por tanto inscrito en el RGPD.

Con la incorporación en el RGPD del código inscrito en el año 2000, se completa la siguiente relación de Códigos inscritos:

"APLICACIÓN EN TELEFÓNICA DE LA LEY ORGÁNICA REGULADORA DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL"

Solicitante:

TELEFÓNICA DE ESPAÑA, S.A.

Presentación e inscripción: 1994, código CT00011994

"CÓDIGO ÉTICO DE PROTECCIÓN DE DATOS PERSONALES DE LAS EMPRESAS DE SERVICIOS COMERCIALES"

Solicitante:

ASOCIACIÓN DE EMPRESAS DE SERVICIOS DE INFORMES COMERCIALES (ASEICO)

Presentación e inscripción: 1995, código CT00011995

Suprimido en 1999, sustituido por el código presentado por ASEDIE

"CÓDIGO ÉTICO DE PROTECCIÓN DE DATOS PERSONALES EN INTERNET"

Solicitante:

FEDERACIÓN ESPAÑOLA DE COMERCIO ELECTRÓNICO Y MARKETING DIRECTO (FECEMD)

Presentación e inscripción: 1998, código CT00021998

"CÓDIGO ÉTICO SOBRE PUBLICIDAD EN INTERNET"

Solicitante: ASOCIACIÓN DE AUTOCONTROL DE LA PUBLICIDAD (AAP)

Inscrito en 1999, con el código CT00011999

"CÓDIGO ÉTICO DE PROTECCIÓN DE DATOS PERSONALES DE LAS EMPRESAS DE INFORMACIÓN COMERCIAL"

Solicitante: ASOCIACIÓN MULTISECTORIAL DE LA INFORMACIÓN (ASEDIE)

Inscrito en 1999, con el código CT00021999. Sustituye al CT00011995

"CÓDIGO TIPO DEL FICHERO HISTÓRICO DE SEGUROS DEL AUTOMÓVIL"

Solicitante: UNIÓN ESPAÑOLA DE ENTIDADES ASEGURADORAS Y REASEGURADORAS (UNESPA)

Inscrito en 2000, con el código CT00012000.

MEMORIA DE 2000 - LA PROTECCION DE DATOS EN ESPAÑA. ANALISIS DE LOS PRINCIPALES DESARROLLOS

1. INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

De conformidad con lo establecido en el artículo 37h) de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de carácter personal (LOPD) corresponde a la Agencia de Protección de Datos informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley Orgánica. Por su parte, el artículo 5 del estatuto de la Agencia concreta, en sus apartados a) y b), este precepto estableciendo que la Agencia informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica así como cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica.

A lo largo de 2000 se han sometido al parecer de la Agencia de Protección de Datos, para su informe preceptivo, un total de 21 disposiciones, debiendo destacarse por su especial relevancia las siguientes:

* Proyecto de Real Decreto por el que se crea y regula la Comisión Interministerial para actuar contra las actividades vulneradoras del los derechos de propiedad intelectual e industrial.

* Segundo borrador de Orden Ministerial por la que se crea la Comisión del Ministerio de Sanidad y Consumo para la gestión de un censo de personas con hemofilia y otras coagulopatías congénitas que hayan desarrollado el virus de la hepatitis C como consecuencia de haber recibido tratamiento en el sistema sanitario público, así como la norma de creación de los ficheros relacionados con el mismo

* Proyecto de Real Decreto sobre Inscripción de los españoles en los Registros de Matrícula de las Oficinas Consulares en el extranjero.

* Proyecto de Real Decreto por el que se desarrolla el régimen de control interno ejercido por la Intervención General de la Seguridad Social.

* Propuesta de norma con rango de Ley para la actualización de la regulación de la Central de Información de Riesgos del Banco de España (CIRBE)

* Proyecto de Orden Ministerial por la que se regulan los ficheros automatizados de datos de carácter personal del Ministerio del Interior sobre ADN.

* Borrador de Anteproyecto de Ley de Protección de Datos de la Comunidad de Madrid.

* Proposición No de Ley del Grupo Socialista relativa a las actuaciones necesarias para impedir el tratamiento masivo de datos de carácter personal por parte de los Operadores de Telefonía.

* Proyecto de Real Decreto por el que se aprueba el Reglamento sobre Protección Sanitaria contra Radiaciones Ionizantes.

2. DESARROLLO NORMATIVO.

Durante el año 2000, deben tenerse en cuenta, dentro de este epígrafe, la aprobación en virtud de Resolución de 30 de mayo, de los modelos de notificación de ficheros públicos y privados al Registro General de Protección de Datos, adaptados a lo establecido en la LOPD, así como la aprobación de la Instrucción 1/2000, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos.

Habiendo sido analizada con detalle en el Capítulo referido al Registro General de Protección de Datos la primera de normas citadas, dedicaremos este lugar de la Memoria al estudio de la Instrucción 1/2000, de 1 de diciembre.

INSTRUCCIÓN NÚMERO 1/2000, DE 1 DE DICIEMBRE, DE LA AGENCIA DE PROTECCIÓN DE DATOS, RELATIVA A LAS NORMAS POR LAS QUE SE RIGEN LOS MOVIMIENTOS INTERNACIONALES DE DATOS.

El régimen del movimiento internacional de datos de carácter personal ha sido, desde la aprobación de la LOPD), una de las cuestiones que ha suscitado un mayor número de dudas por parte de los responsables de los ficheros y la sociedad en general. Ello es debido a la necesidad de conciliar las normas del derecho interno con las previsiones contenidas en la Directiva 95/46/CE. Además, es necesario que los Estados Miembros de la Unión Europea adapten su normativa a lo establecido en las Decisiones que se adopten por la Comisión de las Comunidades Europeas en esta materia.

En este sentido, deben tenerse en cuenta las recientes Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE y 2000/520/CE, de 26 de julio (publicadas en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000), que consideraron adecuado el nivel de protección de datos personales en Suiza, Hungría, así como "el conferido por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos".

Dado este panorama, la Agencia de Protección de Datos consideró sumamente útil la elaboración de un texto único que viniera a interpretar las distintas Disposiciones reguladoras de las transferencias internacionales de datos, teniendo en cuenta que la actuación de la misma a lo largo del tiempo ha generado una abundante casuística relacionada con las transferencias internacionales de datos de carácter personal que hasta la fecha no venía recogida sistemáticamente en ningún texto.

En cuanto a la competencia para dictar la Instrucción, debe recordarse que el artículo 37 c) de la LOPD consagra la competencia de la Agencia de Protección de Datos para "dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley".

Tal y como se indica en el preámbulo de la Instrucción "no es finalidad de esta Instrucción efectuar innovación alguna dentro de la normativa reguladora de la protección de datos de carácter personal sino, simplemente, aclarar y facilitar a todos los interesados en un único texto, el procedimiento seguido por la Agencia para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos".

La Instrucción se compone de 6 normas, divididas en dos secciones, referida la primera a los criterios aplicables a cualquier transferencia internacional de datos y la segunda a supuestos concretos de transferencia.

En cuanto a las Disposiciones generales, la Norma Primera delimita el concepto de transferencia, aclarando lo ya establecido en el Real Decreto 1332/1994, definiendo como "transferencia internacional de datos toda transmisión de los mismos fuera del territorio español", tanto si la misma supone una cesión como si implica la realización de un tratamiento amparado por el artículo 12 de la LOPD. Asimismo se unifican los conceptos de transmitente y destinatario de los datos.

Por su parte, la Norma Segunda no hace sino recordar lo ya establecido en el artículo 25.1 de la Directiva, estableciendo que "La transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento", con especial referencia al deber de información consagrado en el artículo 5 de la LOPD.

Por último, dentro de esta parte general, la Norma Tercera establece, de conformidad con lo previsto en la LOPD y en el Real Decreto 1332/1994 el procedimiento de notificación de la transferencia al Registro General de Protección de Datos, así como el posible requerimiento que pueda efectuarse al Responsable para que acredite el cumplimiento de lo establecido en la Ley. En particular deberá hacerse expresa mención del país al que se pretende efectuar la transferencia y de los motivos que, en su caso, la habilitan, conforme a lo dispuesto en el artículo 34 de la citada Ley Orgánica, para no recabar la autorización expresa del Director de la Agencia de Protección de Datos.

Como ya se dijo, la segunda sección de la Instrucción se refiere a tres supuestos específicos de transferencia, tomando en consideración las normas cuarta y quinta el estado de destino de los datos y la norma sexta el hecho de que la actividad desarrollada por el destinatario sea similar a las previstas en el artículo 12 de la Ley Orgánica.

La Norma Cuarta se refiere a las transferencias internacionales que tengan por destinatario una persona o entidad, pública o privada, situada en el territorio de un Estado no miembro de la Unión Europea, respecto del que se haya declarado la existencia de un nivel adecuado de protección o que sea miembro del Espacio Económico Europeo. En este caso, se podrá requerir al responsable del fichero la aportación de la documentación que acredite el cumplimiento de la LOPD, así como, en los supuestos amparados en la Decisión 2000/520/CE de la Comisión de las Comunidades Europeas, que el destinatario se encuentra adherido a los principios de Puerto Seguro, mediante la correspondiente certificación emitida por la entidad reguladora a cuya jurisdicción se someta.

La Norma Quinta, por su parte, se refiere a las transferencias efectuadas a terceros estados respecto de los cuales no se haya declarado la existencia de un nivel adecuado de protección, viniendo a plasmar los requisitos necesarios para la consideración como adecuado de un contrato en que se funde la transferencia internacional de datos. Dichos requisitos, ampliamente desarrollados en la citada norma, vienen a reproducir los criterios planteados en la documentación aportada por los servicios de la Comisión Europea en esta materia, a los que se hace referencia en otros lugares de esta memoria, y que son similares a los que se contienen en los contratos previamente autorizados por esta Agencia de Protección de Datos.

Ambas normas prevén, de conformidad con lo establecido en las decisiones de la Comisión Europea, la facultad del Director de la Agencia de Protección de Datos de suspender, y en el caso de la norma quinta, prohibir, las transferencias en determinados supuestos en que pueda derivarse un perjuicio para los afectados.

Por último, la Norma Sexta se refiere a las transferencias efectuadas para la realización de actividades de tratamiento por cuenta del responsable del fichero, indicando que dichas transferencias, sin perjuicio del cumplimiento de las restantes normas de la Instrucción, deberán cumplir asimismo lo establecido en el artículo 12 de la LOPD. Además, se recuerda que, de conformidad con el citado precepto, la subcontratación de este tipo de servicios sólo será admisible cuando la contratista actúe en nombre y por cuenta del responsable del fichero.

3. CONSULTAS DE RESPONSABLES DE FICHEROS.

Dentro de la actividad llevada a cabo por la Unidad de Apoyo del Director de la Agencia de Protección de Datos, el

Gabinete Jurídico ha venido desempeñando desde la creación de la Agencia, junto con la función de asesoramiento directo a los distintos órganos de la misma, una importante función de resolución de las cuestiones de mayor complejidad jurídica planteadas por las personas o entidades públicas o privadas que ostentan la condición de responsables de ficheros.

El desarrollo de esta actividad, en línea con lo que ya sucedió en 1999 ha sufrido un gran incremento a lo largo del año 2000, en que se ha pasado de la elaboración de 370 informes en 1999 a la cifra de 606 (un aumento del 63,78%, que sería del 174 % si se compara con la cifra de 1998).

Debe recordarse, como ya se dijo en la memoria correspondiente a 1999, que la función a la que estamos haciendo referencia se lleva a cabo con el ánimo de colaborar con las entidades antes mencionadas en el desarrollo de sus actividades, si bien esta tarea no se encuentra entre aquellas que la Ley y su Estatuto exigen de la Agencia. Precisamente por ello los informes, salvo cuando son preceptivos, carecen de cualquier carácter vinculante, no prejuzgando de modo alguno la actuación de esta Agencia, por cuanto, en la mayor parte de los supuestos, no se tiene conocimiento de la totalidad de las circunstancias que concurren realmente en los hechos que motivan la consulta.

A continuación nos referiremos a las principales cuestiones que han sido planteadas en este tipo de consultas, haciendo en primer lugar referencia a diversas cuestiones relacionadas con el reparto de dichas consultas en función de diversos criterios para, posteriormente, analizar las materias que o bien han sido objeto de un mayor número de consultas o bien revisten una mayor relevancia desde el punto de vista de la interpretación de la Ley.

3.1.- Datos estadísticos de interés relacionados con las consultas.

En el siguiente cuadro se hace constar el reparto de informes emitidos atendiendo a la naturaleza pública o privada del consultante:

Administraciones Públicas..... 235

Admón. General del Estado..... 80

Departamentos Ministeriales..... 58

Organismos Públicos..... 22

Comunidades Autónomas..... 38

Entidades Locales..... 62

- Ayuntamientos..... 57
- Diputaciones Provinciales..... 3
- Otros..... 2

Admón. Corporativa..... 30

- Cámaras de Comercio..... 1
- Colegios profesionales..... 29

Consultas privadas..... 371

Empresas..... 303

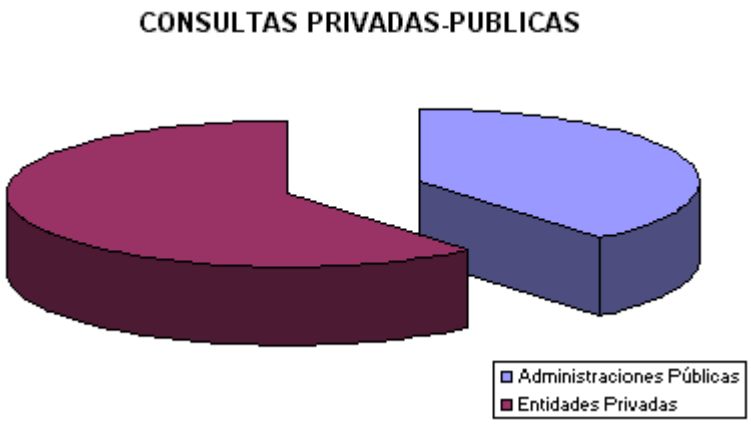
Particulares..... 29

Asociaciones/Fundaciones..... 30

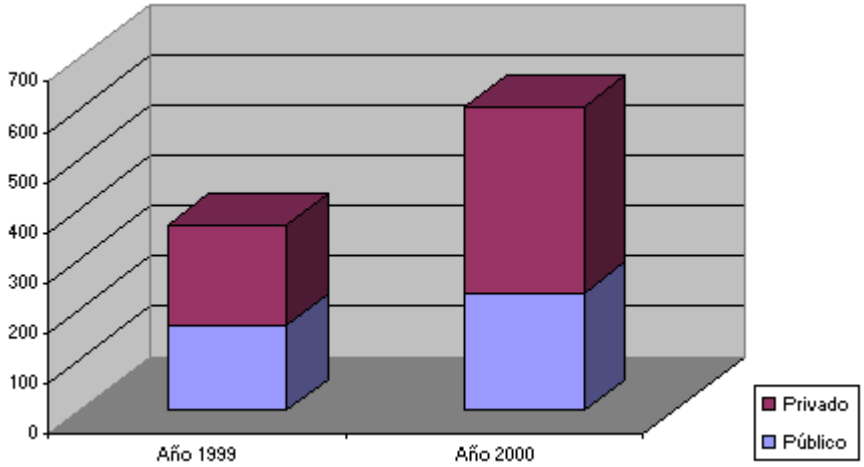
Sindicatos..... 8

Otros..... 1

Total informes..... 606

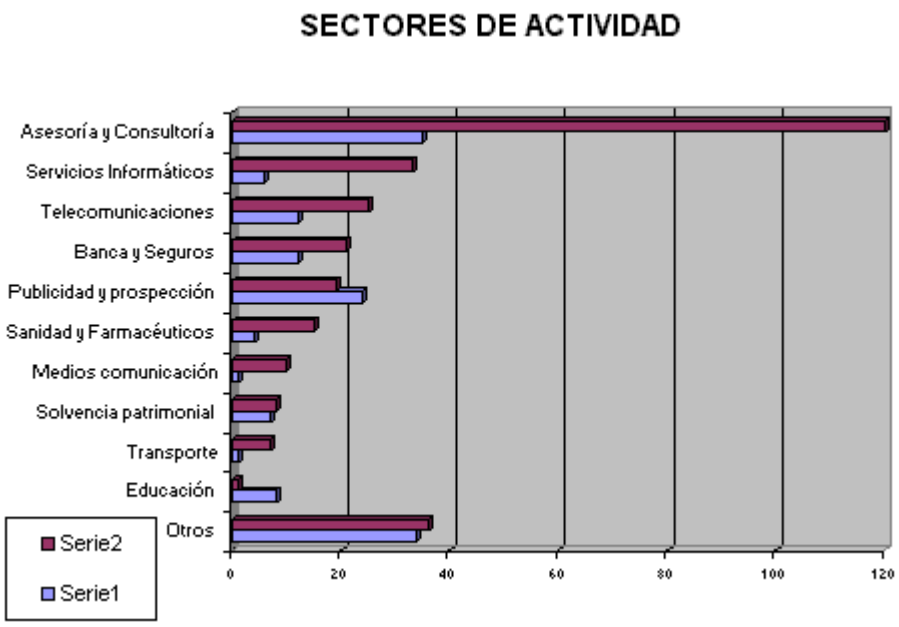


Por otra parte, el siguiente gráfico refleja la evolución del reparto de las consultas en los años 1999 y 2000.



Como se desprende de los gráficos adjuntos, y a diferencia de lo que sucedía en 1999, en que el volumen de las consultas públicas y privadas era similar, en el año 2000 han adquirido un mayor peso el número de cuestiones planteadas por el sector privado (un 62% del total), siendo de destacar asimismo la disminución de las consultas procedentes de Ayuntamientos.

Por otra parte y en relación con el sector privado, el gráfico siguiente se refleja la distribución de las consultas planteadas por los empresarios, atendiendo al sector de actividad al que los mismos pertenecen, teniendo en cuenta los datos correspondientes a 1999 y 2000.



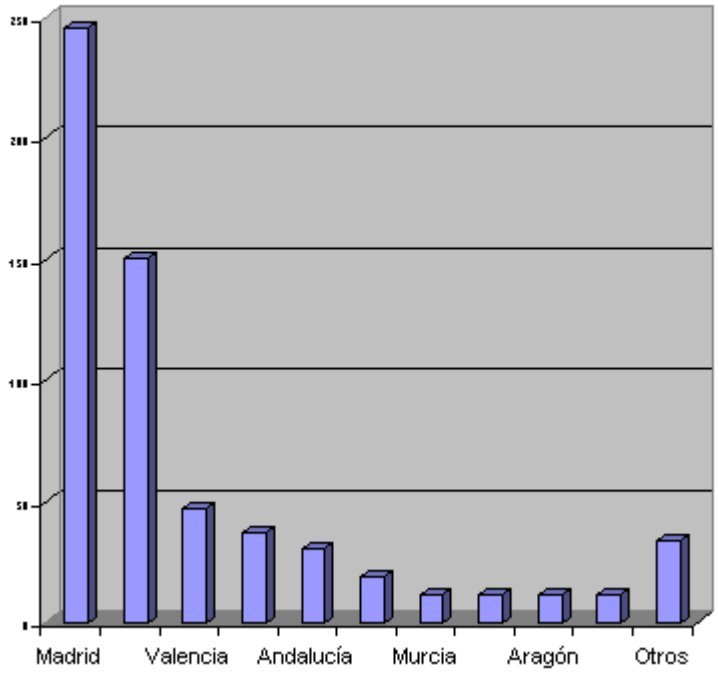
En esta distribución sectorial, resulta sumamente significativo el volumen de consultas planteadas por las entidades que realizan actividades de asesoría y consultoría (que ascienden a un 32 % del total), incluyendo las mismas tanto las relacionadas con sus propios ficheros (fundamentalmente en los casos de empresas dedicadas a actividades de gestoría) como las relacionadas con el asesoramiento y representación de los responsables de los ficheros, dada la especial complejidad de las cuestiones planteadas ante los mismos por sus clientes.

Una vez más debe reiterarse que en modo alguno encaja dentro de las actividades de la Agencia de Protección de Datos el deber de resolver aquellas cuestiones que puedan ser planteadas a las empresas destinadas a actividades de asesoría o consultoría por quienes solicitan los servicios de las mismas. En caso contrario se estaría obligando a la Agencia de Protección de Datos (al margen de las previsiones de la Ley Orgánica y del Estatuto) a llevar a cabo actividades propias de dichas entidades, sin contraprestación alguna, entrando en concurrencia con otras entidades del sector.

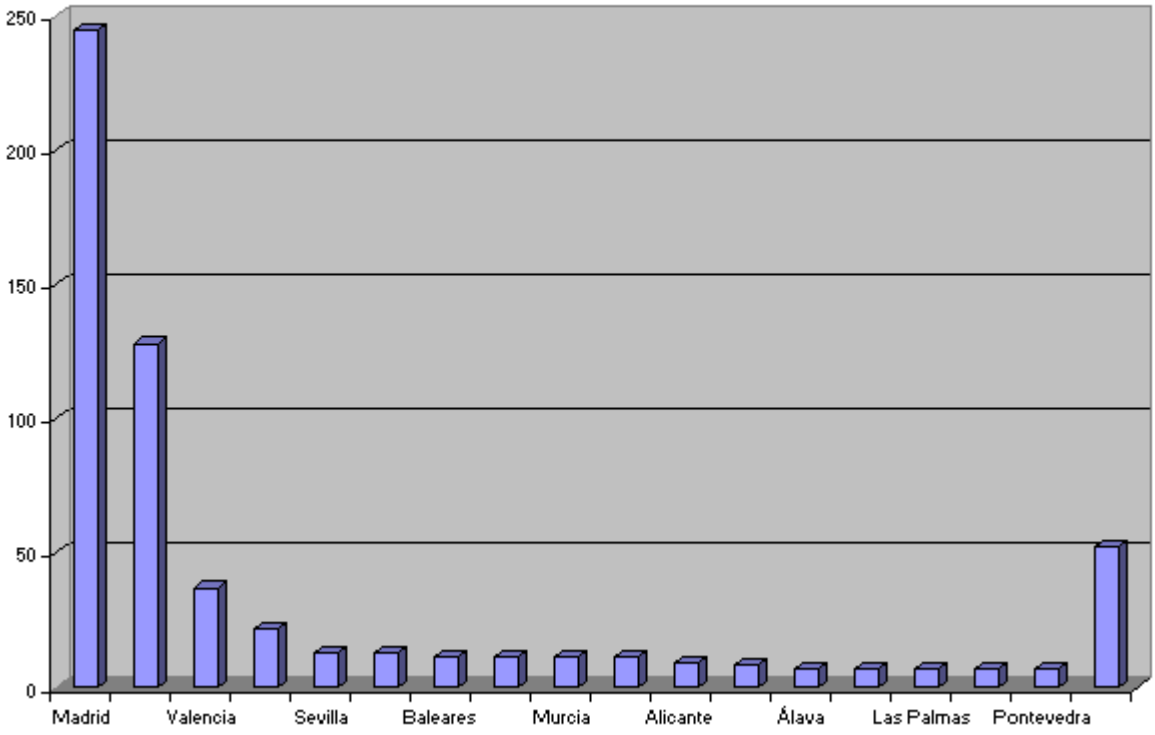
Al margen de esta referencia, es de reseñar la existencia de un cambio significativo en cuanto a los sectores de los que provienen la mayor parte de las cuestiones planteadas, disminuyendo las procedentes de sectores, tradicionalmente vinculados con la protección de datos, tales como el de la publicidad y prospección comercial o el de la solvencia patrimonial y crédito (que incluso ha disminuido en términos absolutos) . Por el contrario, se produce un importante incremento de las consultas efectuadas por las empresas pertenecientes a sectores relacionados con las tecnologías de la información; así sucede en el caso de las empresas de telecomunicaciones y las prestadoras de servicios informáticos. Por último, debe también destacarse el importante incremento producido en el sector sanitario, así como en el de los medios de comunicación.

Atendiendo, por otra parte, al origen geográfico de las consultas planteadas, debe indicarse que la práctica totalidad de las mismas (603) se plantearon por entidades u organismos nacionales, siendo sólo 3 las planteadas por entidades extranjeras. En el Gráfico siguiente se observa la distribución de dichas consultas atendiendo a la Comunidad Autónoma desde la cual se efectuaron, indicándose asimismo el origen de las consultas por provincias.

DISTRIBUCION POR COMUNIDADES AUTONOMAS DE FICHEROS PRIVADOS INSCRITOS

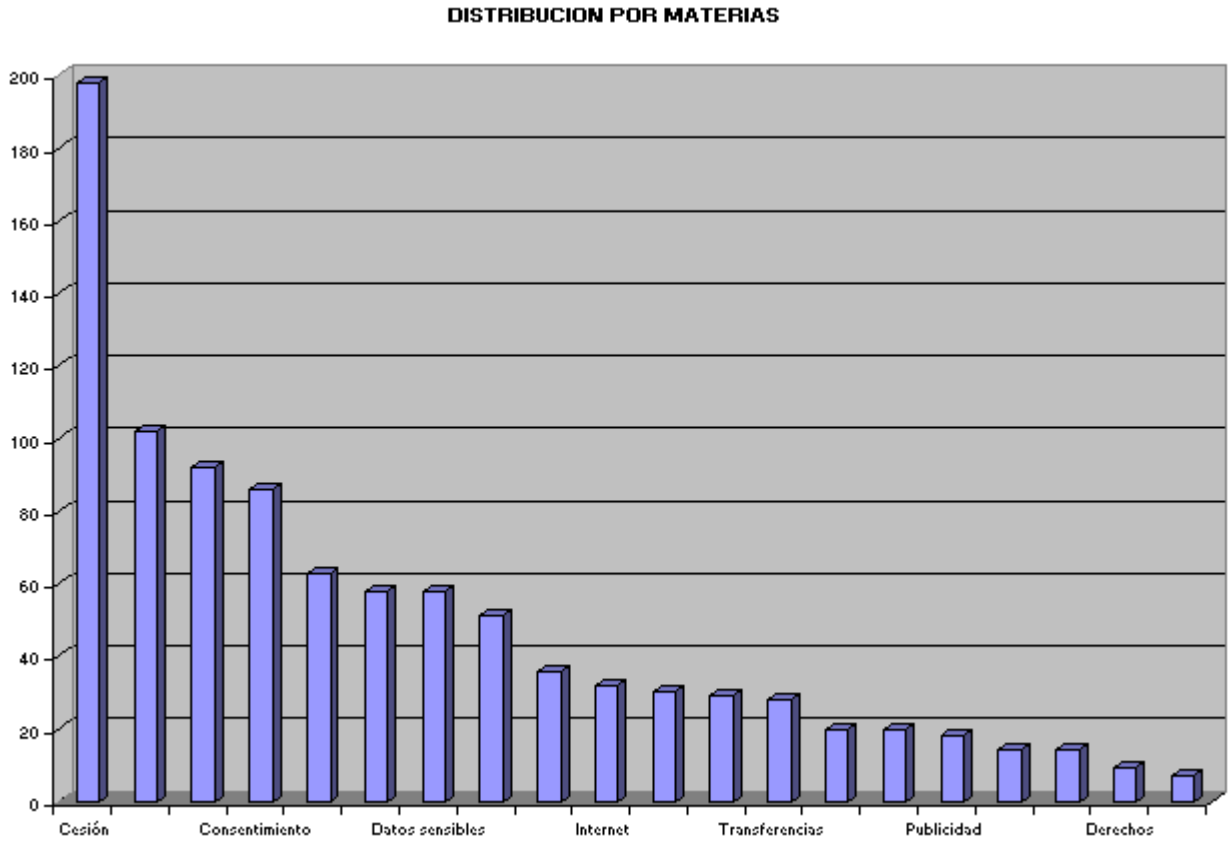


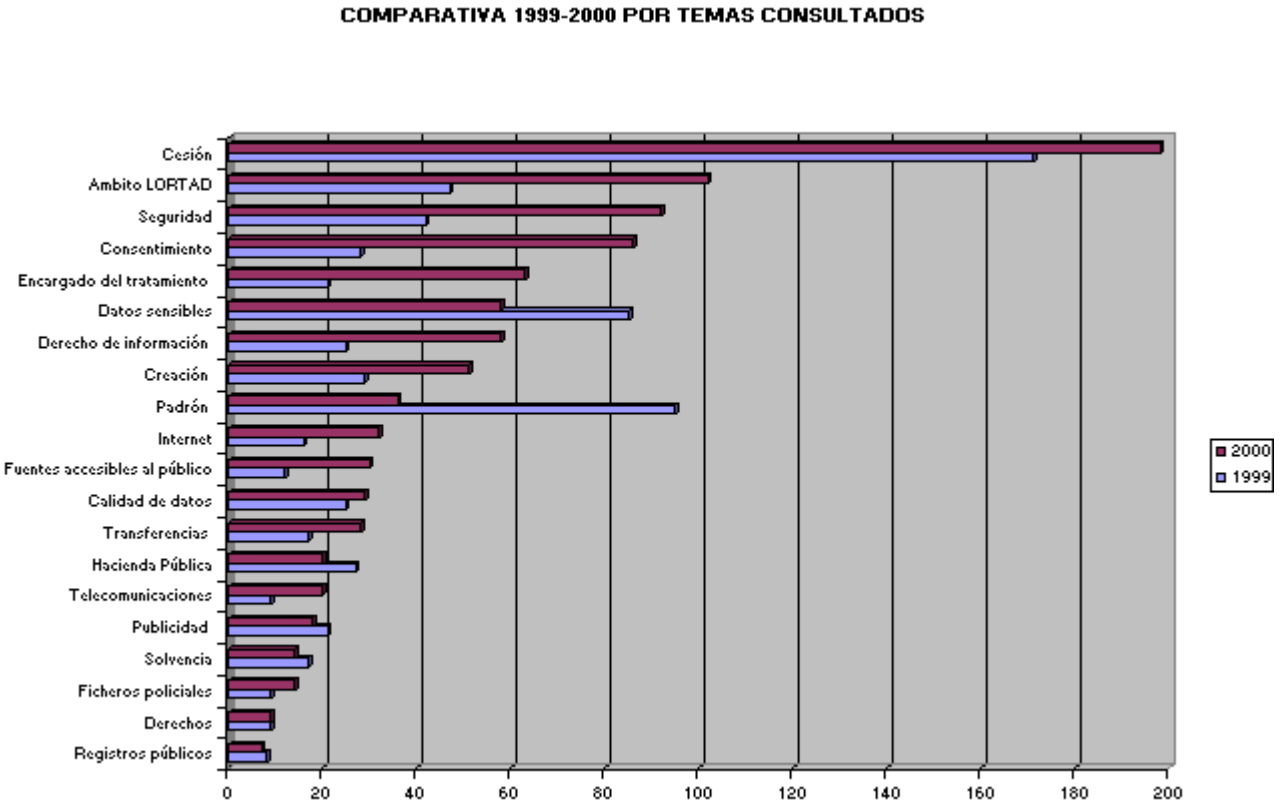
DISTRIBUCION POR PROVINCIAS DE FICHEROS PRIVADOS



De estos datos se desprende que la mayor parte de las consultas planteadas (prácticamente el 70% de las mismas) se concentran en los núcleos correspondientes a Madrid, Barcelona y Valencia, al ser éstos, como también se comprueba en otros lugares de esta Memoria, las zonas en que existe una mayor actividad relacionada con la utilización de datos de carácter personal, si bien el número de consultas planteadas en la Comunidad Valenciana se ha reducido casi a la mitad durante el año 2000.

Por último, los gráficos adjuntos se refieren a los temas objeto de consulta más frecuente, comparando el segundo de ellos las cuestiones planteadas en los años 1999 y 2000.





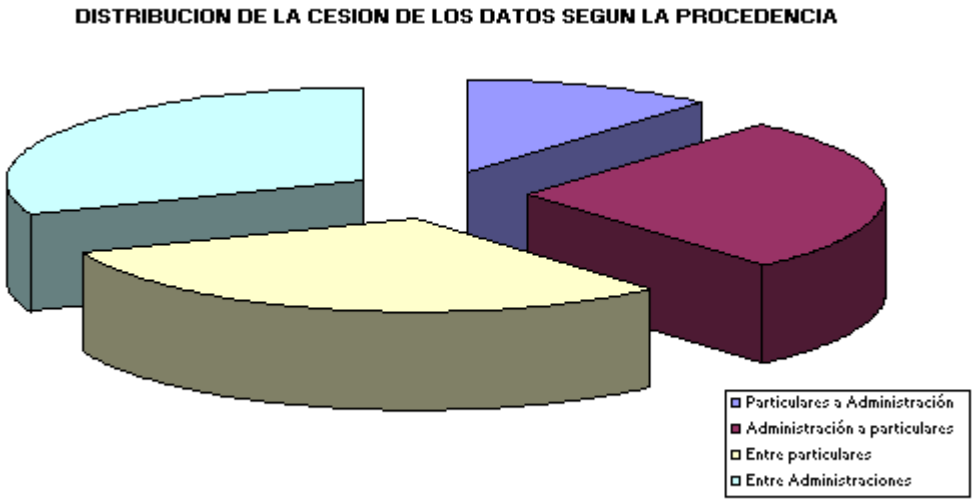
En este punto, resulta sumamente significativa la incidencia de la entrada en vigor de la nueva LOPD, manteniéndose la que se derivó de la aprobación de 1999 del reglamento de medidas de seguridad.

Así, las cuestiones planteadas en el año 2000 se han centrado, en muchos casos en la problemática derivada de las modificaciones sufridas en el régimen de protección de datos como consecuencia de la nueva Ley. Por ello el volumen de consultas relacionadas con el ámbito de aplicación de la misma se ha incrementado en un 120%, siendo especialmente relevantes las cuestiones relacionadas con la aplicación de la Ley a los empresarios individuales y a los denominados ficheros manuales.

En el mismo sentido ha existido un gran número de consultas referentes a la nueva definición de consentimiento, contenido en el artículo 3 i) de la LOPD y las consecuencias derivadas de la misma. Por otra parte también han sufrido un notable incremento (casi del 200%) las consultas relativas a lo que la Ley denomina "acceso a los datos por cuenta de terceros", en su artículo 12, fundamentalmente ligadas con la prestación de servicios a través de Internet.

La incidencia de estas cuestiones generales ha venido acompañada de una disminución en algunas otras de carácter sectorial, que venían revistiendo mayor importancia en años anteriores. En este sentido, debe destacarse la disminución en un 60% de las cuestiones relacionadas con el Padrón Municipal de Habitantes.

No obstante, de entre todos los temas sujetos a consulta, el más importante es el referente a las cesiones de datos. El gráfico adjunto pretende reflejar la distribución de este tipo de consultas, atendiendo a la naturaleza pública o privada del cedente y el cesionario:



3.2.- Estudio de las cuestiones más relevantes planteadas por los responsables de ficheros o tratamientos.

A continuación se hará referencia a aquellas cuestiones que, como consecuencia de su especial complejidad o dada la frecuencia con que han sido planteadas, resulta necesario estudiar con cierto detenimiento. Estas Cuestiones se relacionan, entre otras cuestiones, con el ámbito de aplicación de la LOPD y su entrada en vigor, diversos supuestos de cesión de datos, la aplicación del Reglamento de Medidas de Seguridad a los ficheros estadísticos, el tratamiento de los datos relacionados con la salud de las personas

3.2.1. Entrada en vigor de la LOPD. Alcance de la Disposición Adicional Primera

Se ha planteado en diversas ocasiones el alcance que debe otorgarse al contenido del párrafo primero de la Disposición Adicional Primera de la LOPD, según la cual "los ficheros y tratamientos automatizados, inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente".

El análisis de esta cuestión planteada exigirá tomar en consideración el espíritu, los antecedentes normativos de la Ley Orgánica 15/1999 y su propio contenido literal, siguiendo los criterios establecidos en el artículo 3.1 del Código Civil.

Pues bien, planteada así la cuestión, se considera que la aprobación de la Ley Orgánica 15/1999 no supone una demora en el cumplimiento de las obligaciones impuestas a los responsables de los ficheros. Ello se fundamenta en que el "período transitorio" previsto en la LOPD sólo se refiere a las obligaciones puramente formales impuestas a los responsables de los ficheros, pero nunca al cumplimiento de los deberes que les vienen impuestos por la Ley. A esta conclusión coadyuvan los siguientes motivos

PRIMERO.- El sentido literal de la norma, que prevé la "adecuación" y no el "sometimiento" al régimen previsto en la Ley, que será aplicable desde el mismo día de su entrada en vigor, conforme a lo establecido en Disposición Final Tercera.

SEGUNDO.- En este mismo sentido, la disposición se complementa con la concreción de los deberes formales (de inscripción en el Registro General de Protección de Datos) que habrán de cumplimentarse en el período transitorio de tres años, aplicable tanto a los ficheros anteriormente inscritos como a aquéllos que deberán inscribirse "ex novo" como consecuencia del régimen previsto en el artículo 2 de la Ley Orgánica.

TERCERO.- El antecedente de lo establecido en la disposición analizada se encuentra en la previsión contenida en la Disposición Adicional Segunda de la Ley Orgánica 5/1992, de 29 de octubre, de tratamiento automatizado de datos de carácter personal (LORTAD), que establecía el plazo de cumplimiento del deber formal de inscripción o, tratándose de ficheros de titularidad pública, de adopción de la correspondiente disposición de carácter general, por lo que el contenido de la Disposición Adicional Primera de la Ley Orgánica 15/1999 habrá de ser concebido con una finalidad similar.

CUARTO.- La adopción de un criterio interpretativo distinto supondría una inaplicación práctica de lo establecido en la Disposición Final Tercera de la Ley Orgánica 15/1999, según la cual "la presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el Boletín Oficial del Estado".

En efecto, si el plazo en que los ficheros debieran someterse al régimen previsto en la Ley Orgánica fuera de tres años, teniendo en cuenta que la Ley Orgánica supone una derogación expresa del régimen establecido en la LORTAD, sólo admitiría dos posibles interpretaciones: entender que la nueva Ley no entrará en vigor hasta transcurridos tres años desde el mes al que se refiere la Disposición Final Tercera, rigiendo entre tanto la LORTAD; o considerar que durante ese "período transitorio" no existiría norma alguna vigente en materia de protección de datos de carácter personal.

La segunda de las interpretaciones resulta, lógicamente inaceptable, por lo que sólo sería posible la primera, esto es, la subsistencia de la LORTAD durante el período de tres años (hasta el día 14 de enero de 2003).

Pues bien, esta última tesis tampoco resultaría aceptable si se tiene en cuenta, tal y como indica la exposición de motivos del Proyecto de Ley remitido originariamente a las Cortes, que la reforma trae su causa de la necesidad de adaptar las disposiciones de la LORTAD al régimen establecido en la Directiva 95/46/CE. La citada Directiva establece taxativamente en su artículo 32.1, párrafo primero, que "los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción", plazo que quedó cumplido el día 24 de octubre de 1998.

En consecuencia, no puede considerarse que dentro de la finalidad perseguida por la reforma se pretenda dilatar el plazo de entrada en vigor de las disposiciones contenidas en la Directiva, que debían haber sido transpuestas al derecho interno más de un año antes de la entrada en vigor de la Ley Orgánica.

QUINTO.- Además la interpretación indicada resulta ser la única coherente con la propia lógica y sistemática de la Ley Orgánica 15/1999, ya que otra interpretación supondría la inaplicación de los principios que en la Ley se contienen durante el período de tres años.

A nuestro juicio, esta interpretación carecería de sentido, debiendo prevalecer la norma que supone una mayor protección de los derechos fundamentales y libertades públicas, tal y como consagra reiterada jurisprudencia del Tribunal Constitucional, lo que supone la aplicación de lo establecido en la Disposición Adicional Primera, exclusivamente, a los aspectos formales de "adecuación" de los ficheros a la Ley Orgánica 15/1999.

En consecuencia, se indicó que el periodo de adecuación de tres años contemplado en la Disposición Adicional a la que se viene haciendo referencia se refiere exclusivamente, en cuanto a los ficheros que ya se encontraban sometidos al ámbito de aplicación de la LORTAD a los deberes meramente formales, no incidiendo en la regulación sustantiva de la protección de datos. Este criterio fue posteriormente ratificado por la Dirección del Servicio Jurídico del Estado en su Dictamen de fecha 8 de agosto de 2000.

3.2.2 Alcance del concepto del tratamiento de datos históricos con fines científicos o de investigación

Se ha planteado si es posible el tratamiento, a efectos de estudio científico, de datos contenidos en sentencias judiciales de una antigüedad superior a 50 años.

Respecto de los datos históricos, el art. 4.2 de la Ley Orgánica 15/1999 habilita la utilización de los datos, con independencia del fin para el que hubieran sido recabados, excluyendo el art. 5.5 de la Ley el deber de información a los interesados en relación con los datos que revistieran interés histórico. Del mismo modo, el artículo 11.2. e) de la Ley posibilita la cesión inconsentida de los datos cuando "cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos".

Para delimitar qué ha de entenderse como datos históricos, debe recordarse que el artículo 57.1c) de la Ley 16/1985 de 25 de Junio reguladora del Patrimonio Histórico Español establece que "los documentos que contengan datos personales de carácter policial, procesal, clínico, o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos".

A la vista de este precepto, y siempre que se cumplan los requisitos de plazo que el mismo establece, sería posible el tratamiento de los datos, siendo admisible incluso su divulgación.

En los demás supuestos, es decir cuando los documentos no tengan la antigüedad exigida por la Ley del Patrimonio Histórico Español para que los mismos puedan ser considerados como de interés histórico, será necesario recabar el consentimiento de los afectados para el tratamiento y publicación del documento, dado que en este caso, su tratamiento y divulgación no se encontrarían amparadas en ninguna disposición con rango de Ley. Por ello, sería de aplicación directa lo establecido en los artículos 6.1 y 11.1 de la Ley Orgánica 15/1999, que indica que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".

3.2.3 Caracteres del consentimiento definido por la LOPD.

Se ha planteado si el consentimiento al que se refieren diversos preceptos de la Ley Orgánica 15/1999 puede ser tácito o si, en todos los supuestos, deberá el mismo manifestarse de forma expresa.

El artículo 3.h) de la Ley Orgánica 15/1999 define que el consentimiento del interesado como "toda manifestación de

voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.", de lo cual se desprende la necesaria concurrencia para que el consentimiento pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es a juicio de esta Agencia la interpretación que ha de darse a estas cuatro notas características del consentimiento, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

De lo que se ha indicado se desprende que de las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente; así sucede en el caso de el tratamiento de datos especialmente protegidos indicando el artículo 7.2 la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical, y el artículo 7.3 la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud, el origen racial y la vida sexual.

Por tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3 de la Ley Orgánica 15/1999), si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo.

3.2.4 Consentimiento otorgado por menores de edad

También se ha planteado en diversas ocasiones qué requisitos deberá reunir el consentimiento otorgado por menores de edad, lo que exige analizar en qué supuestos se considerará que los mismos ostentan pleno discernimiento para prestar ese consentimiento y en cuáles aquél habrá de completarse con el de su representante legal.

A nuestro juicio, con carácter general, deben diferenciarse dos supuestos básicos, el primero referido a los mayores de 14 años, a los que la Ley atribuye capacidad para la realización de determinados negocios jurídicos, y el consentimiento que pudieran dar los menores de dicha edad.

Respecto de los mayores de catorce años, debe recordarse en primer término, que el artículo 162.1 del Código Civil exceptúa de la representación legal del titular de la patria potestad a "los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo".

Se plantea entonces si, en el supuesto de mayores de catorce años, ha de considerarse que el menor tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos, debiendo, a nuestro juicio, ser afirmativa la respuesta, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil. Baste a estos efectos recordar los supuestos de adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, que se efectuará por el mayor de catorce años, asistido de su representante legal, o la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 del Código Civil para los mayores de catorce años.

Por otra parte, debe recordarse que, según tiene señalado la Dirección General de Registros y del Notariado, en resolución de 3 de marzo de 1989, "no existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados". En resumen, la minoría de edad no supone una causa de incapacitación (de las reguladas en el artículo 200 del Código Civil), por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la transcendencia del acto de disposición y a la madurez del disponente.

A mayor abundamiento, y en lo referente a la prestación del consentimiento para la cesión, debe recordarse que, conforme dispone el artículo 4.3 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, "se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor,

cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales". Del tenor de esta disposición se deriva la posibilidad de que haya sido el propio menor quien, por sí mismo, haya prestado su consentimiento a la utilización de su propia imagen, sin precisar para ello la asistencia de su representante legal, lo que no hace sino ahondar en la conclusión ya referida anteriormente, a partir de lo dispuesto en el artículo 162 del Código Civil.

En consecuencia, a tenor de las normas referidas, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismo, el tratamiento automatizado de sus datos de carácter personal.

Respecto de los restantes menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162 1 del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez.

En consecuencia, a la vista de lo anteriormente señalado, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales.

3.2.5 Análisis de la figura del encargado del tratamiento

Se han recibido reiteradas consultas referidas al supuesto específico en que las actividades de una determinada empresa que implican un tratamiento automatizado de datos de carácter personal (nóminas, contabilidad, etc,) son efectuadas por una entidad asesora, sin que por la empresa se realice un tratamiento efectivo de dichos datos. En particular, se ha planteado a quien corresponderá el cumplimiento de las obligaciones reguladas por la LOPD.

De lo establecido en la mencionada Ley debe señalarse que las obligaciones que la misma impone, en particular la de proceder a la notificación del fichero a la Agencia de Protección de Datos, habrán de cumplirse por parte de quien ostente la condición de responsable del fichero, definido por el artículo 3.d) de la Ley como "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

Por tanto, la solución a la cuestión planteada deberá basarse en el hecho de si la empresa por cuya cuenta se procede al tratamiento de los datos decide sobre la finalidad y el modo en que se procederá a dicho tratamiento, con independencia de que por la misma se efectúen las operaciones que supongan la incorporación de los datos al fichero.

En concreto, en el caso en que la empresa facilite los datos a la gestoría precisamente con la finalidad de que por la misma se desarrollen las debidas actividades de tratamiento de los datos, por lo que será la cliente quien decida sobre la finalidad y uso de la información, aquella tendrá la condición de responsable del fichero y deberá notificar su existencia al Registro General de Protección de Datos.

Dado que en este caso nos encontraremos ante un supuesto en que la gestoría tendrá la condición de encargado del tratamiento, la relación entre ambas entidades deberá someterse a lo dispuesto en el artículo 12 de la Ley, siendo de destacar las siguientes cuestiones:

* En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 impone que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

* Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento", habiendo desaparecido la posibilidad de conservar los datos durante un periodo máximo de cinco años, que preveía el artículo 27.2 de la LORTAD.

* En lo referente a la cesión de los datos, de lo establecido en el artículo 12.2 se desprende que no procederá esa cesión, de forma que los datos habrán de ser entregados única y exclusivamente al responsable del fichero. Ello impide, a nuestro juicio, la posibilidad de proceder a una subcontratación de este tipo de servicios por parte del encargado del tratamiento, debiendo siempre el responsable ser parte en la relación jurídica, ya que cualquier transmisión de los datos a un tercero que no corresponda al responsable del fichero habrá de ser considerada cesión.

* En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica.

* Por último, según el artículo 12.4, "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", siendo, en consecuencia, de

aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen.

3.2.6 Difusión de datos de Sentencias condenatorias por negligencia médica

Se ha planteado si es posible la difusión a través de Internet de datos relativos a sentencias firmes condenatorias por delitos relacionados con negligencia médica. Se indicaba que los datos serían tratados y cedidos sin recabar con carácter previo el consentimiento del interesado, toda vez que, según indicaba la consulta "los datos se extraerían de fuentes accesibles al público, como lo son las sentencias públicas".

En este caso, tras recordar que el artículo 6 de la LOPD parte de la exigencia de consentimiento para el tratamiento de los datos, con las únicas excepciones de su apartado segundo, se indicó que en cuanto a los ficheros en que se contengan datos relacionados con la comisión de infracciones penales y administrativas, el artículo 7.5 de la LOPD establece que tales datos "sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras".

En consecuencia, el artículo 7.5 de la Ley establece una regla específica para este tipo de datos, que impide, en todo caso, su tratamiento por parte de cualquier entidad de derecho privado, quedando limitado dicho tratamiento a las Administraciones Públicas y, exclusivamente, cuando así lo establezca una norma con rango suficiente. De ello se desprende que, incluso si los datos contenidos en las resoluciones judiciales fueran considerados incorporados a fuentes accesibles al público, su tratamiento inconsentido se encontraría vedado por la Ley a la consultante, dada su naturaleza jurídico-privada.

Dicho lo anterior, y en relación con la alegación de que los datos se encontraban incorporados a fuentes accesibles al público, se recordó que, como se dice en otros lugares de esta memoria, la simple lectura del tenor literal del artículo 3. j) de la LOPD indica que las resoluciones judiciales no pueden ser consideradas como fuente accesible al público, sin perjuicio del principio de publicidad contenido en la Ley Orgánica del Poder Judicial, recordándose así mismo que la regla general establecida en el inciso primero del artículo 3.j) en modo alguno impide que resulte de aplicación la enumeración taxativa contenida en su inciso segundo, dado que el contenido de este primer inciso no hace sino indicar un requisito indispensable para que los ficheros enumerados por la propia norma puedan ser considerados como fuentes de acceso público. En resumen tales ficheros sólo serán considerados como fuentes de acceso público cuando su consulta pueda ser realizada por cualquiera sin ninguna limitación salvo, en su caso, el abono de un precio, pero sólo son fuentes de acceso público las enumeradas, entre las que no se encuentran las resoluciones judiciales.

Por otra parte, la conclusión alcanzada tampoco contradice el principio de publicidad de las actuaciones judiciales, consagrado en cuanto a las sentencias por los artículos 205.6, 232 y 266 de la Ley Orgánica del Poder Judicial, al que ya hicimos referencia.

Ello se funda en que la publicidad a la que se refieren dichos preceptos tiene por objeto asegurar el pleno desenvolvimiento del derecho de las partes a obtener la tutela efectiva de los jueces y Tribunales en el ejercicio de sus derechos, sin que en ningún modo pueda producírseles indefensión, consagrado por el artículo 24.1 de la Constitución. Por ello, entendemos, no puede ampararse en un precepto cuyo fundamento es la salvaguarda de los derechos de los ciudadanos la realización de otras actividades que pueden producir una merma de otros derechos fundamentales, como en este caso, el derecho al honor, la intimidad y la propia imagen, protegido por el artículo 18 de la propia Constitución.

La colisión entre la publicidad de las sentencias y el derecho a la intimidad de las personas ya ha sido, por otra parte, analizado por el Consejo General del Poder Judicial, disponiendo en el Acuerdo de 18 de junio de 1997, por el que se modifica el Reglamento número 5/1995, de 7 de junio, regulador de los aspectos accesorios de las actuaciones judiciales, como apartado 3 del nuevo artículo 5 bis del Reglamento, que "en el tratamiento y difusión de las resoluciones judiciales se procurará la supresión de los datos de identificación para asegurar en todo momento la protección del honor e intimidad personal y familiar".

En consecuencia, el tratamiento de los datos contenidos en las sentencias condenatorias firmes resulta contrario a las previsiones contenidas en la LOPD, al quedar éste limitado a las Administraciones Públicas, en el ejercicio de las atribuciones que les son conferidas por la Ley, sin que quepa amparar su tratamiento por partes ajenas al proceso en normas cuyo fundamento es precisamente salvaguardar los derechos procesales de quienes son parte en el propio proceso.

En cuanto a la difusión de los datos a través de Internet, se recordó que la misma, dado que el contenido de la citada lista podría resultar conocido por cualquier usuario en la citada red, supondría un cesión de datos de carácter personal, respecto de la cual el artículo 11.1 de la Ley Orgánica prevé, con absoluta rotundidad que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".

Esta regla sólo se ve exceptuada en los supuestos contemplados en el apartado segundo del propio artículo 11, ninguno de los cuales daría cobertura a la publicación pretendida, dado que el único que podría resultar de dudosa aplicación al caso es el contenido en la letra b) del artículo 11.2 ("cuando se trate de datos recogidos de fuentes accesibles al público") y, como se ha dicho, los datos no se encuentran, en este caso, recogidos en fuentes accesibles al público.

Debe ponerse de manifiesto que el artículo 44 de la LOPD, que establece los distintos tipos de las infracciones en

materia de protección de datos tipifica, incluye, como infracción grave, en la letra c) de su apartado tercero "proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible" y como infracción muy grave, en la letra b) de su apartado cuarto "la comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas ".

Por ello, tanto el tratamiento como la publicación en Internet de los datos a que se refiere la consulta podrían ser, a tenor de lo que se ha venido indicando, constitutivas de sendas infracciones, sancionables, respectivamente con multas de 10 a 50 y de 50 a 100 millones de pesetas, conforme a lo previsto en el artículo 45 de la Ley.

Por último, se planteó si resultaba admisible establecer listas o repertorios de las sentencias dictadas en que existan condenas por negligencia médica, publicándose los datos con referencia exclusiva al nombre e iniciales de los apellidos de los afectados.

Con carácter general, y en lo referente a los repertorios, su publicación será posible, a juicio de esta Agencia de Protección de Datos, siempre y cuando de la misma no pueda derivarse el conocimiento de la persona que haya resultado condenada por la sentencia. En caso contrario, tal y como se ha venido indicando hasta ahora, no será posible la difusión de las sentencias sin antes recabar el consentimiento de los afectados.

En este sentido, las disposiciones de la LOPD no serán de aplicación siempre que los datos hayan sido previamente sometidos a un procedimiento de disociación, que el artículo 3 f) de la Ley define como "todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable".

En consecuencia, para que un procedimiento de disociación pueda ser considerado suficiente a los efectos de la Ley Orgánica 15/1999, será necesario que de la aplicación de dicho procedimiento resulte imposible identificar un determinado dato con su sujeto determinado.

A la vista de lo anterior, y teniendo en cuenta las especiales circunstancias concurrentes en el presente caso, en que los facultativos pueden ser identificados no sólo por su nombre y apellidos, sino también por el puesto que desempeñan en un determinado centro sanitario o, incluso, en áreas reducidas, por ser el único especialista en una determinada rama de la medicina, la mera sustitución de los apellidos por sus iniciales puede no resultar suficiente para que la disociación pueda considerarse conforme a lo prevenido en la LOPD, dado que si dicha supresión no va acompañada de la referente al puesto desempeñado y, en su caso, a la del área geográfica en la que el facultativo desempeña su profesión, no será posible considerar que aquél no resulta identificable, debiendo, en ese caso, someterse el fichero a las previsiones de la Ley, que exigen el consentimiento del afectado.

Por otra parte, la conclusión anteriormente alcanzada no entorpece la finalidad perseguida mediante la elaboración del repertorio jurisprudencial, que permite al usuario tener conocimiento de la doctrina y jurisprudencia existente en una determinada materia, partiendo del concepto de jurisprudencia como "doctrina que, de modo reiterado, establezca el Tribunal Supremo al interpretar y aplicar la ley , la costumbre y los principios generales del derecho", en los términos prescritos por el artículo 1.6 del Código Civil.

En consonancia con lo indicado, la finalidad que debe perseguir la creación de la base de datos será la de permitir al usuario acceder al conocimiento del modo en que el Tribunal Supremo o los restantes Juzgados y Tribunales han interpretado lo establecido en el ordenamiento jurídico, sin que sea dable que dicha finalidad pueda ser contemplada en un sentido más amplio, con la consiguiente cercenación de los derechos fundamentales de las personas que intervengan en el litigio, como sucedería si se conocieran los datos personales referidos a dichas personas, que en modo alguno aportan información adicional sobre el contenido jurídico de la sentencia. Así lo recuerda el Consejo general del Poder Judicial, en la Exposición de Motivos del Acuerdo de 18 de junio de 1997, al que ya nos hemos referido, al indicar que con la publicidad de las sentencias en el repertorio "se posibilitará un mejor y más directo conocimiento de dichas resoluciones por parte de los Juzgados y Tribunales, contribuyendo al propio tiempo a satisfacer las exigencias derivadas del derecho de igualdad en la aplicación de las Leyes, conforme a la doctrina del Tribunal Constitucional", sin que esta función informadora pueda entenderse en modo alguno completada con el conocimiento de quienes fueron parte en el litigio.

3.2.7.- Cesión de datos de afiliación sindical

Se ha consultado si resulta posible la cesión por parte del empresario del dato referente a la afiliación sindical a aquella entidad aseguradora con quién haya contratado la externalización de sus compromisos de pensiones.

Con carácter general, la cesión a la entidad adjudicataria de los datos referentes a los trabajadores trae causa de lo establecido en la Disposición Adicional Primera de la Ley 8/1987, de 8 de junio, de regulación de los Planes y Fondos de Pensiones, en la redacción que a la misma da el apartado 19 de la Disposición Adicional undécima de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión del Seguro Privado. Según el apartado primero de la citada Disposición "Los compromisos por pensiones asumidos por las empresas, incluyendo las prestaciones causadas, deberán instrumentarse, desde el momento en que se inicie el devengo de su coste, mediante contratos de seguro, a través de la formalización de un plan de pensiones o de ambos. Una vez instrumentados, la obligación y responsabilidad de las empresas por los referidos compromisos por pensiones se circunscribirán exclusivamente a las asumidas en dichos contratos de seguro y planes de pensiones".

En consecuencia, el citado precepto establece una habilitación legal para la cesión, con carácter general, de los datos de carácter personal referidos a los trabajadores con los que la empresa haya asumido el compromiso de pago de las

pensiones, en los términos que la propia Ley establece, toda vez que se impone la obligación de que dichos compromisos sean satisfechos por un tercero ajeno a la propia empresa. Así, la cesión, en general, de los datos encontrará su apoyo en lo establecido en el artículo 11.2 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Sin embargo, el problema se plantea en relación con la cesión de los denominados datos especialmente protegidos y, en particular, en relación con los referidos a la afiliación sindical de los trabajadores.

El artículo 7.2 de la Ley Orgánica 15/1999 establece, en su inciso primero, que "sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias". De este precepto se desprende inequívocamente que cualquier tratamiento de los datos relacionados con la afiliación sindical de los trabajadores exigirá su consentimiento, que además deberá ser expreso y escrito.

En cuanto al concepto de tratamiento, el artículo 3 c) de la Ley considera que serán tratamientos las "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". En consecuencia, la cesión de los datos, como la indicada en la consulta entraría en el concepto establecido por la norma, requiriendo por ello el consentimiento del afectado.

La misma conclusión se alcanza si se tiene en cuenta lo establecido en el segundo inciso del propio artículo 7.2, según el cual "se exceptúan (de la regla ya mencionada) los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado".

De todo ello se desprende que cualquier cesión de datos que se encuentren sometidos al régimen de especial protección contenido en el artículo 7.2 de la Ley Orgánica 15/1999 requerirá el consentimiento expreso y por escrito del afectado, aún cuando la cesión de los restantes datos se encuentre amparada en una norma con rango de Ley.

En consecuencia, será preciso recabar el consentimiento de los afectados para comunicar a la empresa a la que se hayan externalizado los compromisos de pensiones de la consultante los datos referentes a la afiliación sindical de aquéllos.

3.2.8.- Cesión a los Representantes Sindicales de los trabajadores

Se ha planteado reiteradamente por distintas Administraciones Públicas si es posible la cesión a los integrantes de la Junta de Personal de una relación de funcionarios, en la que se incluirán determinados datos de carácter personal referentes a los mismos.

Teniendo en cuenta lo indicado en la Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre, analizada en otro lugar de esta memoria, la cesión de datos por parte de las Administraciones Públicas (salvo cuando el cesionario sea otra Administración y la transmisión se funde en el ejercicio de una misma competencia) se encuentra sometida al principio de reserva de Ley, por lo que es necesario delimitar si en este caso existe una Ley habilitante.

En este sentido, el artículo 9 de la Ley 9/1987, reguladora de los Órganos de Representación y Condiciones de Trabajo y Participación del Personal al Servicio de las Administraciones Públicas enumera las funciones atribuidas a las Juntas de Personal, incluyéndose entre las mismas, no sólo la recepción de información, sino también "vigilar el cumplimiento de las normas vigentes en materia de condiciones de trabajo, seguridad social y empleo, y ejercer, en su caso, las acciones legales oportunas ante los organismos competentes" (artículo 9.6) y "vigilar y controlar las condiciones de seguridad e higiene en el desarrollo del trabajo" (artículo 9.7).

Por su parte, el artículo 15.3 de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, establece el carácter público de las Relaciones de Puestos de Trabajo, si bien las mismas, no contendrán, a la vista del contenido exigido por el artículo 15.1 b), los datos del personal concreto que ocupe un determinado puesto de trabajo, sino exclusivamente las características de cada uno de los puestos de trabajo existentes en cada dependencia Administrativa, siendo los datos personales referidos a cada funcionario público, de acceso restringido a éste último, a tenor de lo dispuesto en el artículo 13.5, párrafo segundo de la propia Ley 30/1984.

Se hace preciso, en consecuencia, cohonestar las atribuciones conferidas a las Juntas de Personal en la Ley 9/1987 con la protección otorgada a los datos automatizados de carácter personal, regulada en la Ley Orgánica 15/1999, y con los límites previstos en el artículo 21 para la posible cesión de esos datos.

Pues bien, según el criterio de la Agencia la función de vigilancia y protección de las condiciones de trabajo, atribuida a las Juntas de Personal por la Ley 9/1987 puede llevarse a adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en el Órgano o Dependencia correspondiente. Sólo en el supuesto en que la vigilancia o control se refieran a un sujeto concreto, que haya planteado la correspondiente queja ante la Junta de Personal, será posible la cesión del dato específico de dicha persona

3.2.9.- Aplicación del Real Decreto 994/1999 a ficheros estadísticos

Se ha planteado si las medidas de seguridad cuya implantación impone el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, resultan exigibles en los ficheros estadísticos sometidos a su legislación específica.

El estudio de la cuestión planteada pasa necesariamente por el análisis del ámbito de aplicación de las normas reguladoras de la protección de datos de carácter personal y, en especial, de la LOPD, de cuyo artículo 9 trae causa el propio Reglamento.

El artículo 2.3 b) de la citada Ley Orgánica establece, como punto de partida que "se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales...los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública". De lo antedicho se desprende que, como punto de partida, la normativa aplicable a los ficheros estadísticos será la que específicamente los regule, sin perjuicio de la aplicación de la Ley Orgánica en aquellos supuestos que la misma prevea.

En materia de seguridad, no obstante, el artículo 37 m) de la Ley, al enumerar las funciones de la Agencia de Protección de Datos, establece expresamente, tras indicar que la Agencia velará "por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico", que le corresponderá a la propia Agencia, "dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46".

En este mismo sentido, el artículo 6 d) del Estatuto de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, establece, dentro de las funciones de la misma relacionadas con los ficheros exclusivamente estadísticos, la de "dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos".

A la vista de lo establecido en los dos preceptos últimamente citados, cabe concluir que corresponde a esta Agencia de Protección de Datos decidir sobre el nivel de seguridad al que deberán someterse los ficheros de datos de carácter personal que sean objeto de tratamiento para fines exclusivamente estadísticos, no encontrándose dichos ficheros excluidos del ámbito de aplicación de la Ley en lo que se refiere a las medidas de seguridad que sea necesario adoptar sobre los mismos.

Dicho lo anterior, del artículo 1 del Reglamento de Seguridad se desprende que sus disposiciones serán aplicables a los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal sujetos al régimen previsto por la normativa reguladora de la protección de datos de carácter personal. Tal previsión tiene su causa en lo establecido en el artículo 9 de la Ley Orgánica, que prevé la necesidad de que se adopten "las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural", prohibiéndose el registro de datos de carácter personal en ficheros que no reúnan las necesarias condiciones respecto a su integridad y seguridad".

En consecuencia, nuestro legislador considera que las medidas de seguridad que se adopten en desarrollo de lo establecido en la Ley Orgánica serán las que efectivamente vendrán a garantizar un adecuado tratamiento de los datos de carácter personal, de forma que, en caso de no adoptarse tales medidas, el tratamiento resultaría contrario a la Ley, por producirse un insuficiente nivel de protección.

A la vista de ello, la Agencia de Protección de Datos considera que cualesquiera ficheros que, en lo referente a la seguridad de los ficheros y tratamientos, no se encuentren expresamente excluidos del ámbito de aplicación de la Ley Orgánica 15/1999 (por ejemplo, los enumerados en el artículo 2.2 de la misma) habrán de someterse a las medidas de seguridad contenidas en el Real Decreto 994/1999, dado que sólo en ese caso quedará suficientemente garantizada la protección de los datos de carácter personal contenidos en el fichero o tratamiento.

Por ello, cabe concluir que, sin perjuicio de la aplicación de su legislación específica en otras materias, los ficheros creados para fines exclusivamente estadísticos que contengan datos de carácter personal habrán de implantar las medidas de seguridad a las que se refiere el Reglamento de Seguridad, siendo el nivel de las mismas el que corresponda en atención a lo previsto en el artículo 4 del propio Reglamento.

3.2.10.- Tratamiento de datos genéticos para la localización de personas desaparecidas o en la investigación criminal.

Habiéndose planteado la viabilidad de la creación de diversos ficheros que contengan muestras genéticas para la identificación de cadáveres de personas desaparecidas, la Agencia de Protección de Datos sin perjuicio de los comentarios específicos al respecto indicó una serie de consideraciones que habrán de ser en todo caso tenidas en cuenta en relación con la creación de ficheros que contengan datos genéticos y que pueden resumirse en las siguientes:

PRIMERA: En primer lugar, en tanto los datos incluidos en los ficheros se refieran a personas identificadas o identificables con arreglo a determinados criterios, los ficheros se encontrarán sometidos a la Ley Orgánica 15/1999.

Ello sucederá, por ejemplo, en el caso de los datos genéticos referentes a personas desaparecidas, toda vez que el

objetivo del tratamiento será, precisamente, asociar la muestra genética con una determinada persona desaparecida, a fin de lograr su identificación futura. Del mismo modo, también se encontrarán sometidos a la Ley Orgánica 15/1999 los datos referentes a quienes voluntariamente se presten a la realización de los análisis.

Por último, en cuanto a los vestigios hallados en el escenario de un determinado hecho, no identificarán, en principio, a la persona a que se refieren. Ello no obstante, en cuanto los mismos puedan ser cotejados con otros datos que pudieran existir, entendemos que el fichero deberá someterse a la Ley, dado que podemos encontrarnos ante datos referidos a personas identificables.

SEGUNDA: En segundo término, debemos recordar que, en todo caso, nos encontraremos ante datos relacionados con la salud de las personas.

Prescindiendo aquí de la discusión acerca de los efectos del análisis de ADN codificante o expresivo y no codificante, debe señalarse que, si bien es posible que del resultado del análisis de ADN no codificante no se deriven directamente datos de salud, dichos resultados vienen a conformar la huella genética de una persona, y por tanto, se encuentran íntimamente relacionados con su salud.

Así lo reconoce la Recomendación (97) 5 del Comité de Ministros del Consejo de Europa, relativa a la protección de datos médicos, que define la expresión "dato médico" como todos los datos de carácter personal relativos a la salud de una persona, añadiendo que dicha expresión afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas.

En este mismo sentido, la Recomendación se refiere expresamente a los datos genéticos, no delimitando en ningún caso aquellos que pudieran derivarse de análisis de distintos de tipos de ADN, sino considerando que tanto uno como otros son datos estrechamente relacionados con la salud. Así, la Recomendación señala que la expresión "datos genéticos" se refiere a todos los datos, de cualquier tipo, relacionados con los caracteres hereditarios de un individuo o que, vinculados a dichos caracteres compongan el patrimonio de un grupo de individuos emparentados. Además se indica que este concepto también se refiere a todos los datos que afecten a intercambios de información genética de un individuo o línea genética, con relación a cualquier aspecto de la salud o de una enfermedad, constituya o no un carácter identificable.

En consecuencia, cualquier dato personal de carácter genético deberá ser considerado como un dato que afecta a la salud de las personas y, por tanto, sujeto a las disposiciones específicas aprobadas para la regulación de este tipo de datos de carácter personal.

TERCERA: Por otra parte, más que en otros supuestos, resulta especialmente importante en este caso tener en consideración los principios de finalidad y calidad de los datos, consagrados por el artículo 4 de la Ley Orgánica 15/1999.

Con arreglo al primero de ellos "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido" (artículo 4.1 de la Ley), siendo además de destacar que "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos" (artículo 4.2).

Además, el principio de calidad de los datos exige que los datos de carácter personal sean cancelados "cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados" (artículo 4. 5).

Quiere ello decir que deberá ser tenida especialmente en consideración esta circunstancia al incorporar y mantener los datos en cualquiera de los ficheros, de forma que únicamente se apliquen para dicho fin, siendo cancelados en caso de cumplirse éste (cuando aparezca, viva o muerta, la persona incluida como desaparecida, así como las de quienes se ofrezcan a incluir sus datos para lograr su identificación o cuando concluya la investigación criminal o, en su caso, el procedimiento penal correspondiente), no siendo posible la conservación de los datos para otros fines y mucho menos para elaborar perfiles genéticos de la población (la denominada codificación genética) o mantener bancos de ADN obtenidos sin consentimiento del afectado para la investigación de futuras conductas criminales. A nuestro juicio, esta conservación sólo sería posible en caso de que una norma con rango de Ley así lo permitiese (ex artículo 7.3 de la Ley Orgánica 15/1999), lo que aún no se ha producido en nuestro país.

Debe tenerse especialmente en consideración que la huella genética de la persona puede afectar, de una manera u otra, su vida futura, por lo que es preciso que esta circunstancia se cumpla estrictamente, a fin de evitar un perjuicio a los afectados como consecuencia de la conservación de un dato durante un período de tiempo superior al admisible.

CUARTA: Por último, y en virtud de lo anteriormente indicado, cualquier tratamiento que se refiera a los datos relacionados con la huella genética de la persona debe efectuarse con suma precisión y cautela, de forma que se respeten íntegramente las previsiones que se han venido señalando. Ello supone que la regulación de estos ficheros deberá huir de cualquier invocación genérica, ambigua o imprecisa, que pudiera permitir una evasión del antedicho régimen.

Del mismo modo si existieran, en su caso, excepciones al régimen general, deben las mismas traer causa de la aplicación del régimen previsto en nuestro derecho positivo, siendo indispensable que tales excepciones consten claramente en la norma de creación del fichero, a fin de evitar, precisamente, las consecuencias perniciosas que pudieran derivarse del tratamiento de los datos genéticos.

3.2.11.- Tratamiento y cesión de los datos contenidos en el Padrón Municipal de Habitantes

Si bien el estudio de las cuestiones relacionadas con el padrón municipal de habitantes se efectuó, con gran detalle, en la memoria correspondiente a 1999, se considera necesario volver a insistir en las cuestiones relativas al mismo, toda vez que, dado que las consultas sobre esta materia (aun siendo menores en número a las planteadas en 1999), han sido abundantes.

En este sentido, y en lo referente al tratamiento de los datos contenidos en el Padrón Municipal, su régimen jurídico viene recogido en los artículos 15 y siguientes de la Ley de Bases de Régimen Local, en la redacción dada por la Ley 4/1996, de 10 de enero, normativa que debe considerase como la disposición de creación del fichero ®Padrón municipal¯, en cuyo cumplimiento los municipios deben organizar y mantener el fichero previsto legalmente.

De la LBRL se deduce que la finalidad para que sirven los datos del Padrón municipal es la constitución de la población del municipio (artículo 15.2 LBRL), la adquisición de la condición de vecino (art. 15.3 y 4) y la acreditación de la residencia en el municipio y del domicilio habitual del mismo (art. 16.1).

Para la efectividad del cumplimiento de estas finalidades se establece la obligación de inscripción en el Padrón municipal por parte de quien resida habitualmente en el municipio respectivo, lo que supone una excepción al principio básico de la necesidad del consentimiento del ciudadano para la legalidad del tratamiento de sus datos, contenido en el artículo 6.1 de la LOPD. Esta excepción se funda en lo establecido en el artículo 6.2 que permite el tratamiento inconsentido de los datos por parte de las Administraciones Públicas "para el ejercicio de sus funciones ... en el ámbito de sus competencias".

Por otra parte, y en cuanto a las cesiones de los datos del padrón, debe recordarse que, siendo Padrón un fichero de titularidad pública, deberá partirse, del principio de delimitación de la finalidad en las cesiones entre Administraciones Publicas consagrado por el artículo 21 de la LOPD, al exigir que si los datos son cedidos a otras Administraciones Publicas sirvan sólo para el ejercicio de competencias iguales o que versen sobre materias semejantes, con la única excepción, tras la STC de 30 de noviembre de 2000, de que el cambio de finalidad esté fundado en una de las causas contenidas en el artículo 11 de la Ley, pudiendo ser sustituida la necesidad del consentimiento para el cambio de finalidad por una previsión realizada en una disposición con rango de Ley (art.11.2 a).

Asimismo, del apartado tercero de dicho artículo 21 se deduce que no es posible, sin el consentimiento del ciudadano, ceder datos de un fichero de titularidad pública a uno de titularidad privada, salvo previsión legal en contrario.

La norma de creación del Padrón Municipal, (LBRL) recoge en su artículo 16.3 los principios que rigen la transmisión de los datos del Padrón Municipal, estableciendo que "los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública. Fuera de estos supuestos, los datos del Padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común"

La Agencia de Protección de Datos ha considerado que la expresión ®datos del Padrón municipal¯ que se emplea en el artículo 16.3 de la LBRL se refiere únicamente a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio. Por ello, cualquier cesión de los datos del Padrón deberá fundarse en la necesidad por la Administración cesionaria, en el ejercicio de sus competencias, de conocer el dato del domicilio de la persona afectada, dado que del artículo 4.2 de la LOPD se deriva la imposibilidad del tratamiento de los datos para fines diferentes de los que motivaron su recogida, salvo que así lo consienta el afectado o la Ley lo prescriba.

Existen numerosas excepciones a esta regla general, entre otras:

1.- Las establecidas en las Leyes Orgánicas de Reclutamiento y de Régimen Electoral General,

2.- La establecida en el artículo 11.2 de la LOPD, respecto de cesiones a la Administración Sanitaria,

3.- La consagrada por el artículo 22 de la LOPD, respecto de cesiones a las Fuerzas y Cuerpos de Seguridad,

4.- Las previsiones de la Ley Orgánica 4/1981, de 1 de junio, Reguladora de los Estados de alarma, excepción y sitio,

5.- La establecida en la Ley Orgánica del Poder Judicial y en el artículo 11.2 d) de la LOPD, respecto de la colaboración con la Administración de Justicia y determinadas instituciones públicas,

6.- La contenida en el artículo 112 de la Ley General Tributaria, de colaboración con la AEAT,

7.- La prevista en la Ley General de la Seguridad Social, en cuanto a procedimiento recaudatorio de recursos.

Por último, se ha planteado la incidencia que sobre esta materia ha podido producir lo establecido, en cuanto al Registro Poblacional, la Disposición Adicional 2¦ de la LOPD, según cuyo párrafo primero "la Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población".

A juicio de la Agencia esta disposición prevé exclusivamente la posibilidad de que el censo poblacional al que la misma se refiere pueda ser solicitado por las Administraciones Estatal y Autonómica del Instituto Nacional de Estadística, único al que se autoriza expresamente la cesión inconsentida de los datos a que la Disposición se refiere, por lo que los Ayuntamientos sólo podrán ceder los datos padronales en aquellos supuestos que se han indicado. En los demás casos, sólo está admitida por la Ley la cesión que efectúa el Instituto Nacional de Estadística, en los términos previstos en la citada Disposición Adicional Segunda.

3.2.12.- Tratamiento y cesión de los datos por parte de las Haciendas Locales

En esta materia, como punto de partida, debe señalarse que el artículo 2.2 de la Ley 39/1988, de 28 de diciembre, consagra el principio de que "Para la cobranza de los tributos y de las cantidades que como ingresos de Derecho público debe percibir la Hacienda de las Entidades locales, de conformidad con lo previsto en el apartado anterior, dicha Hacienda ostentará las prerrogativas establecidas legalmente para la Hacienda del Estado, y actuará, en su caso, conforme a los procedimientos administrativos correspondientes".

Ello supone que, en el ejercicio de sus competencias, resultarán de aplicación a las Haciendas Locales las mismas prerrogativas que la Ley General Tributaria atribuye a la Hacienda Estatal, lo que tiene una enorme trascendencia en lo que se refiere a la aplicación de las normas reguladoras de la protección de datos de carácter personal.

Así, en cuanto al tratamiento de los datos por parte de las Haciendas Locales, este se somete a los principios contenidos en los artículos 111 y 112 de la Ley General Tributaria, debiendo recordarse que, a tenor de lo establecido en el artículo 112.4 (introducido por la Disposición Adicional cuarta de la LOPD) "la cesión de aquellos datos de carácter personal, objeto de tratamiento que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones Públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal".

Del mismo modo, tampoco será necesario obtener el consentimiento del afectado para recabar del mismo cuanta información de trascendencia tributaria sea necesaria para el desempeño por la Hacienda Local de sus competencias en materia tributaria, dada la obligación de declarar impuesta al contribuyente o su sustituto por la Ley General Tributaria y las normas reguladoras de cada Impuesto. Este tratamiento, amparado por la Ley, se fundaría en la excepción contenida en el artículo 6.2 de la LOPD que permite el tratamiento de los datos por la Administración Pública en el ejercicio de sus competencias.

Por otra parte, y en relación con la cesión de datos por parte de las Haciendas Locales, serán de aplicación en este caso las previsiones contenidas en el artículo 113 de la Ley General Tributaria, cuyo apartado primero limita los supuestos de cesión a los que expresamente se enumeran en ese precepto, en relación con "los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones", limitando su utilización a la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada.

Del tenor de este precepto deben diferenciarse dos supuestos de cesión de datos por parte de las Haciendas Locales:

En caso de cesión a otras Administraciones Tributarias, esta cesión se encontraría amparada en todo caso en lo establecido en el artículo 113.1 b) de la Ley General Tributaria, cuando la cesión se ampare en el ejercicio por la cesionaria de sus competencias en materia tributaria.

En este mismo sentido, el artículo 8.1 de la LHL establece que "de conformidad con lo dispuesto en el artículo 106.3 de la Ley 7/1985, de 2 de abril, las Administraciones tributarias del Estado, de las Comunidades Autónomas y de las Entidades locales colaborarán en todos los órdenes de gestión, liquidación, inspección y recaudación de los tributos locales", aclarando el artículo 8.2 c) de la citada Ley que ambas Administraciones "se comunicarán inmediatamente, en la forma que reglamentariamente se establezca, los hechos con trascendencia tributaria para cualquiera de ellas, que se pongan de manifiesto como consecuencia de actuaciones comprobadoras e investigadoras de los respectivos servicios de inspección tributaria".

Por el contrario, si la cesión a otras Administraciones Públicas no tuviera fines tributarios, la cesión sólo podrá limitarse, estrictamente a los supuestos contenidos en el artículo 113.1, sin que los datos puedan ser utilizados por la Entidad Local para ninguna otra finalidad, dado que el citado artículo considera que dichos datos "sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada", lo que limita el alcance de la utilización de los datos a la gestión tributaria, pero nunca a la de otros ingresos de derecho público.

3.2.13.- Conservación de datos de facturación telefónica

Se ha solicitado de la Agencia que se indique el plazo durante el cual procederá la conservación de los datos de carácter personal derivados de la facturación del servicio telefónico, a las que se refiere en el artículo 65.2 del Regla-

mento que desarrolla el Título III de la Ley General de Telecomunicaciones, aprobado por Real Decreto 1736/1998, de 31 de julio.

Con carácter previo, debe indicarse que la conservación a que alude el artículo 65.2 del Reglamento se refiere a aquellos supuestos en que los datos son tratados exclusivamente "al objeto de realizar la facturación y los pagos de las interconexiones", no encontrándose incluidos en el citado plazo los supuestos en que los datos sean tratados, previo consentimiento del interesado, con la finalidad de promoción comercial, en los términos descritos en el artículo 65.3, en cuyo caso, el consentimiento "será válido hasta que los abonados lo dejen sin efecto de modo expreso", lo que supone que, mientras no exista dicha revocación, los datos podrán seguir siendo objeto de tratamiento.

Sentado lo anterior, esta Agencia de Protección de Datos coincide con el criterio sustentado por la Comisión del Mercado de las Telecomunicaciones, que considera que el período de impugnación de la factura será el de tres meses, que se desprende del artículo 61 del propio Reglamento. Del mismo modo, al no existir plazo especial al efecto, el derecho del operador a exigir el abono de la factura se regirá por lo dispuesto en el artículo 1966 del Código Civil, dado el vencimiento de los pagos, inferior a un año, siendo dicho plazo de cinco años.

Del análisis conjunto de ambos preceptos se desprende que, en caso de que haya sido abonada la factura, el operador deberá cesar en el tratamiento de los datos a los que se refiere el artículo 65.2 transcurrido el plazo de tres meses anteriormente indicado, encontrándose legitimado para persistir en el tratamiento exclusivamente en caso de impago y durante el plazo de cinco años que la Ley le concede para ejercitar las acciones conducentes al abono de la factura. Por último, si existieran litigios pendientes, derivados del ejercicio de acciones de impugnación de la factura o tendentes a lograr el cobro de las misma, los datos podrán conservarse durante la tramitación de los mismos, en tanto no recaiga resolución definitiva, si bien sólo podrán utilizarse a fines probatorios.

3.2.14.- Tratamiento de los datos de facturación telefónica

Se planteó por el titular de un Organo similar al Defensor del Pueblo en una determinada Comunidad Autónoma la licitud del escrito remitido por un operador de telecomunicaciones a sus abonados en que se advertía del tratamiento de los datos referentes a la facturación telefónica en caso de que no existiese oposición de los mismos en el plazo de un mes.

Dado que esta misma materia ha sido analizada en otro lugar de esta Memoria, debemos recordar simplemente que el artículo 65 del Reglamento de desarrollo del Título III de la Ley general de Telecomunicaciones prevé que estos datos sólo podrán ser tratados "con objeto de realizar la facturación y los pagos de las interconexiones", así como "para la promoción comercial de sus propios servicios de telecomunicaciones, siempre y cuando el abonado haya dado su consentimiento previo", añadiendo el artículo 69 que "los operadores deberán dirigirse a los abonados, al menos, con un mes de antelación al inicio de la promoción, requiriendo su consentimiento que, de producirse, será válido hasta que los abonados lo dejen sin efecto de modo expreso. Si en el plazo de un mes desde que el abonado reciba la solicitud, éste no se hubiese pronunciado al respecto, se entenderá que consiente".

Por ello, a nuestro parecer, la cláusula cumple con lo dispuesto en las normas anteriormente citadas, dado que pone de manifiesto la existencia de un tratamiento, cuyo responsable será la propia operadora, limitando sus finalidades a las dos que se indican en el artículo 65 del Real Decreto. En este sentido se prevé el tratamiento de los datos para la ejecución del contrato, en el párrafo primero, y para la realización de actividades de promoción comercial, en el párrafo segundo, concediéndose a los afectados la posibilidad de que los datos sean cedidos para esta última finalidad a terceras empresas en el párrafo tercero, en el que además se otorga un periodo de tiempo prudencial (un mes) para ejercer el derecho de oposición, en los términos que prevé la normativa vigente. Además la cláusula pone de manifiesto la posibilidad de revocar en cualquier momento el consentimiento. Del mismo modo se indican cuales serán los datos objeto de tratamiento y ante quien podrán ejercitarse los derechos de acceso, rectificación y cancelación, indicándose a tal efecto una dirección concreta.

No obstante, la consulta planteó que el cauce escogido por la propia operadora para poner esta circunstancia en conocimiento de sus abonados (su remisión junto con la factura telefónica) resultaba inadecuada, señalándose por esta Agencia que :

- En primer lugar, ni la Ley Orgánica 15/1999, ni el Real Decreto 1736/1998 vienen a establecer un procedimiento a través del cual debe recabarse el consentimiento, limitándose el Reglamento a establecer los requisitos que ya se han indicado, a diferencia de lo que señala en otros lugares (por ejemplo, en relación con la utilización del dispositivo de visualización de la línea llamante y su posible ocultación). Por ello, y sin perjuicio de que el procedimiento pueda no considerarse el más idóneo desde el punto de vista de la protección de los derechos de los ciudadanos, lo cierto es que no puede apreciarse vulneración alguna de los citados derechos, toda vez que se han adoptado las medidas que la Ley exige.

- En segundo término, y en lo que se refiere al modo en que se ha producido la notificación, la Ley no exige que la misma se haga en escrito separado ni con referencia especial a su contenido. Por otra parte, se considera que la remisión de la comunicación conjuntamente con la factura telefónica viene precisamente a aclarar a qué datos está haciendo referencia la misma, lo que facilita al interesado el conocimiento de los extremos respecto de los cuales está prestando el consentimiento con mayor claridad que si la comunicación se efectuara de forma separada. Ello se basa en que la factura telefónica desglosada contiene tanto los datos esenciales del contrato como todos aquellos a que se refiere el artículo 69 del Real Decreto 1736/1998. Además, el hecho de que la remisión se efectúe conjuntamente con la factura asegura que el interesado tendrá una mayor probabilidad de conocer su contenido, al quedar sumamente claro

que el envío no es meramente publicitario o de otra naturaleza.

- Por último, si bien podrían existir otros medios por los que el interesado pudiera ejercitar su derecho de oposición al tratamiento o, posteriormente, su derecho de cancelación, lo cierto es que no existe, como se ha venido indicando, previsión alguna que imponga a la compañía de telecomunicaciones la obligación de optar por uno u otro medio. Además el medio contenido en la comunicación tiene una importante ventaja respecto de otros, dado que asegura, en beneficio de ambas partes, la existencia de un documento que, en su caso, tendrá el valor probatorio suficiente para acreditar su remisión por parte del propio afectado o de la compañía.

En consecuencia, se indicó que el procedimiento empleado por la operadora resulta plenamente conforme con la normativa reguladora de la protección de datos de carácter personal.

3.2.15.- Responsable de los ficheros de las Comunidades de Propietarios

Se ha planteado por un determinado Colegio de Administradores de Fincas quien es el responsable de los ficheros que contengan los datos de los propietarios de las viviendas de un edificio objeto de división horizontal.

Tal y como establece el artículo 3 d) de la LOPD, se define como responsable del fichero a la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". Por ello, será necesario determinar quién, a criterio de esta Agencia, decide sobre la finalidad, objeto y uso de los datos, siendo fundamental resolver cuál es la finalidad a la que se encontrarían sujetos los ficheros que contuvieran los datos de los propietarios.

Pues bien, la finalidad de mantener los datos de los propietarios es, precisamente, asegurar el cumplimiento por los mismos de las obligaciones impuestas por la Ley de Propiedad Horizontal (en los términos previstos tras su reforma, operada por la Ley 8/1999, de 6 de abril), así como garantizar el adecuado ejercicio por los mismos de los derechos que les corresponden en la comunidad. En resumidas cuentas, la finalidad perseguida por el mantenimiento de estos ficheros será la de asegurar el correcto desenvolvimiento de la comunidad.

De lo antedicho se desprende que la condición de responsable del fichero recaerá sobre la propia Comunidad de Propietarios que es quien, a través de sus Órganos de Gobierno y, en su caso, de la Junta, resolverá sobre las cuestiones relacionadas con la misma, siendo así que, de lo establecido en el artículo 13 de la Ley se desprende que el Secretario y el Administrador, cuando actúen en el ejercicio de las funciones relacionadas con una determinada comunidad, no son sino órganos integrados en la misma, independientemente de la posibilidad de que una misma persona desempeñe funciones de secretario y/o administrador en varias Comunidades de propietarios. La misma solución se alcanza si se tiene en cuenta que le artículo 13.7 de la Ley, en su párrafo segundo, habilita a la Junta a remover a quienes desempeñen funciones en uno de sus órganos de gobierno, siendo potestad de la Junta nombrar y separar a los mismos (artículo 14.1).

En consecuencia, las actividades que el Administrador (o, en su caso, el Secretario) de una determinada comunidad de propietarios desarrolle como tal no serán sino las derivadas de su propia integración, como órgano de gobierno, en la citada comunidad, sin que el mismo pueda utilizar la información de que tenga conocimiento como consecuencia del ejercicio de su función para un fin distinto del derivado de la gestión que le haya sido encomendada, en el ámbito de las funciones que al administrador atribuye el artículo 20 de la Ley de Propiedad Horizontal.

Por ello, la condición de responsable de los ficheros creados para la adecuada gestión y funcionamiento de la comunidad de propietarios de un inmueble objeto de división horizontal corresponderá a la propia Comunidad, siendo el administrador, en cuanto tal y con relación a ese determinado inmueble, un mero usuario del fichero, en virtud de su condición de órgano de gobierno de la comunidad.

Además, se indicó que en caso de que dichos ficheros se encuentren ubicados en la oficina profesional del administrador, éste no será más que un mero encargado del tratamiento, que limitará (en cuanto oficina) su actividad a la custodia de los datos, siendo necesario el cumplimiento del artículo 12 de la LOPD, en los términos que ya se han indicado en esta memoria.

3.2.16..- Tratamiento por Abogados y Procuradores de los datos de las partes en un proceso

Se ha consultado si los abogados y procuradores habrán de recabar el consentimiento de sus clientes y de la contraparte de los mismos en procesos en que aquéllos les confieran su representación o defensa.

Como regla general, la inclusión de los datos de los clientes y sus oponentes en un fichero supondrá un tratamiento de datos de carácter personal, que requeriría, en principio, el consentimiento del afectado, con el deber de informar al mismo de los extremos contenidos en el artículo 5.1 o, en caso de no recabarse los datos del propio afectado, la obligación de informar a éste de dicha inclusión en el plazo de tres meses, tal y como dispone el artículo 5.4, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

En lo referente al tratamiento de los datos de los clientes, podrá efectuarse el mismo sin consentimiento del afectado, a tenor de lo establecido en el artículo 6.2 de la Ley Orgánica 15/199, que excluye del consentimiento los supuestos en que los datos "se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

Sin embargo, el problema se plantea en el supuesto de que los datos se refieran a los oponentes de los clientes del abogado o procurador, dado que en ese caso el tratamiento resulta absolutamente imprescindible para la asistencia letrada al cliente, si bien ese tratamiento pudiera chocar con el derecho a la protección de datos de la persona cuyos datos son objeto de tratamiento.

A nuestro juicio, en este caso surgiría una colisión entre dos derechos fundamentales: el derecho a la protección de datos de carácter personal, derivado del artículo 18 de la Constitución y consagrado como derecho autónomo e informador del texto constitucional por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, por un lado; y el derecho a la asistencia letrada, como manifestación del derecho de los ciudadanos a obtener la tutela judicial efectiva de los jueces y tribunales, contenido en el artículo 24.2 de la Constitución.

Para resolver esta cuestión, debe indicarse que, en primer lugar, la propia Ley Orgánica 15/1999 permite establecer los límites para la exigencia del consentimiento, dado que su artículo 6.1 exige, como regla general, el consentimiento para el tratamiento de los datos "salvo que la Ley disponga otra cosa".

A la vista de este precepto, el legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En este caso, como se dijo, el tratamiento por los abogados y procuradores de los datos referidos a la contraparte de sus clientes en los litigios en que aquéllos ejerzan la postulación procesal trae su causa, directamente, del derecho de todos los ciudadanos a la asistencia letrada, consagrado por el artículo 24.2 del Texto Constitucional.

En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de "los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Por todo ello, si bien ninguna disposición con rango de Ley establece expresamente la posibilidad del tratamiento por abogados y procuradores de los datos referidos al oponente de su cliente en el seno de un determinado proceso judicial, es evidente que dicha posibilidad trae causa directa de una norma de rango constitucional, reguladora además de uno de los derechos fundamentales y libertades públicas consagrados por la Constitución, y desarrollado por las leyes reguladoras de cada uno de los Órdenes Jurisdiccionales, en los preceptos referidos a la representación y defensa de las partes, por lo que existirá, desde el punto de vista de la Agencia, una habilitación legal para el tratamiento de los datos, que trae su cobertura del propio artículo 24 de la Constitución y sus normas de desarrollo.

Dicho esto, deberá analizarse si el abogado o procurador se encuentra obligado, por imperativo del artículo 5.4 de la Ley Orgánica, a informar a los oponentes de su cliente de la existencia de un fichero o tratamiento, su responsable, su finalidad, la posibilidad que los afectados ejerciten los derechos que la Ley les atribuye y los destinatarios de los datos, dada la concurrencia entre el derecho del cliente a obtener la adecuada asistencia de letrado y, en definitiva, a ver satisfecha la tutela judicial efectiva, consagrada por el artículo 24 de la Constitución, y del oponente a la protección de sus datos de carácter personal, lo que supondrá el cumplimiento del citado deber de información.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) "el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".

Pues bien, aplicando la doctrina antedicha al supuesto concreto, y sin perjuicio de lo que, en su caso, manifestare en el futuro el Tribunal Constitucional, procederá ponderar en qué caso la limitación del ejercicio de uno de los derechos en conflicto puede producir una mayor merma de los derechos de la otra parte o, en su caso, las medidas que permitirán mitigar ese potencial perjuicio.

Siguiendo esta premisa, en nuestra opinión debería darse una prevalencia al derecho consagrado por el artículo 24 de la Constitución, garantizando a su vez las medidas que evitarán un mayor perjuicio a los afectados (en este caso, los oponentes de los clientes cuyos datos son objeto de tratamiento).

Ello se funda en que la comunicación a los afectados de las informaciones de que los abogados o procuradores puedan disponer, procedentes de sus clientes, podrían perjudicar, como ya se indicó, el adecuado ejercicio por el propio interesado de las facultades vinculadas con su derecho a obtener la tutela efectiva de los Jueces y Tribunales (al quedar en conocimiento de la otra parte los datos que pudieran ser aportados a juicio en defensa de su derecho).

4. ANALISIS DE LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL

En este epígrafe se procederá al comentario de las Sentencias de nuestro Tribunal Constitucional que mayor incidencia han producido sobre la materia objeto de la actividad de esta Agencia de Protección de Datos.

A este respecto, debe ponerse de manifiesto la importante incidencia que sobre la normativa reguladora de la protección de datos de carácter personal han producido las Sentencias 290/2000 y 292/2000, ambas de 30 de noviembre, que vinieron a resolver los recursos de inconstitucionalidad planteados contra la LORTAD y la LOPD.

Junto con el análisis de dichas Sentencias, nos referiremos en el presente epígrafe a la Sentencia del Alto Tribunal 202/1999, publicada en el BOE de 16 de diciembre de 1999, referida al tratamiento de los datos relacionados con la salud de los trabajadores por parte del empresario.

4.1.- Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre.

La Sentencia resuelve el recurso de amparo interpuesto contra la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Cataluña, de 14 de octubre de 1996, desestimatoria del recurso de suplicación interpuesto contra Sentencia del Juzgado de lo Social núm. 22 de los de Barcelona, de 30 enero 1996, recaída en autos sobre vulneración de derechos fundamentales.

En cuanto a sus antecedentes, pueden resumirse de la siguiente forma: el actor, presidente del Comité de Empresa de la oficina principal de una entidad financiera, interpuso demanda contra la misma por vulneración de derechos fundamentales, en la que se señalaba que la entidad demandada, que ostenta la condición de colaboradora de la Seguridad Social, dispone de unos locales de empresa en los que se realizan las visitas de sus trabajadores a los facultativos de la Seguridad Social y donde están ubicados, asimismo, los servicios médicos de empresa, disponiendo asimismo de un sistema informático, con una sola base de datos, donde existen unos ficheros médicos en los que constan los resultados de las revisiones periódicas realizadas por los servicios médicos de la empresa y empresas médicas subcontratadas, así como los diagnósticos médicos de todas las bajas por incapacidad temporal de los trabajadores extendidas por los facultativos de la Seguridad Social. El fichero médico, que no se encuentra individualizado, no está dado de alta como tal en la Agencia de Protección de Datos y únicamente tienen acceso al mismo los referidos facultativos y un empleado del Banco, en su calidad de administrador único de informática, encuadrado funcionalmente en la Jefatura de Personal, Sección de Recursos Humanos, que es quien suministra a aquéllos la clave de paso.

El actor se dirigió por escrito a la entidad de crédito donde presta sus servicios, solicitando la cancelación de todos los datos relativos a su salud obrantes en los ficheros informáticos que posee el Banco. En respuesta a esta solicitud, el Director de los Servicios Médicos de Empresa remitió al interesado escrito, dándole cuenta de los datos médicos que al mismo atañían existentes en el fichero informatizado de utilización por el servicio, consistentes todos ellos en las bajas temporales causadas por el trabajador desde el 9 de abril de 1988 hasta el 1 de agosto de 1995, con las fechas de baja y alta y diagnóstico, tal y como figuran en los impresos oficiales del Instituto Catalán de la Salud.

Se considera por el recurrente vulnerado lo establecido en el artículo 18 de la Constitución, en conexión con lo establecido en la LORTAD, dado que los datos médicos, recogidos por la entidad empleadora para el ejercicio de la actividad de control del absentismo, conforme a lo previsto en el artículo 20.4 del Estatuto de los Trabajadores, lo fueron sin su consentimiento.

El Tribunal Constitucional señala, en primer término, y de forma que luego sería ratificada por la Sentencia 292/2000, que "la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada ®libertad informática¯ es así derecho a controlar el uso de los mismos datos insertos en un programa informático (®habeas data¯) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

Para resolver la cuestión planteada, la Sentencia aduce en su Fundamento Jurídico 5 que "lo verdaderamente relevante es que la medida adoptada por la empresa, sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, no reviste la consideración de solución idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral, pues no se trata de medida de suyo ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad".

Ello se funda en que el mantenimiento del fichero "no se dirige a la preservación de la salud de los trabajadores sino al control del absentismo laboral, lo que, por otra parte, resulta plenamente acorde con la denominación ®absentismo con baja médica¯ que recibe el fichero. Consecuentemente, la creación y actualización del fichero, en los términos en que se ha llevado a efecto, no puede ampararse, frente a lo sostenido por la empresa, en la existencia de un interés general (art. 7.3 LORTAD y, por remisión, arts. 10.11 y 61 LGS), que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento automatizado de los datos atinentes a su salud, ni tampoco en lo dispuesto en los arts. 22 y 23 de la Ley de Prevención de Riesgos Laborales, habida cuenta de que en el fichero en cuestión no se reflejan los resultados arrojados por la vigilancia periódica -y consentida por los afectados- del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral, sino tan sólo la relación de períodos de suspensión de la relación jurídico-laboral dimanantes de una situación de incapacidad del trabajador".

En consecuencia, al existir un tratamiento desproporcionado de los datos de carácter personal relacionados con la salud, que no puede traer causa de las excepciones contenidas en el artículo 7.3 de la LORTAD (hoy de la LOPD), dicho tratamiento resulta contrario a derecho, concediendo el Tribunal el amparo solicitado.

4.2.- Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre.

Esta Sentencia resuelve los distintos recursos de inconstitucionalidad en su día planteados contra la Ley Orgánica 5/1992. Así, la Sentencia se refiere a los recursos formulados por el Consejo Ejecutivo de la Generalidad de Cataluña, el Parlamento de Cataluña, el Defensor del Pueblo y 56 Diputados.

Tal y como se indica en la Sentencia, son objeto de la misma los artículos 6.2, 19.1, 20.3, 22.1, 22.2, 24, 31,30.1,30.2, 40.1, 40.2, y la Disposición Final tercera de la Ley. Asimismo se recuerda que los recursos acumulados se refieren, en unos casos, a normas de carácter sustantivo, derogadas al tiempo de dictarse la Sentencia por la LOPD, y, por otra, a normas que pudieran afectar la atribución de competencias entre el Estado y las Comunidades Autónomas. Por ello, la Sentencia analiza separadamente unas y otras.

En relación con las normas sustantivas, la Sentencia, en su Fundamento Jurídico 3, recuerda que "en aquellos casos en los que los preceptos objeto de un recurso de inconstitucionalidad fueron impugnados por motivos distintos de los referidos al orden de reparto competencial entre el Estado y las Comunidades Autónomas, la regla general es que su derogación al tiempo de resolver dicho recurso produce la extinción del mismo, por pérdida sobrevenida de su objeto. Con la reserva, claro es, de que un determinado precepto, pese a su derogación, pudiera continuar proyectando sus efectos sobre situaciones posteriores a ese momento si así se desprende con toda evidencia de los términos en los que tal derogación se ha producido por la ley posterior".

A la vista de tal argumentación, y tomando en cuenta el Tribunal que "del examen de la Disposición derogatoria LOPD. en relación con los preceptos impugnados no cabe llegar a la conclusión de que éstos, tras su derogación por dicha Ley, hayan de continuar produciendo efectos respecto a situaciones posteriores" la Sentencia señala que procede estimar la pérdida sobrevenida de objeto en cuanto a los recursos de inconstitucionalidad fundados en aspectos sustantivos de la Ley. Del mismo modo el Tribunal resolvió no entrar en el análisis de lo establecido en aquéllas normas de la LORTAD reproducidas por la nueva LOPD y que habían sido objeto de recurso por parte del Defensor del Pueblo, dado que las mismas serían analizadas, resolviéndose la constitucionalidad o inconstitucionalidad de las mismas en la Sentencia que recayera sobre el citado recurso.

Dicho esto, el Tribunal centra su análisis en el estudio de las normas referidas a la existencia o inexistencia de una infracción del reparto competencial establecido en nuestra Constitución. Así, el Tribunal Constitucional razona que "cabe apreciar, en primer lugar, una identidad sustancial de contenidos respecto al art. 24 LORTAD y el que le ha sucedido en el tiempo (art. 26 LOPD), salvo ciertas precisiones en su apartado 2. Y otro tanto cabe decir, en segundo término respecto a los arts. 31 y 40.1 y 2 LORTAD respecto de los correspondientes de la Ley posterior (arts. 32 y 41 LOPD)", sin entrar a conocer del recurso interpuesto contra el artículo 39 de la LORTAD, por la novedad introducida en el artículo 40 de la LOPD, que sustituye la referencia a la Agencia de Protección de Datos por una referencia genérica a "las autoridades de control". En consecuencia, la Sentencia analiza exclusivamente las tachas de inconstitucionalidad que, desde la perspectiva del orden constitucional de distribución de competencias entre el Estado y las Comunidades Autónomas, se han dirigido contra los artículos 24, 31 y 40.1 y 2 LORTAD.

En cuanto a este análisis, el fundamento jurídico 7 de la Sentencia considera necesario "que el examen de la presente disputa competencial se lleve a cabo partiendo de dos presupuestos, a saber: el contenido del derecho fundamental a la protección de datos personales y, en segundo término, los rasgos generales que caracterizan a la Agencia de Protección de Datos dado que la función general de este órgano es la de "velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación", como se expresa en el primer inciso del apartado a) del art. 36 LORTAD".

En el análisis de la primera de las cuestiones, el Tribunal Constitucional recuerda que el derecho consagrado en el artículo 18.4 de la Constitución "es, además, en sí mismo, "un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama la informática". Este derecho fundamental comprende, según indica el Tribunal un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos, de suerte que "es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes".

Por otra parte, y en relación con la segunda de las cuestiones apuntadas, el fundamento jurídico 8 de la Sentencia señala que "en lo que respecta a las funciones y potestades atribuidas a la Agencia Protección Datos, el apartado a) del art. 36 LORTAD ofrece una caracterización general de las primeras al encomendar a la Agencia la función general de "Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación de datos". Y en cuanto especificación de esta función de carácter tuitivo en orden a la protección de datos personales, los restantes apartados del citado precepto le atribuyen tanto funciones de intervención o control respecto a ciertos sujetos y actividades como funciones registrales y consultivas". Asimismo, en correspondencia con el carácter público de sus funciones, la Agencia de Protección de Datos dispone de potestades administrativas expresamente atribuidas por dicha Ley, tales como la de investigación o de inspección, la sancionadora, la de resolución de las reclamaciones de los afectados por incumplimiento de las previsiones de dicha Ley y la normativa, ceñida en lo esencial a dictar las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la LORTAD.

En consecuencia, se señala que "existe una correspondencia entre las funciones y potestades que la LORTAD ha atribuido a la Agencia de Protección de Datos y el carácter preventivo de sus actuaciones. Pues es este carácter tuitivo

o preventivo el que, en última instancia, justifica la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática con la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada".

Se alegaba por las Comunidades Autónomas "que las actividades relativas a los ficheros automatizados de carácter personal no son en sí mismas el objeto de una materia competencial, sino que constituyen una actividad instrumental al servicio de otras actividades encuadrables dentro de otras materias sobre las que las comunidades Autónomas pueden ostentar títulos competenciales según el orden constitucional de reparto de competencias". Sin embargo, el Tribunal Constitucional considera que tal argumento no resulta admisible por cuanto, con su planteamiento "se está desvirtuando cuál es el bien jurídico constitucionalmente revelante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales de los ciudadanos o afecta al pleno ejercicio de sus derechos, como claramente se desprende del tenor de dicho precepto constitucional".

Por último, en cuanto a la concurrencia en este caso de un título competencial habilitante para el ejercicio de las competencias derivadas de la LORTAD por la Agencia de Protección de Datos, la Sentencia recuerda, en su fundamento jurídico 14, que "la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10.1 C.E.), tengan una proyección directa sobre el reparto competencial entre el Estado y las comunidades Autónomas ex art. 149. 1.1 C.E. para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales".

"A este fin -prosigue la Sentencia- la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros".

En consecuencia, concluye la Sentencia, "es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el presente caso justifica que la Agencia de Protección de Datos puede ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada", por lo que las normas discutidas son consideradas por el Alto Tribunal como conformes a la Constitución.

4.3.- Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

El Tribunal Constitucional, en Sentencia de 30 de noviembre de 2000, estima el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999. Pese a que la Sentencia sólo resuelve sobre la inconstitucionalidad de estos preceptos, resulta sumamente importante en materia de protección de datos, dado que su fundamentación jurídica, siguiendo la línea ya mantenida por el Alto Tribunal, viene a reconocer tajantemente el derecho fundamental a la protección de datos de carácter personal. Por otra parte, la citada Sentencia, al estimar el recurso, no sólo declara la inconstitucionalidad de los citados preceptos sino también la nulidad de los mismos

Los fundamentos jurídicos 6 y 7 de la Sentencia vienen íntegramente dedicados a la definición y configuración del derecho a la protección de datos personales. Se señala al respecto por el Tribunal que "el derecho fundamental a la protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" (Fundamento Jurídico 6). Más adelante y en el mismo Fundamento Jurídico se establece que "el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal".

La propia Sentencia indica que "el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros ... Dicha peculiaridad radica en su contenido, ya que ... el derecho a la protección de datos atribuye a su titular un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos ... y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva el poder de disposición sobre los datos personales" (Fundamento Jurídico 6).

El Fundamento Jurídico 7 viene a remarcar el contenido del derecho fundamental a la protección de datos y las facultades que proporciona al individuo tanto frente al Estado como ante un particular.

Así, se señala que "de todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos."

De la anterior doctrina viene pues a deducirse que el Tribunal Constitucional ha venido a configurar, sin ningún tipo de duda, el derecho a la protección de datos como un derecho fundamental autónomo, desarrollando hasta sus últimas consecuencias la doctrina iniciada por el propio Tribunal en su Sentencia 254/1993. Este derecho fundamental no reduce su protección a los datos íntimos, sino que su objeto de protección es cualquier tipo de dato personal, traspasando su objeto la intimidad personal y viniendo constituido su contenido por un haz de facultades consistentes en diversos poderes que imponen a terceros deberes tales como requerir el consentimiento para la recogida y uso de los datos personales, ser informado sobre el destino y poder acceder, rectificar y cancelar los propios datos. En definitiva el contenido del derecho a la protección de datos personales que reconoce el Tribunal Constitucional viene a coincidir con los principios y derechos que establece la Ley Orgánica 15/1999, consistiendo este derecho, en resumen, en un poder de disposición y control sobre los datos personales, tanto frente al Estado como ante cualquier particular.

Entrando ya en las cuestiones sometidas expresamente al parecer del Tribunal Constitucional, se declara, como se indicó, la inconstitucionalidad de determinados incisos de los artículos 21 y 24 de la Ley Orgánica 15/1999.

En cuanto al primero de los mismos, el artículo 21.1 de la Ley Orgánica, en similares términos a los previstos en el artículo 19.1 de la LORTAD, venía a posibilitar la cesión de datos entre Administraciones Públicas, sin consentimiento del afectado, cuando la misma se fundase en el ejercicio de competencias que versen sobre materias distintas, "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por otra disposición de superior rango que regule su uso".

El Tribunal Constitucional considera que las citadas previsiones vulneran el principio de reserva de Ley que impone el artículo 53.1 de la Constitución, así como la necesidad de señalar la justificación y proporcionalidad de cualquier limitación a un derecho fundamental, como es el caso del derecho a la protección de datos personales. Por ello declara contrario a la Constitución y en consecuencia nulo el citado inciso del artículo 21 LPD.

También se declaran contrarias a la Constitución y nulas algunas excepciones a los derechos de los afectados, contempladas por el artículo 24 de la Ley Orgánica 15/1999, de forma similar a la que ya preveía el artículo 22 LORTAD. Así este precepto permitía al responsable del fichero que fuera Administración Pública no informar a los afectados, en los términos del artículo 5.1 y 2, "cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas" o "cuando afecte a infracciones administrativas".

En relación con este precepto el Tribunal Constitucional recuerda que las posibles limitaciones al derecho fundamental no sólo precisan de su fundamentación en una previsión legal que tenga justificación constitucional, sino que la Ley que restrinja el derecho a la intimidad debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. Respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional a su restricción no puede estar basada simplemente en la actividad de la Administración Pública ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites.

5. ANÁLISIS DE LAS PRINCIPALES SENTENCIAS DE LA JURISDICCIÓN CONTENCIOSO-ADMINISTRATIVA

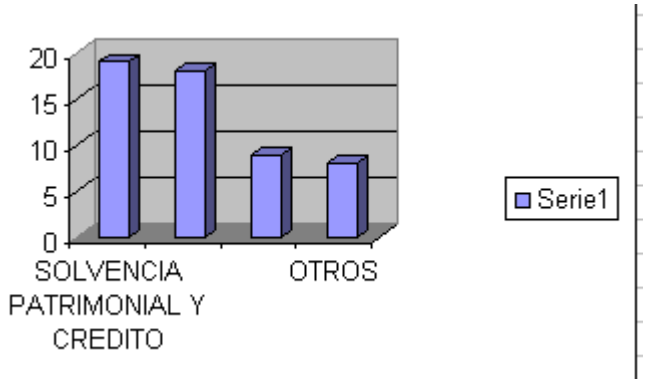
Según dispone el artículo 48.2 de la LOPD, que reproduce lo que ya establecía el artículo 48.2 de la derogada LORTAD, las resoluciones del Director de la Agencia de Protección de Datos ponen fin a la vía administrativa., Por ello, y sin perjuicio de la eventual interposición del recurso potestativo de reposición (al que se refiere el artículo 116 Ley 30/1992), dichas resoluciones sólo serán susceptibles de impugnación en vía contencioso-administrativa.

En este orden jurisdiccional, los órganos fiscalizadores competentes durante el año 2000 han sido las Salas de lo Contencioso-administrativo tanto de los Tribunales Superiores de Justicia como de la Audiencia Nacional, tomando en cuenta que el recurso hubiera sido interpuesto, respectivamente, antes de la entrada en vigor de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-administrativa, que atribuyó a la Audiencia Nacional la competencia anteriormente radicada en los tribunales Superiores de Justicia.

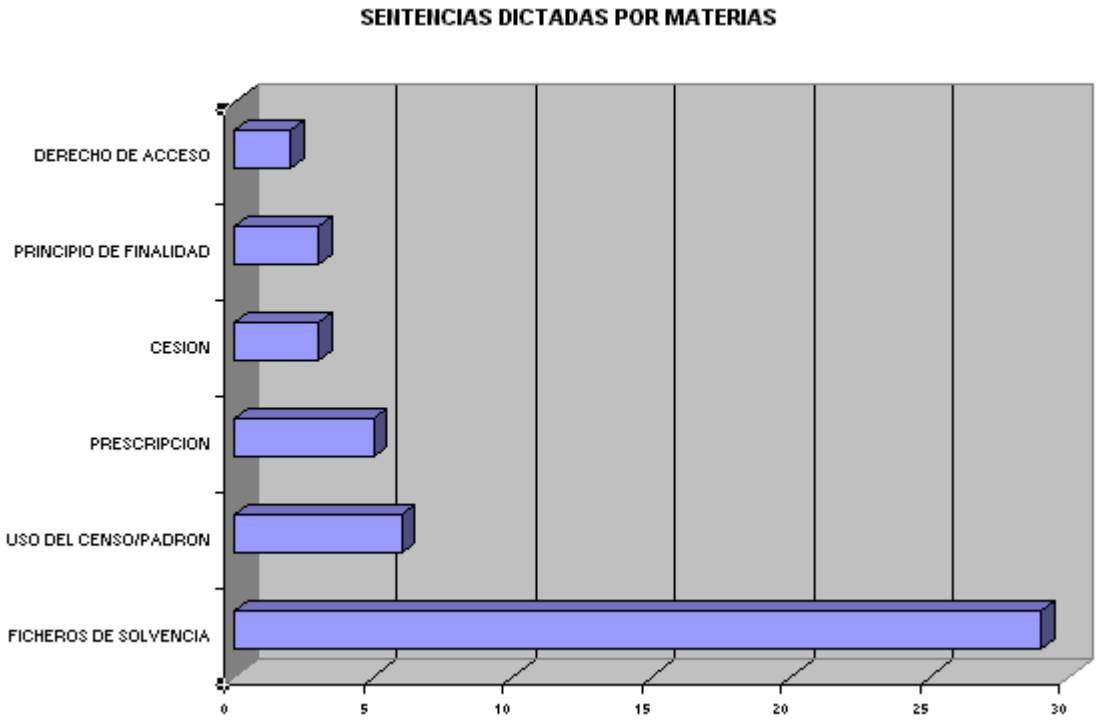
Pues bien, durante el año 2000 han recaído 54 sentencias que han resuelto otros tantos recursos contencioso-administrativos interpuestos contra resoluciones de la APD, habiendo sido 37 de las mismas dictadas por la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid, 16 por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional y una por la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Cataluña.

Esta cifra supone un notable incremento, del 86 %, respecto de las sentencias dictadas por esos mismos órganos jurisdiccionales en el ejercicio anterior, como lógica consecuencia de la mayor actividad de la Agencia al haber aumentado el número de resoluciones dictadas por la misma.

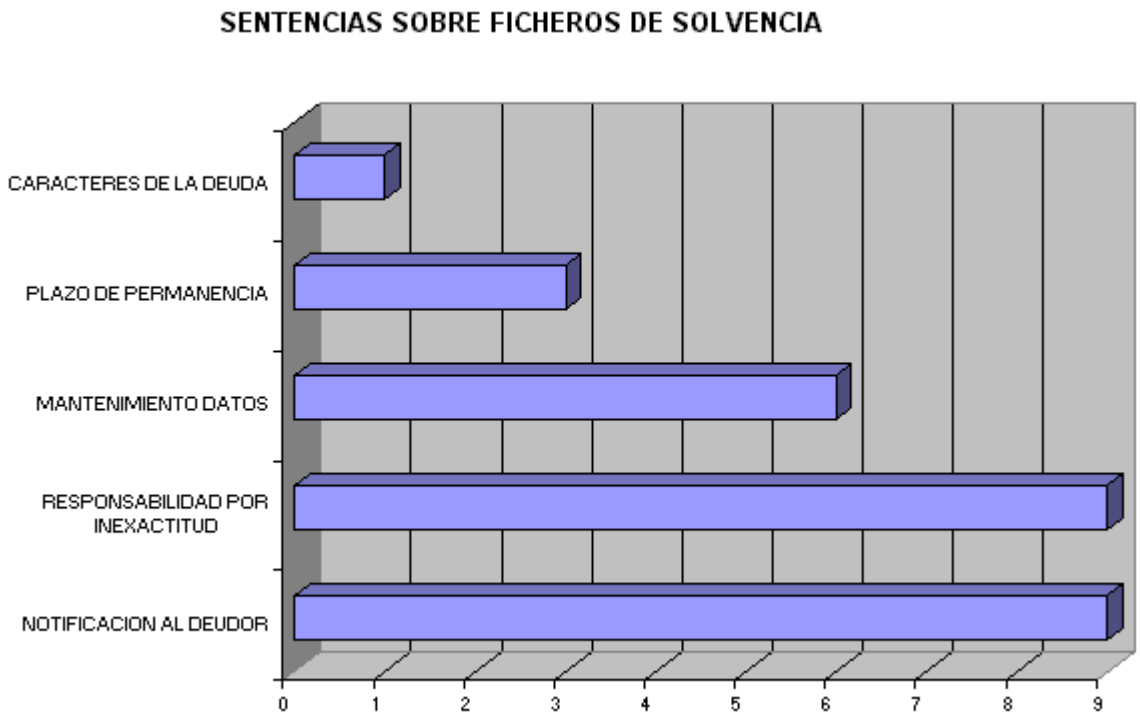
Del total de sentencias recaídas, atendiendo al sector al que pertenece la entidad recurrente, se desprende la siguiente estadística:



Por último, en cuanto a las cuestiones objeto de la litis, el siguiente gráfico refleja las mismas:



Como puede comprobarse, una amplia mayoría de las sentencias se refiere a la aplicación del artículo 28 de la LORTAD (hoy reemplazado por el artículo 29 de la LOPD). El siguiente gráfico desglosa las cuestiones más relevantes planteadas en relación con los ficheros de solvencia patrimonial y crédito:



A continuación se comentará el contenido de las citadas resoluciones, haciendo hincapié en aquéllas que revisten una mayor relevancia, bien por lo frecuente de su planteamiento, bien por la importancia de la doctrina sentada en las sentencias. Debe indicarse, como cuestión esencial, que la totalidad de las sentencias se refieren a cuestiones resueltas por la Agencia con base en las disposiciones de la derogada LORTAD, razón por la cual las referencias a la vigente LOPD se efectúan en las sentencias por razones esencialmente interpretativas o por aplicación del principio de retroactividad de las disposiciones sancionadoras más favorables.

5.1.- Cuestiones relacionadas con los ficheros de solvencia patrimonial y crédito.

5.1.1.- Obligación de notificación al deudor de su inclusión en el fichero.

Nueve de las sentencias dictadas a lo largo del año 2000 resolvieron recursos planteados contra resoluciones de esta Agencia por las que se imponía a la recurrente una sanción derivada del incumplimiento por parte del responsable del fichero común de solvencia de notificar al afectado su inclusión en un fichero, tal y como dispone el artículo 28.1 in fine de la LORTAD. No planteando problemas los supuestos en que el fichero contiene datos referidos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor, el mayor problema, en el que se han observado criterios discrepantes en las sentencias dictadas, se refiere a si dicha obligación procede, en todo caso, en los ficheros comerciales de evaluación de solvencia patrimonial y crédito, fundamentalmente en los supuestos en que los datos hayan sido recabados de fuentes accesibles al público.

En la Memoria correspondiente al año 1999 ya se dio cuenta de la existencia de estas divergencias, aclarándose la postura sostenida por esta Agencia y su fundamentación jurídica. La discrepancia entonces anunciada entre las Secciones Octava y Novena de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid ha persistido durante el año 2000.

Así, la Sección 8¦ del Tribunal Superior de Justicia de Madrid ha declarado, en dos ocasiones, la no obligatoriedad del responsable del fichero de notificar al afectado su inclusión en un fichero de solvencia patrimonial y crédito cuando sus datos han sido obtenidos de fuentes accesibles al público (Sentencias de 29 de marzo de y 30 de mayo de 2000).

Por su parte, la Sección Novena del mismo Tribunal destaca que la obligación de notificar la inclusión en un fichero sobre solvencia, aun cuando se trate de datos provenientes de fuentes accesibles al público, constituye una obligación legal, por imponerlo así el art. 28 de la Ley Orgánica 5/1992. Según el Tribunal, de acuerdo con la Ley, hay que notificar a los afectados una relación de los datos de carácter personal que se hubieren incluido en los ficheros automatizados, tanto si los ficheros son de prestación de servicios sobre solvencia patrimonial y crédito, como si son relativos al cumplimiento o incumplimiento de obligaciones dinerarias (Sentencias de 9 de febrero, 22 de febrero y 10 de marzo de 2000).

Por último, la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 29 de septiembre de 2000 considera no haber lugar a la notificación en el caso de los ficheros que no se refieran al cumplimiento o incumplimiento de obligaciones dinerarias, tomando como referente interpretativo el texto del nuevo artículo 29 de la LOPD (pese a que los hechos habían acaecido antes de su entrada en vigor y bajo la vigencia de la antigua LORTAD), que diferencia en sus dos primeros apartado ambos tipos de ficheros, reservando el deber de notificación al regulado por el apartado segundo de la misma exclusivamente.

5.1.2.- Responsabilidad por la inexactitud de los datos introducidos en los ficheros comunes de morosidad.

A lo largo de un total de ocho sentencias, se ha consolidado la doctrina de las Salas de lo Contencioso-Administrativo de considerar que la responsabilidad por la inclusión de un dato inexacto en los ficheros comunes referidos al cumplimiento o incumplimiento de obligaciones dinerarias recae sobre la entidad asociada que facilita el dato al fichero. Así, se han desestimado los recursos interpuestos contra resoluciones que sancionaban a las entidades asociadas, estimándose, por el contrario, los interpuestos por las responsables de los ficheros comunes cuando las mismas habían sido sancionadas.

En este sentido, cabe destacar la sentencia de 4 de mayo de 2000, dictada por la Sección Octava de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid, por la que se estima el recurso interpuesto por la responsable de un fichero común de solvencia, en que se indica que la entidad recurrente, si bien se encuentra obligada a efectuar la notificación a que se refiere el inciso final del artículo 28.1 de la LORTAD, no puede ser responsable de una infracción predicable exclusivamente de la entidad asociada, dado que la Instrucción 1/1995 impone a la entidad acreedora la obligación referente a "la comunicación del dato inexistente o inexacto, con el fin de obtener su cancelación".

Este criterio ha sido sustentado asimismo por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, en Sentencia de 3 de marzo de 2000, en que se desestima el recurso interpuesto por una entidad bancaria, sancionada por la inclusión de un dato inexacto en un fichero de solvencia patrimonial y crédito.

5.1.3 Mantenimiento de datos inexactos en los ficheros.

El criterio sustentado por las Salas de lo Contencioso-Administrativo en este punto es el de considerar que el tipo contenido en el artículo 42.3 f) de la antigua LORTAD será de aplicación cuando se dé uno de los siguientes supuestos

* Cuando instada la rectificación y cancelación de un dato inexacto, no se proceda a la actualización de los datos.

* Cuando conociéndose la inexactitud del dato, no se proceda a su corrección y ello pese a no haberse ejercitado el derecho de rectificación y cancelación, pues conforme se infiere del apartado 4.4 de la Instrucción 1/1995, los datos inexactos "serán cancelados y sustituidos de oficio".

En consecuencia, cuando exista ejercicio del derecho o concurran motivos racionales para entender que la responsable del fichero o la entidad acreedora podían conocer de la inexactitud del dato, la omisión de la cancelación del mismo será constitutiva de infracción de la LORTAD.

5.1.4 Otras cuestiones relacionadas con estos ficheros.

El criterio de la Agencia, consolidado a lo largo de sus resoluciones, ha sido ratificado por los Tribunales, al resolver los recursos interpuestos contra las mismas, en lo relativo al momento a partir del cual debe computarse el plazo de permanencia de los datos en los ficheros de solvencia patrimonial y crédito, cuando estos sean perjudiciales para los afectados.

En este sentido la Sentencia de la Audiencia Nacional de 3 de marzo de 2000, tras indicar que la permanencia indefinida del dato en el fichero podría perjudicar a los ciudadanos, "al constituir de facto una limitación importante a su capacidad económica en los mercados de crédito con clara vulneración de sus derechos fundamentales", indica que el dies a quo del mencionado plazo "no podrá ser otro que el día del vencimiento de la obligación impagada".

También el criterio de la Agencia se ha ratificado en lo referente a los requisitos exigibles a la deuda para que la misma pueda ser incluida en el fichero de morosidad, siguiendo en este punto lo establecido en la Instrucción 1/1995. Así, junto con la Sentencia de la Audiencia Nacional citada, cabe hacer referencia a la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid de 18 de octubre de 2000.

5.2. Cuestiones relacionadas con los ficheros para actividades de publicidad y prospección

5.2.1. Cumplimiento del principio de finalidad

A lo largo del año 2000 han sido reiteradas las Sentencias que han confirmado el criterio de la Agencia de Protección de Datos al resolver procedimientos sancionadores en que una determinada entidad fue sancionada por la utilización de los datos que le habían sido suministrados por los afectados para la realización de una determinada actividad y fueron posteriormente utilizados por la misma para la realización de actividades de publicidad y prospección.

En relación con estos supuestos, siguiendo el criterio de las resoluciones recurridas, la Sala ha considerado que la utilización de los datos para esta finalidad resulta contraria a lo establecido en el artículo 4.2 de la antigua LORTAD

(reproducido hoy por el artículo 4.2 de la LOPD), aclarando que cuando los datos hayan sido suministrados a los solos efectos de dar cumplimiento a una finalidad concreta, no procederá el tratamiento para una finalidad distinta, considerándose así mismo que la actividad de publicidad y prospección no es compatible con esa finalidad principal a menos que se haya recabado el consentimiento del afectado.(Así, Sentencia de la Sección Novena de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid de 25 de enero de 2000 y Sentencias de la Sección Octava de la misma Sala de 15 de noviembre y 7 de diciembre del mismo año).

5.2.2. Utilización de los datos del censo electoral

Siguiendo el criterio reiteradamente sostenido por las Salas, durante el año 2000 aquéllas se han vuelto a pronunciar en el sentido de considerar que los datos contenidos en el censo electoral no se encuentran incorporados a una fuente accesible al público, siendo ilícita su recogida para fines de publicidad y prospección. En relación con esta cuestión, cabe reiterar lo ya señalado en las memorias de esta Agencia correspondientes a los años 1998 y 1999.

En este sentido, deben traerse a colación las Sentencias dictadas por la Sección Octava de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid de 12 de enero, 1 de marzo y 29 de marzo de 2000 y la Sentencia de la Sección Novena de esa misma Sala de 18 de diciembre de 2000.

5.3.Otras cuestiones de interés

5.3.1. Falta de legitimación del denunciante para la interposición del recurso contra resoluciones de archivo.

Una de las Sentencias dictadas a lo largo del año 2000 (concretamente la Sentencia de la Sección Novena de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid de 29 de junio de 2000) inadmitía el recurso interpuesto. Dicha inadmisión fue fundada en la consideración de que el denunciante carecía de legitimación para la interposición del recurso contencioso-administrativo contra una resolución de archivo de la Agencia de Protección de Datos, al no concurrir en el mismo el criterio esencial para dicha legitimación, cual es la existencia de un interés legítimo.

En este sentido, la citada Sentencia recuerda que la imposición de una sanción a una tercera entidad "no produce ningún beneficio en la esfera jurídica de la denunciante ni aún partiendo que la declaración de responsabilidad administrativa pudiera facilitar una declaración judicial de responsabilidad civil", con expresa referencia a la doctrina sentada por el Tribunal Supremo en su Sentencia de 2 de marzo de 1999.

5.3.2. Cesión de los datos del Padrón Municipal.

La Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de noviembre de 2000 confirmó la sanción impuesta por esta Agencia de Protección de Datos a un determinado Ayuntamiento por la cesión a una entidad privada de los datos contenidos en el Padrón Municipal de Habitantes, siendo posteriormente aportados a un proceso seguido ante un Juzgado de Primera Instancia e Instrucción.

En primer lugar, y tomando en cuenta lo establecido en el artículo 16.3 de la Ley Reguladora de las Bases del Régimen Local del que ya se ha hecho cita en otros lugares de esta memoria la Sala como ya indicó la resolución recurrida, estima que los datos del Padrón son confidenciales y, en consecuencia, será necesaria para la cesión de los mismos la concurrencia del consentimiento de los vecinos.

Por otra parte, se indicó que el hecho de que los datos fuesen posteriormente aportados a un proceso judicial no permitía amparar la cesión en la excepción prevista por el artículo 11.2 aplicable a la cesión de los datos a los jueces y fiscales, toda vez que "en caso contrario bastaría alegar por cualquier persona que el destinatario último de la certificación es cualquiera de los sujetos indicados en el artículo 11.2.d) para obtener el dato. Interpretación que resulta absurda".

Por último, y frente a la alegación que consideraba potestativa la potestad sancionadora atribuida al Director de la Agencia sobre los ficheros de titularidad pública por el artículo 45.2 de la LORTAD, la Sala desestima esta consideración en todos sus términos, considerando que tal facultad no puede ser considerada como una atribución que el Director de la Agencia pueda adoptar libremente.

Además, es de destacar que la Sala, siguiendo el criterio de la temeridad, impuso a la Corporación recurrente las costas del proceso.

5.3.3. Cesión de datos entre entidades del mismo grupo.

El criterio de la Agencia de Protección de Datos, que considera que la transmisión de datos entre empresas de un mismo grupo es constitutiva de un supuesto de cesión que, en consecuencia, requiere el consentimiento del afectado o la habilitación legal para la misma, ha sido ratificado por la Sentencia de la Sección Novena de la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia de Madrid, de 16 de octubre de 2000, en la que literalmente se señala que "cualquier empresa es libre de constituirse en cualquiera de las formas societarias que el Derecho Mercantil regula. Asimismo, las empresas que pueden unirse a través de las distintas formas reguladas en derecho: fusión, absorción, sociedades anónimas y, como tales, independientes y con personalidad jurídica autónoma y que por el hecho de que la una sea propiedad de la otra, el particular que contrata con la primera pueda verse perjudicado, precisamente, por la estructura empresarial que la sociedad ha elegido. Si la recurrente ha preferido constituir dos sociedades y trabajar con ellas de manera independiente, beneficiándose así del mantenimiento de dos personas jurí-

dicas distintas, no puede, al mismo tiempo, pretender justificar el conocimiento por parte de la matriz de los datos que le constan a la filial por las operaciones en que esta última ha intervenido pues ello supone olvidarse de que se trata de personas jurídicas distintas. Por otro lado, si el particular contrata con la filial, es a esta sociedad a la que, voluntariamente, se le comunican los datos que, en consecuencia, la filial no puede comunicar a la sociedad matriz en perjuicio del particular".

5.3.4 Límites legales a la prestación de servicios de tratamiento automatizado de datos de carácter personal.

Por su trascendencia, teniendo en cuenta la incidencia que la figura del encargado del tratamiento ha comenzado a revestir a partir de la entrada en vigor de la LOPD, debe también procederse en este punto a comentar la Sentencia de la Audiencia Nacional de 14 de abril de 2000, desestimatoria del recurso interpuesto contra resolución sancionadora de esta Agencia.

En este caso, una persona denunció la recepción de un catálogo publicitario de una determinada entidad, resultando que sus datos habían sido obtenidos por dicha entidad en virtud de una cesión efectuada por otra que, según se alegaba, ostentaba la condición de encargado del tratamiento de otra tercera a la que el afectado había facilitado sus datos con ocasión de la adquisición de un determinado producto.

La sentencia declara que existe en este caso una cesión de datos de carácter personal, sin que pueda considerarse que la misma se encontraría amparada por la mera existencia de un contrato de prestación de servicios de tratamiento automatizado de datos de carácter personal, regulado por el artículo 27 de la LORTAD, toda vez que es esencia de dicho contrato que "la utilización no podrá realizarse con fines distintos a los que figuren en el contrato de servicios", del mismo modo que el encargado del tratamiento no podrá en ningún caso ceder los datos, ni siquiera para su conservación a terceras personas.

Por ello, sólo podrán ampararse en el artículo 27 aquellas relaciones que supongan la realización de una determinada actividad "exclusivamente a favor de la persona contratante del servicio", no amparando, en modo alguno, "bajo una u otra forma la cesión a terceros sin el consentimiento del afectado".

5.3.5. Ficheros de los profesionales de la medicina.

Debe, por último, hacerse una referencia, siquiera somera al contenido de la Sentencia de la Sección Octava de la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia de Madrid, de 12 de julio de 2000, que estima el recurso contencioso-administrativo interpuesto por un profesional de la medicina contra resolución de esta Agencia en que se le imponía una sanción de carácter grave por obstrucción de la actividad inspectora.

La Sentencia se funda para estimar el recurso, con base en lo establecido en la derogada LORTAD, en el hecho de considerar que en este supuesto los datos se encuentran incorporados a un fichero mantenido por personas físicas con fines exclusivamente personales (artículo 2.2 b de la LORTAD), relacionando la cuestión con el deber de secreto del profesional de la medicina.

Se plantea así por la Sentencia una interesante novedad en materia de protección de datos, que deberá ser abordada a la luz de las disposiciones incorporadas por la vigente LOPD.

A juicio de esta Agencia, las previsiones constitucionales sobre el secreto profesional deberán compatibilizarse con las relativas a la protección de datos de carácter personal, derivadas también de la Norma Fundamental. Esta compatibilidad deberá permitir el acceso a los datos del propio denunciante que admite el acceso a la información que le afecte, limitar los accesos a información sensible de terceros no afectados y, con carácter general, posibilitar la comprobación del cumplimiento de los principios de protección de datos y de tutela de los derechos reconocidos por la propia LOPD.

6. COMPARECENCIAS PARLAMENTARIAS DEL DIRECTOR

En el año 2000 el Director de la Agencia de Protección de Datos ha comparecido en dos ocasiones ante la Comisión Constitucional del Congreso de los Diputados para informar sobre la Memoria Anual de la Entidad así como para abordar los temas más candentes relacionados con la Agencia, suscitados por los propios Grupos Parlamentarios.

La primer comparecencia tuvo lugar el 20 de septiembre de 2000, a escasos meses del inicio de la legislatura, posibilitando que, desde los primeros momentos del comienzo de la actividad parlamentaria, se sometiera la actividad de la Agencia al control parlamentario.

La intervención del Director se refirió, en primer lugar, al informe sobre la Memoria de la Agencia correspondiente al año 1999.

A continuación los Portavoces de los Grupos Parlamentarios manifestaron su valoración sobre la actividad de la Agencia y destacaron los aspectos que, a su juicio, resultaban más relevantes respecto de la protección de datos carácter personal.

Con carácter general, los Grupos Parlamentarios valoraron positivamente la actuación de la Agencia remarcando los problemas derivados del incremento de actividad producido en la misma, y de la falta de adecuación de los medios materiales de que dispone respecto de las competencias que tiene atribuidas.

La principal inquietud, común al conjunto de los Grupos Parlamentarios, afecta al desconocimiento por parte de las empresas de la normativa de protección de datos; circunstancia que, añadida a la existencia de niveles más intensos de protección en la legislación española que en la de otros países comunitarios, puede dificultar el ejercicio de su actividad o, incluso, la deslocalización empresarial. En tal sentido los Grupos Parlamentarios hicieron especial hincapié en la necesidad de que la Agencia multiplicara sus actuaciones informativas, de carácter preventivo, con el fin de facilitar el conocimiento y la aplicación de la Ley.

En particular, se hizo referencia específica a la urgencia de desarrollar el censo promocional para actividades de publicidad.

Ambas preocupaciones fueron compartidas por el Director de la Agencia, quien destacó las actuaciones llevadas a cabo para informar sobre las exigencias legales, especialmente a las pequeñas y medianas empresas, y la necesidad de que dichas actividades no se circunscriban a las poblaciones que concentran una mayor actividad empresarial, como Madrid y Barcelona, sino que se extienda a todo el territorio nacional. Adicionalmente, puso de manifiesto su disposición a intensificarlas en la medida en que lo permitan los medios humanos de la Agencia.

Como cuestiones específicas destacadas por los Portavoces cabe señalar las que a continuación se mencionan.

Garantías para la protección de datos en las transferencias internacionales .

Según se había informado en comparecencias anteriores, la Agencia había autorizado transferencias internacionales de datos basadas en cláusulas contractuales que garantizaran estrictamente los derechos de los afectados. A la vista del incremento de solicitudes de autorización de transferencias internacionales se planteó si se mantenía el rigor preexistente.

El Director informó sobre el mantenimiento de las exigencias para autorizar las transferencias advirtiendo, no obstante, que el nivel de protección se vería rebajado en el caso de los Estados Unidos de Norteamérica como consecuencia de la aprobación de los principios de "puerto seguro" y de las "preguntas más frecuentes" (FAQ) que los interpretan, dado su carácter de principios genéricos al que se añade la complejidad de interpretarlos conforme a las FAQ.

Protección de datos en el ámbito de las Administraciones Públicas.

La gestión de los ficheros de titularidad pública mereció una mención específica relacionada con las deficiencias que pueden producirse en materia de seguridad. En este sentido se destacó la necesidad de dotar al personal de las Administraciones Públicas de formación suficiente, a cuyo efecto, se instaba a la Agencia a desarrollar actuaciones que permitan incrementarla.

Asimismo, se suscitó la necesidad de conseguir la coordinación y el mantenimiento de criterios comunes con el Defensor del Pueblo.

El Director informó de las gestiones realizadas para conseguir la inscripción de los ficheros de titularidad de las Corporaciones Locales en el Registro General de Protección de Datos y de las relaciones fluidas con el Defensor del Pueblo, especialmente en los expedientes de infracción de las Administraciones Públicas en las que la Agencia está obligada a dar cuenta a dicha Institución de las resoluciones adoptadas y de las medidas adoptadas para su cumplimiento.

Problemas relacionados con la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre.

Las actividades descritas en la Memoria de 1999 se realizaron bajo la vigencia de la derogada Ley Orgánica 5/1992, de 29 de octubre. Sin embargo, en el momento de producirse la comparecencia se encontraba en vigor la Ley Orgánica 15/1999, que la sustituyó, lo que determinó que los Grupos Parlamentarios solicitaran información sobre los problemas planteados en la aplicación de la nueva norma.

El Director de la Agencia centró su intervención en los problemas relacionados con la Disposición Adicional Primera de la Ley Orgánica, que afecta al sistema transitorio para su aplicación, comunicando las actuaciones realizadas para obtener un Dictamen consultivo del Consejo de Estado.

Reglamento de Medidas de Seguridad .

La aprobación del Reglamento de Medidas de Seguridad durante la tramitación parlamentaria de la nueva Ley orgánica 15/1999, suscitó dudas de los Grupos Parlamentarios acerca de la compatibilidad y congruencia entre ambas normas.

A juicio del Director, la aprobación del Reglamento de Medidas de Seguridad ha sido uno de los elementos más importantes para posibilitar el conocimiento de la normativa de protección de datos por parte de las empresas, cuyo cumplimiento ha exigido a éstas un esfuerzo más organizativo que económico. Por lo demás, a juicio de la Agencia, el

Reglamento se adecúa a las exigencias de la Ley Orgánica, habiéndose facilitado su implantación toda vez que su aplicación ha sido gradual en el tiempo.

En la misma sesión de la Comisión Constitucional se abordó el tema de la protección de la intimidad en Internet, a solicitud del Grupo Parlamentario Socialista del Congreso.

El Portavoz del Grupo solicitante de la comparecendcia inició su intervención haciendo una referencia genérica al desarrollo de Internet y a los riesgos que puede suponer para la intimidad personal. En particular abordó los problemas relacionados con la seguridad en Internet, con la posibilidad de obtener información sin conocimiento del usuario y con el retraso de la respuesta jurídica respecto de las nuevas iniciativas empresariales que pueden afectar a la intimidad. En relación con este último aspecto hizo una referencia crítica al hecho de que la respuesta jurídica aparezca más vinculada a los sistemas de autorregulación privada que a iniciativas de los poderes públicos.

Finalmente, planteó tres cuestiones relativas a las acciones de la Agencia en este ámbito, a la reacción política que ha habido respecto de este fenómeno en relación con los derechos fundamentales y a los problemas relacionados con la seguridad.

El Director de la Agencia, compartiendo las inquietudes del Portavoz Parlamentario, abordó los problemas de la protección de datos en Internet haciendo referencia a los siguientes aspectos.

En primer lugar señaló que la protección de la intimidad en Internet tiene, como primeros agentes, a los propios usuarios que deben utilizar la red siendo conscientes de los riesgos que conlleva y adoptando medidas adecuadas para protegerse de los mismos.

En este sentido, hizo referencia a los dictámenes del Grupo del Artículo 29 -grupo consultivo formado por las autoridades de protección de datos de los Estados miembros de la UE-, así como a las recomendaciones a los usuarios de Internet publicadas por la Agencia de Protección de Datos.

El segundo lugar valoró las ventajas de la autorregulación y, en particular, las previsiones del Código-tipo de la Asociación Española de Comercio Electrónico.

Finalmente, aludió a los expedientes sancionadores incoados por la Agencia por infracción de la normativa de protección de datos en Internet. Entre ellos hizo referencia a los supuestos de remisión de publicidad no deseada a través de la dirección de correo electrónico, a la obtención de datos a través de páginas web ubicadas en los Estados Unidos de Norteamérica sin respetar las exigencias de la normativa española de protección de datos que posteriormente eran cedidos a filiales radicadas en España, a la publicación en una página web de datos relativos a infracciones penales o administrativas y al tratamiento de datos personales por la productora del programa "Gran Hermano". El detalle de estos expedientes puede analizarse en otros epígrafes de la Memoria.

La segunda comparecencia tuvo lugar el 14 de diciembre de 2000 para responder a diversas iniciativas planteadas por los Grupos Parlamentarios.

La comparecencia se inició con la intervención del Portavoz del Grupo Parlamentario solicitante de la misma, quien planteó los problemas que, a su juicio, se producen respecto de la protección de datos personales por parte de dos tipos de titulares de ficheros que disponen de datos masivos de los ciudadanos, como son las entidades financieras y las Administraciones Públicas.

La intervención se apoyó, adicionalmente, en la Sentencia del Tribunal Constitucional de 30 de noviembre de 2000 en la que, además de declararse la inconstitucionalidad y consiguiente nulidad de diversos preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, se configura el derecho a la protección de datos como un derecho autónomo independiente del derecho a la intimidad que otorga al ciudadano un poder de disposición y control sobre los datos personales que le afectan, así como sobre su uso y destino.

En relación a las entidades financieras, tras resaltar la cantidad y calidad de datos personales que pueden tratar, se suscitó el problema de la seguridad en el tratamiento de dichos datos, a la vista de informaciones periodísticas sobre la obtención de los mismos en contenedores de basura.

La segunda cuestión relacionada con estas entidades -así como con otras grandes compañías como las de telecomunicaciones o las aseguradoras- afectó a la cesión de datos personales a terceros.

En tercer lugar se hizo referencia a los problemas en el tratamiento de datos por parte de empresas dedicadas a informar sobre la solvencia patrimonial y el crédito y, en particular, a las relevantes consecuencias que tiene para las personas la inclusión errónea en dichos ficheros, equivalente a su "muerte civil", y a la necesidad de que desaparezcan de los mismos los deudores que han pagado sus deudas.

Por lo que respecta a las Administraciones Públicas se suscitaron, a la vista de la Sentencia antes citada, los problemas relativos a la cesión de datos a otros Administraciones sin habilitación legal y a la omisión del deber de información a los ciudadanos respecto de los datos tratados por ellas.

Por último, como cuestión de especial relevancia, se planteó el problema de la seguridad en el tratamiento de los datos por parte de las instituciones sanitarias.

En relación con los problemas de seguridad de las entidades financieras el Director de la Agencia informó sobre las actuaciones inspectoras llevadas a cabo para determinar si los problemas de seguridad eran o no imputables a aquéllas, o a sus propios clientes. En el primer caso refirió los expedientes sancionadores incoados y, en el segundo, la decisión de archivo de las actuaciones. Las actuaciones de la Agencia no se limitaron a la iniciación de estos expedientes sino que incluyeron una comunicación a la Asociación Española de Banca dirigida a poner en su conocimiento tales hechos y a solicitar la adopción de medidas apropiadas; comunicación que tuvo una favorable respuesta por parte de su Presidente.

Complementariamente, hizo referencia a la utilización de nuevas técnicas potencialmente invasoras de la intimidad por parte de tales entidades como las realizadas a través de sistemas "data warehouse" y "data mining", así como a los tratamientos de "scoring", que añaden riesgos adicionales al permitir la elaboración de perfiles de los ciudadanos. A juicio del Director tales tratamientos sólo podrán realizarse con el consentimiento del afectado.

Como cuestión relevante conexa con el tratamiento de datos por parte de las entidades financieras, el Director de la Agencia informó sobre los ficheros de solvencia patrimonial y crédito regulados en el art. 29 de la Ley Orgánica 15/1999, distinguiendo los dos tipos de ficheros contemplados en el mismo.

Tras sintetizar las Instrucciones aprobadas por el Director de la Agencia en relación a aquéllos, hizo referencia al caso concreto de los ficheros de información positiva, que permiten obtener información sobre el cumplimiento de obligaciones. A este respecto, manifestó su criterio de que tales ficheros podrán incluir datos positivos, pero no toda la información de la solvencia de un ciudadano añadiendo que ello será posible siempre que el afectado consienta y no por iniciativa exclusiva del acreedor.

La referencia a los ficheros de morosidad finalizó con una manifestación sobre su utilidad, no sólo para las entidades financieras, sino también y, muy especialmente, para las pequeñas y medianas empresas que pueden tener importantes quebrantos e, incluso, desaparecer, si no disponen de información sobre los riesgos que asumen.

Informó, asimismo, sobre los problemas de seguridad en el tratamiento de datos por parte de algunas Administraciones Públicas y de los expedientes sancionadores incoados.

En el ámbito de las medidas de seguridad, puso de manifiesto la importancia de la aprobación del Reglamento de Medidas de Seguridad y las actividades informativas desarrolladas por la Agencia en relación al mismo, tanto a través de consultas al Gabinete Jurídico y al Area de Atención al Ciudadano, como por medio de la participación del Director y de funcionarios de la Agencia en multitud de foros, cursos y seminarios. A estas actuaciones se añaden las vinculadas a planes sectoriales de inspección, que analizan las medidas de seguridad existentes en cada ámbito de actividad económica concluyendo con la formulación de recomendaciones que permitan su mejora.

También aludió a los Protocolos suscritos para facilitar el cumplimiento de la Ley Orgánica.

El Director hizo referencia a diversos expedientes sancionadores incoados por la Agencia por incumplimiento de las medidas de seguridad en diversos sectores, cuyo detalle puede analizarse en otros apartados de esta Memoria.

La intervención terminó con un análisis de la Sentencia del Tribunal Constitucional antes referida.

El Director alabó la rapidez con que se había producido el pronunciamiento del Alto Tribunal y, tras dar cuenta de sus aspectos más relevantes, puso en conexión la configuración del derecho a la protección de los datos personales reconocido por la Sentencia con el contenido del art. 8 de la Carta Europea de Derechos Fundamentales aprobada en la Cumbre de Niza.

La referencia a la Sentencia terminó con una consideración sobre sus efectos, en el sentido de que, en aplicación del principio de irretroactividad "in peius" de las disposiciones sancionadoras no podrá producir efectos retroactivos en este ámbito.

MEMORIA DE 2000 - ASPECTOS INTERNACIONALES DE LA PROTECCIÓN DE DATOS. ANÁLISIS DE LAS TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES.

1. EL DERECHO A LA PROTECCIÓN DE DATOS EN LA CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

En la cumbre de Jefes de Estado y de Gobierno de la Unión Europea, celebrada en Niza el 7 de diciembre de 2000 se proclamó la Carta de Derechos Fundamentales de la Unión Europea, paso esencial en la construcción de la Europa de los ciudadanos.

En el último párrafo de su Preámbulo se señala que "la Unión reconoce los derechos, libertades y principios enunciados a continuación", incluyendo, en su artículo 8 el derecho a la protección de datos de carácter personal, como derecho específico de los ciudadanos europeos. El citado artículo dispone:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."

En consecuencia, la Carta reconoce el derecho a la protección de datos como independiente del derecho a la intimidad, siendo su reconocimiento en la misma mucho más detallado que el previsto para otros derechos fundamentales, dado que el artículo dedicado al mismo no se limita a efectuar ese reconocimiento, sino que explicita claramente el contenido básico del derecho y la existencia misma de las autoridades de protección de datos existentes en los distintos Estados de la Unión Europea

2. UNIÓN EUROPEA. GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES CREADO POR EL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE

El artículo 29 de la Directiva 95/46/CE creó el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Este grupo tiene, entre otras funciones, la obligación de facilitar a la Comisión, al Parlamento Europeo y al Consejo un informe anual sobre el estado de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal en la Comunidad y en terceros países.

El Grupo de Trabajo se compone de representantes de las autoridades nacionales independientes encargadas de la protección de datos y un representante de la Comisión. Asimismo, incluirá en el futuro un representante de la autoridad responsable de las cuestiones relacionadas con la protección de datos dentro de las instituciones europeas, conforme a lo establecido en el Reglamento regulador de dicha institución. Por último, pueden asistir a las reuniones del Grupo, en calidad de observadores, representantes de las Autoridades de Control existentes en los Estados signatarios del Convenio sobre el Espacio Económico Europeo, no integrantes de la Unión Europea (Noruega, Islandia y Liechtenstein).

Al compartir la experiencia de las autoridades nacionales, el Grupo de Trabajo impulsa la aprobación de una estrategia coherente para la aplicación de los principios generales enunciados en la Directiva, aconsejando a la Comisión en aquellas cuestiones que se encuentran relacionadas con la protección de datos.

Por otra parte, una de las funciones principales del Grupo de Trabajo es la de formular dictámenes sobre el nivel de protección en la Unión y en los terceros países, y en emitir recomendaciones sobre cualquier cuestión referente a la protección de las personas con respecto al tratamiento de datos de carácter personal, pudiendo instarse por las propias Autoridades integrantes del Grupo la formación de grupos de estudio de determinadas cuestiones.

La Agencia de Protección de Datos española forma parte de este Grupo de Trabajo, participando activamente en los diferentes debates y trabajos preparatorios de los distintos documentos elaborados por el mismo.

Como fruto de este trabajo y en el ejercicio de las competencias atribuidas por la Directiva, el Grupo de Trabajo del Artículo 29 ha elaborado los siguientes documentos durante 2000:

* Dictamen 1/2000, sobre determinados aspectos de protección de datos del comercio electrónico. Adoptado por el Grupo de Trabajo el 3 de febrero de 2000 (DG MARKT 5007/00/ES/final WP 28).

* Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones. Adoptado por el Grupo de Trabajo el 3 de febrero de 2000 (DG MARKT 5009/00/ES/final WP 29).

* Recomendación 1/2000 sobre la aplicación de la Directiva 95/46/CE. Adoptada por el Grupo de Trabajo el 3 de febrero de 2000 (DG MARKT 5139/00/ES/final WP 30).

* Dictamen 3/2000, sobre el Diálogo entre la Unión Europea y los Estados Unidos en relación con el Acuerdo de "Puerto Seguro". Adoptado por el Grupo de Trabajo el 16 de marzo de 2000 (DG MARKT 5019/00/ES/final WP 31).

* Dictamen 4/2000, sobre el nivel de protección que proporcionan los principios de "Puerto Seguro". Adoptado por el Grupo de Trabajo el 16 de mayo de 2000 (DG MARKT CA07/434/00/ES WP 32).

* Dictamen 5/2000, sobre el uso de guías telefónicas para servicios de búsqueda inversa o multicriterio (Guías inversas). Adoptado por el Grupo de Trabajo el 13 de julio de 2000 (DG MARKT 5058/00/ES/final WP 33).

* Dictamen 6/2000, sobre la cuestión del genoma. Adoptado por el Grupo de Trabajo el 13 2000 (DG MARKT 5062/00/ES/final WP 34).

* Dictamen 7/2000, sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y para la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de julio de 2000 COM (2000) 385. Adoptado por el Grupo de Trabajo el 2 de noviembre de 2000 (DG MARKT 5042/00/ES/final WP 36).

* Documento de Trabajo "Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea". Adoptado por el Grupo de Trabajo el 21de noviembre de 2000 (DG MARKT 5063/00/ES/final WP 37)

Al propio tiempo, a lo largo del año 2000, el Grupo de Trabajo ha analizado la existencia de un nivel adecuado de protección en otros terceros Estados, así como la evolución de las reuniones entre los representantes de la Comisión y otras Entidades y Asociaciones con vista a la aprobación de modelos contractuales de transferencia internacional de datos y la adopción de Códigos Tipo en el seno de diversos sectores de actividad, siguiendo los criterios establecidos en los diversos documentos que fueron aprobados a lo largo de 1998, a los que ya se hizo referencia en la Memoria Anual de la Agencia de Protección de datos correspondiente a ese año. Precisamente en relación con esta última cuestión se acordó la participación de varios representantes del Grupo de Trabajo, entre los que se encontraba una representación de la Agencia de Protección de Datos en un subgrupo cuya función consistiría en la elaboración de unas cláusulas contractuales tipo aplicables a un gran número de transferencias a empresas ubicadas en estados respecto de los cuales no se hubiera declarado un nivel adecuado de protección.

Además, en lo relativo a las transferencias internacionales, deben tenerse en cuenta las Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE y 2000/520/, de 26 de julio (publicadas en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000), que consideraron adecuado el nivel de protección de datos personales en Suiza, Hungría, así como "el conferido por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos".

Asimismo, el Grupo de Trabajo ha centrado buena parte de sus reuniones en el análisis de los nuevos acontecimientos producidos, esencialmente a nivel legislativo, en los Estados miembros.

Como puede comprobarse, de lo indicado hasta ahora se desprende la necesidad de referirnos separadamente a los distintos campos de actividad del Grupo de Trabajo, haciendo en primer lugar una, siquiera somera, referencia a los problemas derivados de la transposición de la Directiva, refiriéndonos posteriormente a aquellas materias en que la producción del Grupo de Trabajo ha revestido una mayor relevancia: la actuación del Grupo en relación con Internet, el análisis de la concurrencia de un nivel adecuado de protección en terceros Estados, centrado esencialmente en el análisis del denominado Puerto Seguro, las cuestiones relacionadas con el sector de las Telecomunicaciones y la preparación de un modelo de cláusulas contractuales tipo que habiliten las transferencias internacionales de datos, con arreglo a los dispuesto en el artículo 26.4 de la Directiva.

LA TRANSPOSICIÓN DE LA DIRECTIVA

Cada vez que se ha reunido, el Grupo ha venido efectuando un seguimiento constante del grado de transposición de la Directiva 95/46 por parte de los Estados miembros.

En este sentido, se ha tratado de instar a aquellos Estados que no habían cumplido con la transposición en el plazo establecido al efecto (que concluyó el 24 de octubre de 1998) para que adoptaran las medidas necesarias a la mayor brevedad. Así, en su reunión de 3 de febrero de 2000, el Grupo de Trabajo adoptó una recomendación, dirigida a los Estados miembros que no han cumplido debidamente con el deber de transposición lo adopten en el plazo más breve posible.

En la citada recomendación se indicaba que "El Grupo de Trabajo lamenta que no todos los Estados miembros hayan incorporado la Directiva a su debido tiempo. La consecuencia de este retraso es la persistencia de regímenes divergentes, que perpetúan la inseguridad jurídica en lo relativo a las obligaciones de los responsables del tratamiento de datos personales (empresas y administraciones públicas) y a los derechos de los particulares". Asimismo se señalaba que "el Grupo de Trabajo sólo puede dar plena eficacia a su mandato y, por consiguiente, contribuir a la aplicación uniforme de las medidas nacionales para facilitar el libre flujo de los datos personales dentro y fuera de la Unión, si tiene un conocimiento preciso de las normas nacionales", máxime teniendo en cuenta los esfuerzos efectuados por terceros estados para adoptar sus legislaciones al contenido de la Directiva, con la finalidad de entenderse que proporcionan un nivel adecuado de protección que, sin embargo, no ha sido adoptado por las legislaciones de algunos

Estados miembros.

En definitiva, el Grupo manifestaba su preocupación porque "en aquellos países en que no se haya hecho tal esfuerzo, y en ausencia de incorporación de la Directiva, las transferencias de datos personales puedan originar vulneraciones de los derechos y libertades fundamentales de la persona garantizados por dicha Directiva", recomendando a los Estados miembros, a sus Gobiernos y sus Parlamentos la adopción urgente de las medidas necesarias para que la Directiva se incorpore al Derecho nacional tan pronto como sea posible.

Al final de 2000 no habían concluido, sin embargo los trabajos de transposición a la Directiva en Alemania, Francia, Irlanda y Luxemburgo.

Por otro lado, el Grupo de Trabajo trata de vigilar que las tareas de transposición no incrementen las diferencias existentes en la actualidad entre las diversas legislaciones de la Unión Europea en materia de protección de datos personales, lo que haría inviable el deseo de eliminar los obstáculos a la circulación de datos personales. Con ello se trata de hacer posible que, como señala el considerando octavo de la Directiva, el nivel de protección de los derechos y libertades de las personas, en lo que se refiere al tratamiento de dichos datos, sea equivalente en todos los Estados miembros.

ANÁLISIS DE LA EXISTENCIA DE UN NIVEL ADECUADO DE PROTECCIÓN EN TERCEROS ESTADOS

Introducción

Es necesario, antes de entrar en el análisis de los supuestos concretos objeto de estudio en el año 2000, tomar en cuenta los criterios sentados por el propio Grupo de Trabajo para la apreciación de la existencia de un nivel adecuado de protección de datos en Estados no miembros de la Unión Europea, contenidos fundamentalmente en el documento de trabajo sobre Transferencias de datos personales a terceros países y aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998 (DG XV D/5025/98 WP 12).

El objetivo de la protección de datos es ofrecer asistencia a las personas cuyos datos son objeto de tratamiento. Normalmente, dicho objetivo se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento. Las obligaciones y los derechos establecidos en la Directiva 95/46/CE se basan en aquellos dispuestos en el Convenio n§ 108 (1981) del Consejo de Europa, que a su vez no son diferentes de los incluidos en las directrices de la OCDE (1980) o en las directrices de la ONU (1990). Por eso, parece que existe un alto grado de consenso en relación con el contenido de las normas de protección de datos que traspasa los límites del espacio ocupado por los quince Estados de la Comunidad.

Es necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema utilizado para asegurar la eficacia de dichas normas. En Europa las legislaciones han incluido en general las normas de procedimiento como el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Estos aspectos relativos al procedimiento están plasmados en la Directiva 95/46/CE, con sus disposiciones sobre responsabilidades, sanciones, recursos, autoridades de control y notificaciones.

Fuera del ámbito comunitario es menos común encontrar estos medios de procedimiento para asegurar el cumplimiento de las normas de protección de datos. Los signatarios del Convenio 108 deben incorporar los principios de la protección de datos en su legislación, pero no se requieren mecanismos complementarios tales como una autoridad de control. Las directrices de la OCDE sólo exigen que "se tengan en cuenta" en la legislación nacional y no prevén procedimientos para garantizar que las directrices deriven en una protección efectiva de las personas físicas.

Por otro lado, las últimas directrices de la ONU sí incluyen disposiciones de control y sanciones, lo que refleja una creciente sensibilización a nivel mundial sobre la necesidad de aplicar debidamente las normas de protección de datos.

Tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debería ser posible lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento y de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. El grado de riesgo que, en el caso de una transferencia internacional, supone para el interesado será un factor importante para determinar los requisitos concretos de un caso determinado.

De lo analizado por el Grupo de Trabajo, los principios que, necesariamente, deberían concurrir en un sistema de protección de datos para considerarlo adecuado, a los efectos de la Directiva 95/46/CE, serían los de de limitación de objetivos (finalidad), proporcionalidad y de calidad de los datos, transparencia (información en la recogida de los datos), seguridad, respecto al ejercicio de los derechos de acceso, rectificación, cancelación y oposición, el establecimiento de restricciones respecto a transferencias sucesivas a otros terceros países

Además, deben aplicarse otros principios adicionales a tipos específicos de tratamiento como a los datos sensibles, la publicidad directa - con la posibilidad de negarse a transferencias de datos cuyo fin sea la publicidad directa, o la decisión individual automatizada - cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

Por su parte, los objetivos de un sistema de protección de datos son básicamente:

a) Asegurar un **nivel satisfactorio de cumplimiento** de las normas.

b) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos.

c) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas.

* Aplicación práctica de estos criterios durante el año 2000. Estudio del nivel de protección en los Estados Unidos. Los llamados principios de Puerto Seguro.

Tomando estos datos en consideración, el procedimiento seguido por el Grupo de Trabajo consiste en un estudio preliminar de la legislación existente en el Estado objeto de análisis (referida no solo a la protección de datos sino a cualesquiera otras cuestiones que puedan encontrarse relacionadas con esta materia, como por ejemplo, el régimen de las telecomunicaciones), llevado a cabo, generalmente por los servicios de la Comisión Europea. Este estudio es sometido al Grupo, a fin de que manifieste su parecer, planteando las cuestiones que resulten discutibles o dudosas. Las cuestiones son planteadas a las autoridades del tercer Estado por la Presidencia del Grupo, pudiendo, en caso de estimarse necesario, plantear cuestiones adicionales en una reunión del Grupo con las citadas autoridades. Cumplidos estos trámites, el Grupo de Trabajo, en caso de apreciar la existencia de un nivel adecuado de protección, aprueba un dictamen en ese sentido, quedando la cuestión sometida al Comité regulado por el artículo 31 de la Directiva, de cara a la adopción de una decisión definitiva sobre la cuestión por parte de la Comisión Europea.

Siguiendo este procedimiento, durante el año 2000 se ha proseguido con el análisis del régimen existente en otros terceros Estados, tales como Eslovaquia, Eslovenia o Polonia y los territorios extracomunitarios británicos de la Isla de Man, Guernsey y Jersey, habiendo centrado el Grupo de Trabajo sus esfuerzos en el estudio del nivel de adecuación ofrecido por los principios de Puerto Seguro, adoptados por el Departamento de Comercio de los Estados Unidos, lo que exige atender en particular a este tema, dado que las opiniones del Grupo de Trabajo en materia de transferencias se han referido exclusivamente al mismo.

Como ya se indicó en la Memoria correspondiente a 1999, durante aquel año el Grupo de Trabajo informó favorablemente el nivel de adecuación de las legislaciones de protección de datos de Suiza y Hungría. Como culminación de este procedimiento, la Comisión de las Comunidades Europeas dictó, en fecha 26 de julio de 2000 sendas Decisiones (2000/518/CE y 2000/519/CE) que declaraban adecuado el nivel de protección de datos ofrecido en ambos países.

Tal y como se indicaba en la memoria correspondiente a 1999, y frente al estudio de otros Estados, en los que el punto de partida para el análisis de la cuestión ha sido el estudio de una legislación de protección de datos aplicable en todo el territorio del estado, el problema de partida para el análisis de la cuestión en los Estados Unidos se centra en el hecho de que no existe, dado el marcado carácter autorregulador del comercio en dicho país, una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad, sino a lo sumo normas dispersas aplicables a sectores muy concretos.

En efecto, la protección de la intimidad y de los datos en Estados Unidos se enmarca en un complejo entramado de regulación sectorial, tanto a nivel federal como estatal, que se combina con la autorregulación industrial. En este sentido, el Grupo de trabajo ha considerado que este conjunto de leyes sectoriales muy segmentadas y la autorregulación voluntaria no son suficientes para proporcionar protección adecuada en todos los casos a los datos personales transferidos desde la Unión Europea.

A fin de superar los problemas derivados de esta dispersión normativa, el Departamento de Comercio de los Estados Unidos presentó, como documento para la discusión entre las autoridades norteamericanas y de la Unión Europea un borrador de "principios de puerto seguro", a fin de garantizar a los operadores que se adhirieran a los mismos una "presunción de adecuación" al nivel de protección exigido por la Directiva, permitiéndose así la libre transferencia internacional de datos a dichos operadores. Para ello, aquéllos debían manifestar ante la Oficina Federal de Comercio (u otra entidad por ella designada) su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas.

El texto de los principios se dividía en siete apartados, dedicados a las materias más importantes recogidas en los Acuerdos y normas fundamentales sobre protección de datos, así como a la aplicación de los principios.

Por otra parte, durante el desarrollo de las negociaciones, los principios se vieron complementados por una serie de "preguntas más frecuentes" (FAQ), en que se daba explicación a los principios, modificando en muchos de los supuestos el contenido que parecía derivarse de los mismos. El Grupo de Trabajo exigió, a la vista de estas FAQ que se otorgara a las mismas el mismo grado de obligatoriedad que a los principios, constituyendo aquéllas y éstos un único cuerpo normativo.

Como ya se indicó también en la memoria de 1999, el Grupo de Trabajo dictó una serie de documentos en que se ponían de manifiesto aquéllos aspectos del Puerto Seguro que se consideraban insuficientes frente al nivel de protección mínimo exigible para que fuera posible recomendar una decisión afirmativa de la Comisión Europea.

Durante el año 2000, el Grupo de Trabajo siguió insistiendo en la necesidad de que se introdujeran en el Puerto Seguro mejoras tendentes a lograr esos objetivos.

Así, entre los documentos aprobados a lo largo del año 2000, el Grupo de Trabajo adoptó dos documentos referentes al

Puerto Seguro.

El primero de dichos documentos fue adoptado en la reunión de 16 de marzo de 2000 a propuesta de la Agencia de Protección de Datos, como reacción a las noticias aparecidas en los medios de comunicación en los que se consideraba que el Acuerdo en su versión de enero de 2000 iba a ser finalmente considerado adecuado en una decisión de la Comisión. En ese documento (opinión 3/2000) se recordaba a la Comisión Europea que en el último dictamen del Grupo adoptado en diciembre de 1999, cuyo resumen puede encontrarse en la memoria correspondiente a ese año, el Grupo consideraba insatisfactorio el texto presentado por las Autoridades de los Estados Unidos. Por esta razón, se instaba a la Comisión a continuar las negociaciones, tomando especialmente en consideración lo establecido en aquéllos dictámenes.

Teniendo en cuenta lo indicado en el documento anteriormente señalado, se elaboró una nueva versión del documento de Puerto Seguro, siendo la misma sometida al parecer del Grupo, que informó, en su dictamen 4/2000 de 16 de mayo, en el sentido de manifestar que, si bien algunos aspectos del texto anterior habían sido mejorados en la nueva versión, "habría sido posible conseguir un mayor nivel de protección de los datos", insistiendo en aquéllas cuestiones en las que ya se había manifestado la preocupación del grupo en los anteriores dictámenes emitidos por el mismo.

Así, en particular se consideraba necesaria la introducción de mejoras para conseguir los siguientes objetivos:

- En cuanto al alcance del Puerto Seguro, sería necesario, por una parte especificar el mismo, eliminando cualquier aplicación del Puerto Seguro en supuestos que resultaran contrarios a lo establecido en la Directiva. Por otra parte deberían de limitarse las materias en las que existe una autoridad administrativa competente para la resolución de las cuestiones planteadas por los ciudadanos, que apareciera como entidad reguladora de quienes se adhirieran al Puerto Seguro, dada la indefinición derivada del contenido de las FAQ.

- Por otra parte, deberían limitarse las excepciones al régimen del Puerto Seguro en que podrían ampararse las empresas adheridas para eludir, en determinados supuestos la aplicación de los principios, limitándose las mismas a los supuestos de conflictos de obligaciones impuestos por las leyes, indicándose por las autoridades norteamericanas los motivos que podrían amparar estas excepciones. En especial se consideró necesario reducir al máximo las excepciones relacionadas con los datos de dominio público y las restricciones del derecho de acceso.

- En tercer lugar, se consideró necesaria una mejora del contenido de los principios de acceso, opción y transferencia ulterior, que ajustaran lo establecido para el Puerto Seguro a las previsiones contempladas por la Legislación Europea. En especial, se consideró que resultaba necesario establecer mecanismos claros que facilitaran el ejercicio del derecho de acceso, delimitando las limitaciones que pudieran derivarse de la inexistencia de un adecuado cauce de resolución de controversias. También se exigió que se limitaran las transferencias ulteriores de datos por empresas adheridas al Puerto Seguro, de forma que el mismo no sirviera de instrumento para una salida masiva de datos de ciudadanos europeos fuera del territorio de la Unión.

- Por último y siguiendo con lo establecido en anteriores dictámenes, se exigió la adopción de mecanismos adecuados de ejecución de los acuerdos que, por una parte garantizaran los derechos de los ciudadanos Europeos afectados, y , por otra, superaran la indefinición existente en cuanto a las vías de recurso facilitadas.

- Asimismo, el Grupo de Trabajo destacó la importancia de continuar e incluso acelerar el trabajo sobre las cláusulas de los contratos tipo, con el objeto de tomar una o varias decisiones en virtud del apartado 4 del artículo 26 de la Directiva, lo que constituye una parte importante de la simplificación y transparencia de las salvaguardias necesarias para la transmisión a zonas en las que no hay otros medios de garantizar la protección adecuada.

La participación de la Agencia de Protección de Datos en los debates tendió siempre a lograr la máxima garantía del derecho a la protección de datos de los afectados residentes en la Unión Europea. En este sentido, la Delegación española se mostró partidaria de hacer constar en los documentos del Grupo del artículo 29 la necesidad de efectuar en los principios todas las aclaraciones imprescindibles para que el nivel de protección garantizado por los principios de Puerto Seguro se asimilara en todo momento a los contenidos en la Directiva (un resumen de la opinión española en la materia se expone en la memoria correspondiente al año 1999).

No obstante el Dictamen crítico emitido por el Grupo de Trabajo del artículo 29 de la Directiva, así como el informe del Parlamento Europeo de 11 de julio de 2000 en el que se consideró que las garantías ofrecidas por el acuerdo de Puerto Seguro eran susceptibles de ser mejoradas a la luz de lo indicado en los sucesivos informes del citado Grupo, la Comisión Europea adoptó la decisión 2000/520/CE, de 26 de julio, por la que se declaró la adecuación del nivel de protección conferido por los principios de Puerto Seguro, tomando en consideración el texto objeto de aquel Dictamen, si bien la Administración norteamericana introdujo ciertas mejoras como consecuencia del contenido del Dictamen del Grupo del artículo 29.

La Decisión prevé que se considerará que los principios de Puerto Seguro suponen la existencia de un nivel adecuado de protección, siempre y cuando las entidades norteamericanas manifiesten inequívocamente su compromiso de respetar los citados principios (en consonancia con lo previsto en las "preguntas más frecuentes") y se sometan a la jurisdicción de uno de los Organismos estadounidenses que figuran como Anexo VII de la propia Decisión (Oficina Federal de Comercio y Departamento de Transporte de los Estados Unidos). Debe indicarse que dichas autoridades en ningún caso pueden ser consideradas autoridades de control en el sentido previsto en la Directiva, sino que son órganos de vigilancia de buenas prácticas comerciales.

Por otra parte, el artículo 2 de la Decisión prevé que su aplicación no afecta a la que haya de producirse de las normas internas de los Estados miembros con anterioridad a la transferencia de los datos, añadiendo el artículo 3 la posibilidad de que las Autoridades de Control suspendan una determinada transferencia de datos en caso de que exista una resolución del Organismo estadounidense competente en que se declare la vulneración por la destinataria de los principios de "Puerto Seguro" o existan indicios de que dicha vulneración pueda producirse, con perjuicio de los derechos de los afectados.

El Acuerdo de "Puerto Seguro" consta de siete principios básicos, referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). Dichos principios son, como se indicó, complementados con las "preguntas más frecuentes", básicamente referidas a tipos específicos de datos o tratamientos.

Como consecuencia de lo previsto en la Decisión, será válida la transferencia a las empresas que reúnan los requisitos previstos, pudiendo las autoridades de control verificar su concurrencia. A tal efecto, la Norma Cuarta de la Instrucción 1/2000, de 1 de diciembre, de esta Agencia de Protección de Datos, de la que se efectúa un estudio más detallado en otro lugar de esta Memoria, prevé en su apartado 3 que "si la transferencia se funda en lo establecido en la Decisión 2000/520/CE de la Comisión de la Comunidades Europeas, "sobre la adecuación de la protección conferida por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos", quien pretenda efectuar la transferencia deberá acreditar que el destinatario se encuentra entre las entidades que se han adherido a los principios, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión.

* DICTAMEN 5/2000 SOBRE EL USO DE GUÍAS TELEFÓNICAS PÚBLICAS PARA SERVICIOS DE BÚSQUEDA INVERSA O MULTICRITERIO

En los últimos tiempos, cada vez con mayor frecuencia, se ofrecen nuevas posibilidades de acceso a la información contenida en repertorios o guías de servicios de comunicación en formato electrónico, bien sea a través de acceso a los mismos a través de Internet o mediante la distribución de CD-ROMs que contienen dicha información, que habitualmente comprende el nombre, dirección y números de teléfono de millones de ciudadanos europeos de diversos Estados miembros.

En relación con estos servicios y como consecuencia del planteamiento en España de diversas denuncias en las que se hacía referencia a la existencia de este tipo de directorios ubicados en servidores radicados en otros Estados miembros de la Unión Europea, la Agencia de Protección de Datos propuso que se emitiera por el Grupo de Trabajo del artículo 29 un Dictamen que aclarara la postura a seguir en relación con estos directorios, así como su legalidad desde el punto de vista de la Directiva 95/46/CE.

Una vez tenida en consideración esta propuesta, se acordó la creación de un subgrupo, liderado por la Agencia, que elaborara un documento referido a esta materia. Como resultado de la actividad del mismo, el Grupo de Trabajo, en su reunión de 13 de julio de 2000 adoptó su Dictamen 5/2000, que se analiza a continuación.

Una de las principales innovaciones que ofrece la publicación electrónica es la posibilidad de proporcionar, de forma práctica y a coste reducido, capacidades ampliadas para el tratamiento de la información que figura en las guías telefónicas. Estas capacidades se refieren, básicamente, a la posibilidad de utilizar criterios más amplios de búsqueda para revelar la información que contiene la guía, que se pueden concretar en lo que se conoce como**servicios de búsqueda inversa o multicriterio**.

Estos nuevos servicios, aparte de la utilización tradicional de una guía en papel, es decir, averiguar el número de teléfono de una persona determinada conociendo sus apellidos, nombre y, quizás, su dirección, comprenden nuevas capacidades como la posibilidad de obtener el nombre y la dirección de un abonado indicando su número de teléfono o de realizar búsquedas basadas en la dirección o parte de la dirección, que permiten encontrar el nombre y el número de teléfono de, por ejemplo, todos los abonados residentes en una determinada área geográfica (calle, barrio, ciudad, etc.).

Esta nueva funcionalidad podría implicar un cambio significativo en las expectativas de intimidad de los ciudadanos en relación con los datos personales que figuran en las guías telefónicas públicas. En realidad, antes de la existencia de estos nuevos productos, el hecho de que una persona comunicara su número de teléfono a un tercero no implicaba, en circunstancias normales, la posibilidad de obtener cualquier otra información adicional a partir de esos datos. En cambio ahora, al existir estos productos en el mercado, la situación ha cambiado radicalmente: la simple revelación, intencionada o casual, de un número de teléfono podría ser la clave de acceso a información como la que generalmente figura en una tarjeta de visita, incluidos el nombre y la dirección y, en algunos casos, la profesión y el empleo. Estos datos podrían incluso completarse con datos de carácter geográfico, dado que existen también sistemas informatizados que los proporcionan, como mapas de ciudades y bases de datos con fotografías de viviendas y con la que aparece, por ejemplo, en registros públicos.

De lo anteriormente expuesto, se deduce que utilizar las guías para averiguar datos personales relativos a la persona física a partir de un número de teléfono cuyo abonado es desconocido o los nombres y números de teléfono de las personas que viven en una zona determinada, constituye un uso totalmente diferente del que el consumidor puede esperar cuando se le incluye en la guía. Por lo tanto, se trata de una nueva finalidad que no es compatible con la inicial

(véase la letra b) del artículo 6 de la Directiva 95/46/CE) y que requeriría el cumplimiento de una serie de condiciones para considerarse legítima:

- Deberá obtenerse un *consentimiento específico e informado* del abonado antes de la inclusión de sus datos personales en cualquier clase de guía telefónica pública (telefonía tradicional, telefonía móvil, correo electrónico, firma electrónica, etc.) que permita la realización de búsquedas inversas o multicriterio. La información debe incluir la descripción de las búsquedas multicriterio posibles y la posibilidad de autorizar u oponerse, gratuitamente y en cualquier momento, a este tipo de tratamientos.

- El responsable del tratamiento deberá aplicar también las *medidas técnicas y de organización* apropiadas en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse (véase el artículo 17 de la Directiva 95/46/CE). Esto significa, por ejemplo, que la base de datos debería diseñarse de manera que evite, en la medida de lo posible, usos fraudulentos, como modificaciones ilícitas de los criterios de búsqueda o la posibilidad de copiar o acceder a toda la base de datos para un tratamiento posterior (por ejemplo, los criterios de búsqueda deben ser lo suficientemente precisos para permitir únicamente la presentación de un número limitado de resultados por página). El resultado debería ser que el fin para el que el abonado dio su consentimiento se garantice también por medios técnicos.

Estas condiciones no se aplican solamente a los operadores de telecomunica-ciones, sino también a otros actores, por ejemplo los editores de este tipo de guías, es decir, a *todos* los que desean utilizar datos personales para ofrecer guías o servicios de búsqueda multicriterio.

Para finalizar, el documento establece como conclusiones principales:

- Que el tratamiento de datos personales en las guías inversas o en los servicios de búsqueda inversa o multicriterio sin el consentimiento inequívoco e informado del abonado es desleal e ilícito, si no se cumplen las condiciones establecidas anteriormente.

- Que apoya y acoge con satisfacción la propuesta de la Comisión Europea en el proyecto de revisión de la Directiva 97/66/CE, en la que se recoge la necesidad de contar con el consentimiento informado del afectado sobre si sus datos personales pueden incluirse en una guía pública, con qué fin específico y en qué medida, adaptando, de este modo, las normas a la realidad, puesto que en los nuevos servicios de comunicaciones electrónicas, como GSM y correo electrónico, la mayoría de los abonados no desean hacer públicos sus números de teléfono móvil ni sus direcciones electrónicas y la mayoría de los proveedores de servicios han respetado, en la práctica, los deseos de sus abonados.

* DICTAMEN 7/2000 SOBRE LA PROPUESTA DE LA COMISIÓN EUROPEA DE DIRECTIVA RELATIVA AL TRATAMIENTO DE LOS DATOS PERSONALES Y A LA PROTECCIÓN DE LA INTIMIDAD EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS DE 12 DE JULIO DE 2000 COM (2000) 385

El 12 de julio de 2000, la Comisión Europea adoptó una propuesta de nueva Directiva encaminada a revisar la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Ya en su dictamen 2/2000, de 13 de febrero, el Grupo de Trabajo expresó su opinión sobre algunos aspectos particulares de este proyecto de revisión, realizando en este nuevo documento una revisión integral y sistemática de la propuesta final de la Comisión.

Las principales preocupaciones del Grupo de Trabajo giran en torno al tratamiento de los datos personales que se realizan en Internet o utilizando Internet como medio, cuestión que deberá abordarse de forma más específica, así como a los nuevos problemas creados por la liberalización del mercado de las telecomunicaciones. A continuación se esbozan aquellos aspectos más relevantes que el Grupo de Trabajo puso de manifiesto en su dictamen.

En primer lugar, ve con satisfacción la aclaración producida en la terminología empleada y en el reconocimiento de la opinión del Grupo según la cual, ambas directivas de protección de datos son plenamente aplicables al tratamiento de datos en Internet.

Respecto de la definición de *datos de tráfico*, señala como muy positiva la nueva redacción que implica que todos ellos deben destruirse una vez finalizada la comunicación e incluye dentro de los datos de tráfico los referidos a localización y navegación, que pueden contener datos especialmente protegidos, por lo que se propugna sean revestidos de la confidencialidad prevista para las comunicaciones.

Debería especificarse sin dejar lugar a dudas con qué objetivos y en qué medida los distintos tipos de datos sobre tráfico (correspondientes a la nueva definición ampliada) pueden generarse, recabarse y almacenarse y para qué fines pueden utilizarse posteriormente. El Grupo de trabajo desearía subrayar que, incluso en caso de que se autorice el tratamiento de los datos con un fin específico y con el consentimiento del abonado, éste no renuncia definitivamente por ello a sus derechos a la protección de la intimidad y de los datos.

Asimismo, el Grupo de Trabajo solicita que se armonice el plazo durante el cual es posible conservar los datos de tráfico necesarios para la facturación de los servicios a aquel que resulte lo más breve posible y pide clarificación sobre el exacto significado de la expresión *"servicios de valor añadido"* y solicita garantías específicas sobre la utilización de los datos de localización para la prestación de este tipo de servicios.

En relación con la definición de *servicios de comunicación electrónica*, se da la bienvenida a la claridad que la misma aporta, dejando claro que los servicios que transmitan contenido quedan excluidos del ámbito de aplicación de la Directiva de Telecomunicaciones, debiendo regirse por los preceptos de la Directiva general.

Otro aspecto importante que requiere clarificación, es el hecho incluido en la definición de que los servicios deben prestarse contra remuneración. A pesar de que la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas sostiene que la remuneración no tiene por qué ser necesariamente pagada por los beneficiarios del servicio, pudiendo correr, por ejemplo, a cuenta de los anunciantes, sería conveniente introducir una redacción que clarificara este hecho.

Por lo que respecta a las medidas de seguridad, se acoge favorablemente las consideraciones realizadas en este aspecto y, en particular, la mención de la información que los prestadores de servicios deben ofrecer al público respecto de los posibles riesgos de violación de la seguridad y las medidas que pueden utilizar para minimizarlos, en particular usando determinados tipos de soporte lógico o tecnología de cifrado.

Se resalta el hecho de que la confidencialidad de las comunicaciones constituye uno de los principales elementos de salvaguardia de derecho fundamental a la protección de la intimidad y los datos personales del secreto de las comunicaciones, debiendo estar cualquier excepción a dicho derecho estrictamente limitada y regulada a aquellos supuestos admisibles en una sociedad democrática y, en particular, a los mencionados en los artículos 13 y 15 de la Directiva 95/46/CE. Por ello, se solicita la supresión del apartado 2 del artículo 5 por lo impreciso de su formulación.

También se recuerda la opinión manifestada en su Recomendación 2/99, respecto de la necesidad de que los operadores de telecomunicaciones y los proveedores de servicios de telecomunicaciones adopten las medidas necesarias con el fin de hacer técnicamente difíciles o imposibles, según el estado actual de la técnica, la interceptación de las telecomunicaciones por instancias no autorizadas por la ley.

Estas obligaciones toman un sentido particular cuando las telecomunicaciones entre personas situadas en el territorio de los Estados miembros transiten o puedan transitar por el exterior del territorio europeo, en particular en la utilización de satélites o de Internet.

Por lo que respecta a las guías de abonados, apoya la propuesta de que sean los propios abonados quienes indiquen si desean figurar o no en las guías, ya sean impresas o electrónicas. Además, habida cuenta de la dimensión adquirida por las guías electrónicas en la actual sociedad de la información, los abonados deberían recibir información acerca de los posibles usos de las guías. Adicionalmente, los datos que éstas pueden incluir deberían limitarse a los necesarios para identificar a los abonados sin revelar otra información personal.

Este requisito se pone en conexión con los riesgos para la privacidad derivados de la posibilidad de implantar servicios de búsqueda inversa o multicriterio, que se abordan más ampliamente en el Dictamen 5/2000, analizado en el apartado anterior de esta Memoria.

Otro aspecto muy importante es el relativo a las comunicaciones comerciales no solicitadas (spam), respecto de cuya nueva regulación, basada en el consentimiento previo del usuario (armonizando los requerimientos para el "spam" y los sistemas de llamada automática sin intervención humana y los aparatos de fax), el Grupo de Trabajo se muestra muy favorable.

Además, se hace hincapié en la transparencia con la que se debe facilitar información al usuario acerca de todos aquellos aspectos que afectan al tratamiento de datos personales y se concluye haciendo una valoración, en general, positiva del nuevo marco jurídico propuesto y del objetivo de que los servicios de comunicación sean objeto de una regulación equivalente con independencia de los medios por los que se presten.

El documento finaliza solicitando a la Comisión, al Parlamento Europeo y al Consejo que tengan en cuenta las observaciones realizadas.

* ACTUACIÓN DEL GRUPO DE TRABAJO EN RELACIÓN CON INTERNET

El Grupo de Trabajo ha seguido con gran atención el desarrollo y generalización del uso de Internet y siempre ha puesto de manifiesto su preocupación por aquellos tratamientos que se llevan a cabo en la Red que, a su juicio, constituían una amenaza para la privacidad de los ciudadanos.

Por este motivo ha aprobado y publicado diversos documentos sobre temas específicos en los que se han ido recogiendo sus puntos de vista sobre determinados asuntos: Recomendación 3/97: Anonimato en Internet (1997); Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma Abierta de Perfiles (OPS) (1998); Tratamiento de datos personales en Internet (1999); Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware (1999) y la Recomendación 3/99 sobre la conservación de los datos de tráfico por los proveedores de servicios de Internet a efectos de cumplimiento de la legislación.

Algunos de estos documentos, en concreto todos los publicados desde 1999 en adelante, son el fruto de la actividad del Grupo Operativo de Internet, subgrupo especializado creado por el Grupo de Trabajo del Artículo 29 y en el que participan miembros de las distintas autoridades de control provenientes tanto del campo del Derecho como de las Tecnologías de la Información para proceder a un estudio sistemático de aquellos temas o categorías de tratamientos en Internet que tuvieran una mayor incidencia sobre la intimidad de las personas.

No obstante el trabajo realizado con anterioridad, el Grupo de Trabajo decidió que era necesario proceder a realizar un estudio sistemático e integrado sobre la privacidad en Internet y la protección de datos *on-line*. Por ello, encargó al Grupo Operativo Internet que abordara esta difícil y compleja tarea que, finalmente, se plasmó en el Documento de Trabajo "Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea", aprobado por el plenario del Grupo de Trabajo el 21 de noviembre de 2000.

Este documento de trabajo pasa revista, a lo largo de sus cien páginas, a todos los temas relevantes en este momento para la protección de datos en Internet. Comienza con un primer capítulo en el que se exponen los principios tecnológicos básicos del funcionamiento de la Red para, a continuación, describir los actores principales que desarrollan su actividad en la misma y sus respectivos papeles.

Tras ello, se pasa revista a una serie de riesgos para la privacidad inherentes a los protocolos utilizados para establecer y mantener una comunicación en Internet, principalmente aquellos derivados del protocolo TCP/IP, sobre el que se construyen todo el resto de servicios. También se analizan los riesgos derivados de la implementación del protocolo HTTP, utilizado para *navegar* entre los millones de páginas web existentes en Internet.

En el capítulo 3 se pasa revista a distintas consideraciones legales de carácter general, partiendo del principio de que tanto la Directiva 95/46/CE como la 97/66/CE, específica para el sector de las telecomunicaciones, son aplicables a los tratamientos realizados a través de Internet. Posteriormente, se estudia qué directivas afectan a qué actores en función de las actividades que realicen; el impacto de la propuesta de revisión de la Directiva 97/66/CE realizada por la Comisión Europea; las cuestiones más relevantes abordadas por otros instrumentos legales comunitarios, como la Directiva 1999/93/CE, sobre un Marco Común para la Firma Electrónica, y los efectos internacionales de la aplicación de las leyes nacionales de transposición de la Directiva sobre aquellos tratamientos realizados en el territorio de la Unión Europea, independientemente de la ubicación del responsable de dicho tratamiento.

Los capítulos siguientes pasan revista a los servicios más relevantes que se pueden encontrar en Internet usando un esquema común: introducción, actores implicados, descripción técnica, riesgos para la privacidad, análisis legal y posibles medidas que pueden mejorar el mantenimiento de la privacidad al utilizar dichos servicios.

Los servicios examinados fueron: correo electrónico (capítulo 4), navegación y búsqueda de información en la Red (capítulo 5), información disponible al público y foros de discusión (capítulo 6), transacciones electrónicas en Internet (capítulo 7), *cibermarketing* (capítulo 8) y medidas de mejora de la privacidad (capítulo 9).

El estudio finaliza con un capítulo dedicado a las conclusiones más importantes y se completa con un glosario de términos para ayudar a la mejor comprensión del documento.

En el capítulo de las conclusiones, se pueden destacar las siguientes:

- El desarrollo de Internet es exponencial. Una creciente cantidad de servicios está disponible para el usuario de Internet, desde compras *on-line* hasta la participación en foros de discusión con personas de todos los lugares del mundo. Las compañías intentan atraer al usuario distinguiéndose de las demás mediante el ofrecimiento de servicios gratuitos o personalizados.

La personalización de estos servicios requiere, por su propia esencia, la utilización de datos personales cada vez más detallados obtenidos de diversas fuentes: programas de fidelización, regalos, provisión de servicios gratuitos, utilización de información disponible públicamente en Internet, etc. Esta información tratada en su conjunto constituye un perfil de las personas que es extremadamente valioso, no sólo para las compañías que buscan localizar a los consumidores más sensibles a comprar los productos o servicios que ofrecen, sino que han llegado a tener un valor económico por sí mismos, puesto que son vendidos o alquilados a terceros.

- El desarrollo de nuevas tecnologías hace más fácil rastrear al usuario de Internet. Por ejemplo, si el consumidor utiliza un dispositivo portátil para conectarse a Internet (teléfono, ordenador, asistente personal digital, etc.), se pueden generar datos relativos a su localización geográfica que pueden incluso enriquecer el perfil que de él se tenía (por ejemplo, si realiza cierto tipo de transacciones comerciales cuando se encuentra en una determinada ciudad o zona de la ciudad). Por otro lado, también existen numerosos ejemplos (suministrados a lo largo del documento) de tratamientos de datos que pueden darse sin el conocimiento del usuario tales como procesos invisibles o los llamados "E.T. software". Esto añadido al uso creciente de las direcciones IP estáticas, esto es, fijas a lo largo del tiempo para una persona determinada, hace que sea cada vez más difícil permanecer anónimo en Internet.

- La combinación de estas capacidades lleva aparejada nuevos riesgos para la intimidad de los usuarios de Internet, especialmente cuando la información se concentra en manos de un número limitado de responsables. Si estos responsables hacen uso, por ejemplo, de tecnologías de *data mining* (minería de datos), tienen la posibilidad no sólo de procesar y reorganizar los datos sino también desvelar nuevos enlaces y características relacionados con el afectado quien, usualmente, no es consciente de estas posibilidades y no espera dichos tratamientos.

Estos riesgos también pueden provenir de que ciertos datos, como aquellos obrantes en los grupos de noticias y listas de correo, permanecen *on-line* durante mucho tiempo (incluso varios años) y pueden ser consultados utilizando herramientas de búsqueda inversa.

Todo ello posibilita usos secundarios de la información que, en muchos casos, pueden ser incompatibles con la finali-

dad para la que los datos fueron originalmente recogidos.

Por todo ello, el documento finaliza con una serie de directrices y recomendaciones encaminadas a mejorar el nivel de respeto por la intimidad de los usuarios de Internet. Las más importantes se pueden resumir de la siguiente forma:

- Proporcionar al usuario toda la información necesaria para que pueda tomar sus propias decisiones respecto del tratamiento de sus datos personales con conocimiento de causa. Esta información debe contener, como mínimo, todos los aspectos incluidos en el artículo 10 de la Directiva 95/46/CE.

- Aplicar la legislación existente de una forma coherente y coordinada. Esto es de capital importancia no sólo para afectados y responsables europeos, sino también para todos aquellos externos no pertenecientes a la Unión Europea pero que recogen y tratan datos utilizando medios situados en territorio de la Unión. El Grupo de Trabajo debe jugar un importante papel en la interpretación armonizada de las reglas europeas de protección de datos.

En particular, el Grupo de Trabajo se siente preocupado por el hecho de que ciertas modificaciones de la legislación existente puedan conducir a una mayor vigilancia de las actividades que se producen en la red y a la generalización de la necesidad de identificar a todos los usuarios. Siendo consciente de la existencia de otros intereses legítimos, debería buscarse un equilibrio entre los mismos y el derecho fundamental a la protección de datos personales.

- Promover el desarrollo y uso de tecnologías conformes con los principios de protección de datos. Como ya se ha establecido, el tipo de tratamiento de los datos personales en Internet depende, en gran medida, de la configuración técnica tanto de los equipos físicos como de los programas, protocolos y estándares tecnológicos. Por ello, es especialmente importante que el respeto a la privacidad se tenga en cuenta como un elemento fundamental de seño desde las primeras etapas de desarrollo de nuevas herramientas y tecnologías.

- Sin perjuicio de las atribuciones de las autoridades de protección de datos, construir mecanismos fiables de control y comunicación de incumplimiento de las normas sobre protección de datos. Una posibilidad en este campo es la existencia de planes específicos que garanticen que los asociados al mismo respetan los estándares europeos en materia de protección de datos, condición que podría hacerse visible mediante la visualización de un sello específico.

El Grupo de Trabajo tiene intención de iniciar acciones en este sentido para asegurarse de que las etiquetas de privacidad se otorgan realmente a sitios web que cumplen la normativa europea de protección de datos.

Además del estudio antes mencionado, el Grupo Operativo de Internet también preparó el documento que sirvió de base para el Dictamen 1/2000 sobre determinados aspectos de protección de datos en el comercio electrónico, que, en el marco de los primeros pasos para la revisión de la normativa de telecomunicaciones avanzada por la Comisión Europea, quiso dar la visión del Grupo de Trabajo sobre un aspecto muy específico: las comunicaciones comerciales no solicitadas.

En las conclusiones del documento se distinguen dos situaciones posibles:

- Si una empresa ha obtenido una dirección de correo electrónico directamente del interesado para envíos electrónicos que realizará dicha empresa o un tercero al que proporcione los datos, la empresa inicial debe informar al interesado de dicha finalidad en el momento de recibir la dirección. Además, la empresa inicial y las que hayan recibido los datos posteriormente deberán proporcionar al interesado, como mínimo, en el momento de la recogida y en todo momento posterior, el derecho a oponerse a este uso de sus datos por medios electrónicos sencillos, tales como señalar una casilla creada a tal efecto. Determinadas leyes nacionales por las que se aplican las Directivas pertinentes exigen incluso que la empresa obtenga el consentimiento del interesado. Los requisitos del artículo relativo a las comunicaciones comerciales no solicitadas del proyecto de Directiva sobre comercio electrónico completarían estas normas en un nivel técnico imponiendo al proveedor de servicios la obligación de consultar una lista, pero no eliminarían ninguna de las obligaciones generales aplicables a los responsables del tratamiento de los datos.

- Si una dirección de correo electrónico se obtiene en un espacio público de Internet, su utilización para envíos comerciales electrónicos sería contraria a la legislación comunitaria correspondiente, por tres motivos. En primer lugar, se podría considerar tratamiento ®desleal¯ de los datos personales en el sentido de la letra a) del apartado 1 del artículo 6 de la Directiva general. En segundo lugar, sería contraria al principio de la finalidad de la letra b) del apartado 1 del citado artículo 6, ya que el interesado proporcionó su dirección de correo electrónico para una finalidad muy distinta, como puede ser la participación en un foro, por ejemplo. En tercer lugar, dado el desequilibrio del coste y la interrupción para el destinatario, se puede considerar que estos envíos no superarían la prueba del equilibrio de intereses establecida en la letra f) del artículo 7.

Por otra parte, en la conclusión del Dictamen, se mencionaba que éste no podía considerarse como la posición definitiva del Grupo de Trabajo sobre esta materia, siendo su único objetivo sensibilizar sobre las cuestiones planteadas por un tipo concreto de tratamiento de los datos que era (y es) objeto de debate en numerosos círculos, así como contribuir a la comprensión del marco jurídico aplicable al comercio electrónico. De hecho, el Dictamen 7/2000, aprobado el 21 de noviembre de 2000, sobre la sobre la propuesta de la Comisió Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de julio de 2000 COM (2000) 385, completó al anterior y sirvió para que el Grupo de Trabajo emitiera su opinión sobre el proyecto completo de revisión de la Directiva 97/66/CE.

El Grupo de Trabajo consideraba necesario desarrollar una política común sobre aspectos tales como el ®cibermarke-

ting¯, el pago electrónico o las Tecnologías para mejorar la protección de la vida privada, tarea que había sido encomendada al Grupo Operativo de Internet y que han sido desarrolladas en el documento que se estudió anteriormente.

* ACTIVIDAD DEL GRUPO DE TRABAJO EN RELACIÓN CON LA ELABORACIÓN DE UN MODELO DE CONTRATO PARA TRANSFERENCIAS INTERNACIONALES DE DATOS.

Como ya se indicó, los distintos dictámenes elaborados por el Grupo de Trabajo del Artículo 29 en relación con el nivel de adecuación ofrecido por los denominados principios de puerto seguro ahondaron en la necesidad de que por la Comisión Europea se adoptaran los esfuerzos necesarios para la fijación de un modelo tipo de cláusulas contractuales que habilitaran, en general, la transferencia internacional de datos.

En este sentido, debe recordarse que, como ya se ha indicado en otro lugar de esta Memoria, la Agencia de Protección de Datos ha autorizado, en los últimos años numerosas transferencias de datos que se han verificado mediante la celebración de contratos entre exportador e importador no situado en un Estado que concediera un nivel adecuado de protección de datos, en virtud de cláusulas que han sido consideradas como adecuadas. La celebración de estos contratos ha permitido que se produjera la libre transferencia de datos a terceros estados sobre los que no se ha acordado la existencia de un nivel adecuado de protección, sin que ello menoscabara las garantías que la Directiva y la Ley española consagran a favor de las personas a que los datos se refieren.

Asimismo, el Parlamento Europeo, en el Dictamen referido a los citados principios de Puerto Seguro al que ya se ha hecho referencia en otro lugar de esta Memoria, venía a instar a la Comisión Europea a que dichas medidas contractuales fueran adoptadas a la mayor brevedad, a fin de garantizar los derechos de los ciudadanos y facilitar el movimiento internacional de datos.

La actividad de la Comisión en esta materia había sido, hasta bien entrado el año 2000 la de negociar separadamente distintos modelos sectoriales de contratos con distintas Organizaciones. Sin embargo, como consecuencia de la indicación efectuada por el Parlamento Europeo, se acordó la realización de un modelo contractual único, aplicable a un gran número de operaciones que encerraran una transferencia internacional de datos a terceros estados que no tuvieran un nivel adecuado de protección. Para ello, se instó la colaboración del Grupo de Trabajo, creándose (en la reunión del Grupo celebrada el 13 de julio) un Subgrupo que colaboraría con los servicios de la Comisión en la elaboración de un texto que posteriormente sería sometido a la aprobación del Comité regulado por el artículo 31 de la Directiva, previo informe del Grupo de Trabajo, con la finalidad de que existiera una Decisión final de la Comisión sobre la adecuación de las transferencias basadas en dicho modelo contractual, tal y como prevé el artículo 26.4 de la Directiva.

El citado Subgrupo, formado por representantes de las Autoridades de Protección de Datos de España, Italia, Austria, Francia, Alemania, Países Bajos y Reino Unido se reunió en tres ocasiones a lo largo del último cuatrimestre del año 2000, analizando los sucesivos textos presentados por la Comisión, con el fin de lograr un texto final que obtenga el dictamen favorable del Grupo de Trabajo, previéndose que dicho dictamen sea emitido en la primera reunión que el Grupo celebre a lo largo del año 2001.

La Agencia de Protección de Datos, teniendo en consideración su larga experiencia en la materia, consideró que un modelo contractual que pudiera ser considerado adecuado a los efectos previstos en la Directiva, debería contener, como estipulaciones mínimas, las siguientes:

- Una cláusula de tercera parte beneficiaria, que permita exigir el cumplimiento del contrato al afectado, en todo caso. Esta cláusula debería ser innegociable, no pudiendo las partes derogar la misma. Del mismo modo, la sumisión de las partes a una determinada jurisdicción debería tener en cuenta que la misma reconozca la validez de esta cláusula, no siendo válido el sometimiento a jurisdicciones para las que la misma no sea aplicable.

- El principio general de responsabilidad solidaria del exportador y el importador ante cualquier violación del contrato o en caso de cualquier perjuicio a los afectados, de forma que éstos puedan libremente elegir a quién exigir la compensación que corresponda. Este principio debe ser aplicable en todos los supuestos de transferencia internacional a través del modelo contractual, sin que quepa ninguna excepción. Su fundamento se encuentra en las dificultades prácticas que podrían tener los afectados para proteger sus derechos.

- La consideración, sin límite alguno, de que la recogida y tratamiento de los datos, producida con carácter previo a la transferencia, respetará íntegramente las disposiciones nacionales adoptadas para la transposición de la Directiva 95/46/CE, tal y como se desprende de lo establecido en los artículos 25 y 26 de la misma. De esta forma, cualquier especialidad en el régimen al que se encuentra sometida la transferencia será efectiva única y exclusivamente una vez los datos hayan sido transferidos.

- En todo caso se considera esencial, en orden a preservar los derechos de los afectados que éstos puedan ejercitar sus derechos de acceso, rectificación, cancelación u oposición, en relación con los datos objeto del tratamiento por parte de la importadora como consecuencia de la transferencia, tanto ante la empresa importadora como ante la propia exportadora.

- La necesidad de depósito del contrato, al objeto de que las agencias nacionales puedan llevar a cabo sus obligaciones de control contenidas en la Directiva

- A fin de garantizar el principio de responsabilidad solidaria, resulta imprescindible que el contrato no habilite al importador para realizar ninguna transferencia ulterior de los datos. En este sentido se consideró que la única solución

admisible era la firma de un contrato distinto entre la exportadora y el nuevo importador que permitiría aplicar al mismo un régimen similar y evitar la existencia de posibles fraudes o situaciones no controlables por el mecanismo contractual.

- Por último, y como criterio general, se consideró imprescindible que las cláusulas no excluyan el poder de decisión de las Agencias de Protección de datos cuando, por las circunstancias del importador o del país de destino, no existan garantías de respeto de los derechos fundamentales de los afectados o la legislación del importador no permita la ejecución del contrato, habilitándose a las Agencias a prohibir o suspender las transferencias atendidas las circunstancias del Estado del importador, tal y como ya indicaba el Documento del Grupo de Trabajo sobre criterios en materia de transferencias internacionales (WP 12, de 24 de julio de 1998), ya citado en otro lugar de esta Memoria.

El texto finalmente sometido al parecer del Grupo de Trabajo incorporó la mayor parte de las propuestas de la Agencia de Protección de Datos, así como otras efectuadas por los restantes integrantes del Subgrupo, siendo favorablemente acogido por el Grupo de Trabajo en su reunión de 21 de noviembre de 2000.

Dicho texto incorporaba un borrador de Decisión de la Comisión que consideraba que las cláusulas adjuntas a la misma se consideraban como adecuadas a los efectos previstos en el artículo 26.4 de la Directiva y cuyo artículo 3 planteaba la posibilidad de que la Autoridades de Protección de Datos prohibieran una transferencia, o la suspendieran si ésta había sido iniciada, cuando el Estado destinatario de los datos no garantizase suficientemente la protección de los derechos de los afectados. Asimismo, se preveía la posibilidad de revisión de la Decisión, a la luz de la experiencia.

3. CONSEJO DE EUROPA

En 1981 se firmó el Convenio 108 para la protección de los individuos en relación con el tratamiento automatizado de datos. Este Convenio permitía, en principio, el libre flujo de datos personales entre los Estados que son parte del mismo, flujo que sólo podría impedirse en los supuestos en que dichos Estados dejen de ser parte del Convenio o en caso de que la protección datos en el país en cuestión, aún habiendo sido firmado el Convenio, no sea equivalente o en caso de que los datos se transfieran a un tercer Estado que no sea signatario del Convenio.

El Convenio crea un Comité Consultivo (T-PD), compuesto por los representantes de los Estados que son parte en el mismo. Este Comité es el encargado de la interpretación de las normas, cuidando asimismo del cumplimiento del Convenio.

Los principios contenidos en el Convenio deben adaptarse e interpretarse en función de los diferentes sectores implicados en la actividad. La actividad del Consejo de Europa con este fin se ha desarrollado mediante la aprobación de diversas recomendaciones, dado que su procedimiento de adopción es sencillo y se adaptan mejor a las circunstancias cambiantes de la protección de datos. Se ha considerado que las recomendaciones, a pesar de carecer de obligatoriedad, son una referencia para los Estados.

Con el fin de elaborar estas recomendaciones el Comité de Ministros creó en 1976 un Comité de Expertos sobre protección de datos, que se convirtió después en el Grupo de Proyectos sobre protección de datos (CJ-PD). Este Comité se compone de expertos de los todos los Estados Miembros del Consejo de Europa, los cuales desempeñan tareas de responsabilidad en relación con la protección de datos en sus respectivos países. Asimismo asisten como observadores a las reuniones del CJ-PD representantes de Estados Unidos, Canadá, Japón, la Santa Sede, Australia, la OCDE, UNIDROIT, la Cámara Internacional de Comercio, la Organización Internacional del Trabajo y otras Organizaciones Internacionales.

Durante estos años el CJ-PD no sólo ha elaborado una serie de Recomendaciones, sino que también ha publicado estudios sobre temas específicos en el ámbito de la protección de datos. Del mismo modo, el Grupo ha elaborado diversos dictámenes relacionados con aquellos documentos elaborados en el seno de otros Comités del Consejo de Europa que pudieran incidir en la protección de datos de carácter personal.

La Agencia de Protección de Datos española forma parte de este Comité, participando activamente en los diferentes debates y trabajos preparatorios de los distintos documentos elaborados por el mismo.

Tal y como se indicó en la correspondiente Memoria, durante el año 1999, el Grupo concluyó los trabajos relacionados con el articulado de la Recomendación sobre la protección de datos de carácter personal recogidos y procesados para fines relacionados con el sector asegurador. En el año 2000, se concluyó asimismo el análisis de la Exposición de Motivos ("memorandum explicativo") de la citada Recomendación, siendo este instrumento de sumo interés para el análisis e interpretación del articulado de la misma.

Como se ha indicado, la memoria de 1999 ya dio cuenta detallada del contenido articulado de la citada recomendación, habiendo éste permanecido inalterado, lo que hace innecesario reiterar su contenido en esta Memoria.

Por otra parte, las discusiones a lo largo del año 2000 se han centrado en la elaboración de unas recomendaciones (o, en su caso, directrices) sobre la protección de los datos de carácter personal en relación con las actividades de vigilancia, manifestándose la preocupación de la aplicación de dichas técnicas en el establecimiento de sistemas de vigilancia en el puesto de trabajo o a la vigilancia masiva de lugares públicos, siendo necesario encontrar un justo término medio entre la seguridad y la intimidad.

Además, se han iniciado las discusiones referentes al borrador de Recomendación sobre acceso a documentos públi-

cos (elaborado por otro grupo de Proyectos del Consejo de Europa), que deberán continuar a lo largo del año 2001, dadas las discrepancias existentes entre los diversos Estados. Así, un nutrido grupo de países consideran que el derecho a acceso a información obrante en los ficheros administrativos debe ceder en caso de que dichos datos pudieran afectar a la intimidad de las personas a que los mismos se refieren (tal y como es el caso de España, teniendo en cuenta lo establecido en el artículo 37 de la Ley 30/19992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común), mientras que otros Estados (fundamentalmente los nórdicos) consideran que esa limitación de acceso es una restricción impropia de una sociedad democrática.

También se informaron los Proyectos de Convenios de Colaboración entre los Estados Miembros del Consejo de Europa en materia criminal y de lucha contra el denominado "cibercrimen", exigiendo tomar en consideración en el mismo los principios referentes a la protección de datos de carácter personal.

Por último, se propuso la creación de un grupo de Estudio en materia de cooperación policial y judicial, continuando los trabajos ya iniciados sobre las tarjetas inteligentes. Asimismo, se prevé efectuar un informe multidisciplinar relacionado con la utilización de datos genéticos para fines de investigación criminal, en colaboración con otros grupos de expertos del Consejo de Europa.

Por otra parte, dentro de la actividad desarrollada durante el año 2000, merece especial atención la adopción por el Comité Consultivo (T-PD) del texto de Borrador de Protocolo adicional al Convenio 108, por lo que se procederá a su estudio independiente.

* BORRADOR DE PROTOCOLO AL CONVENIO 108 REFERENTE A AUTORIDADES DE CONTROL Y AL RÉGIMEN DE LAS TRANSFERENCIAS INTERNACIONALES

Como ya se dijo, el Convenio 108 del Consejo de Europa fue el primer texto articulado de carácter vinculante que vino a regular específicamente el derecho a la protección de datos de carácter personal. Sin embargo dicho Convenio, había sido frecuentemente criticado por el hecho de no contener normas específicas relativas a la exigibilidad de que una autoridad independiente pudiera adoptar mecanismos coercitivos que garantizaran ese derecho. Asimismo, se había criticado el régimen referido a las transferencias internacionales de datos.

Por ello desde 1999, se iniciaron en el seno del Consejo los trabajos necesarios para la adopción de un protocolo adicional al Convenio que mejorara la aplicación de los principios contenidos en el mismo, mediante de adición de dos nuevas normas sustantivas referidas, precisamente, a las transferencias internacionales y las autoridades de protección de datos.

Como resultado de dichos trabajos se sometió al Grupo consultivo de protección de datos el citado borrador, siendo el mismo adoptado en su reunión de junio de 2000, procediéndose a su remisión al Comité de Ministros para su definitiva aprobación.

En cuanto al contenido del protocolo, se compone de tres artículos, siendo el tercero de ellos una Disposición final referente a su entrada en vigor, indicando su apartado primero que las normas contenidas en los artículos 1 y 2 deberán ser consideradas por las partes como artículos adicionales al Convenio 108 debiendo el mismo ser interpretado de conformidad con esos preceptos.

El artículo 1 se refiere a las autoridades de control en materia de protección de datos, estableciendo que cada Estado Parte deberá tener una o varias autoridades responsables de asegurar el cumplimiento del Convenio, de conformidad con lo establecido en sus leyes nacionales. Dichas autoridades deberán ejercitar sus funciones con absoluta independencia y cooperar entre sí para el adecuado cumplimiento de las mismas.

En cuanto a estas funciones, el protocolo atribuye a las autoridades de control facultades de investigación y de intervención, así como los poderes para imponer sanciones en caso de vulneración de las disposiciones de protección de datos. Además deberán responder a las quejas que se planteen por cualquier persona en relación con su derecho a la protección de datos, siendo sus decisiones susceptibles de recurso ante los Tribunales.

Por su parte, el artículo 2, referente a las transferencias internacionales de datos, prevé que cada Estado Parte sólo podrá permitir la transferencia a estados u organizaciones que no sean parte en el Convenio si aseguran un adecuado nivel de protección para dicha transferencia.

No obstante, se habilita la posibilidad de permitir la transferencia en los supuestos previstos en las leyes nacionales como consecuencia de la existencia de un interés específico del afectado o de un interés público. Asimismo, la transferencia será posible en caso de que el receptor de los datos garantice el derecho de los afectados a través de cláusulas contractuales.

4. AUTORIDAD COMÚN DE CONTROL DEL SISTEMA DE INFORMACIÓN SCHENGEN

El objetivo del Convenio de Aplicación del Acuerdo de Schengen es permitir la supresión de los controles en las fronteras comunes en la circulación de personas entre los Estados miembros (en la actualidad Alemania, Austria, Bélgica, España, Francia, Grecia, Italia, Luxemburgo, Países Bajos y Portugal), manteniendo en el interior del territorio Schengen creado un nivel de seguridad al menos igual al que ya existía; además de los países señalados, el Convenio se aplicará también en marzo de 2001 en los países nórdicos: Noruega, Suecia, Finlandia, Dinamarca e Islandia.

Entre las medidas compensatorias previstas en el Convenio que persiguen este objetivo, se encuentran la armonización de la política en materia de expedición de visados, una política común en materia de determinación del Estado responsable del examen de la solicitud de asilo, la mejora de la cooperación policial y judicial, la intensificación de la lucha contra el tráfico ilegal de estupefacientes, la armonización del nivel de control de las fronteras exteriores del territorio Schengen y la creación del Sistema de Información Schengen (SIS).

El principal objeto del SIS es, con la ayuda de la información que se transmite en el sistema, preservar el orden y la seguridad públicos, incluida la seguridad del Estado, así como la aplicación de las disposiciones previstas en el Convenio relativas a la circulación de personas en los territorios de los países que conforman el territorio Schengen. El SIS consta de una parte nacional (NSIS) en cada uno de los países que aplican el Convenio y de una unidad de apoyo técnico central ubicada en Estrasburgo (CSIS), estableciéndose de esta forma una conexión entre todos los Estados miembros que permite a los usuarios del sistema la posibilidad de disponer en tiempo real de la información necesaria para sus misiones. Esta información está disponible al efectuar controles en la frontera, así como cuando se realizan otros controles de policía y de aduanas; en el caso de los extranjeros, la información está disponible a efectos del procedimiento de expedición de visados, de expedición de permisos de residencia y de la administración de aquéllos en el marco de la aplicación de las disposiciones sobre la circulación de personas.

En el Capítulo Tercero del Título IV del Convenio se establecen los principios y mecanismos destinados a garantizar una adecuada protección de los datos de carácter personal residentes en el SIS. En su artículo 114 figura que en cada país debe designarse una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre la parte nacional del SIS y de comprobar que el tratamiento y la utilización de los datos introducidos en el SIS no atentan contra los derechos de la persona que se trate. Asimismo, se indica que toda persona tendrá derecho a solicitar a esta autoridad que compruebe los datos referentes a ella integrados en el SIS, así como el uso que se haga de dichos datos. El artículo 10 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, encomienda a ésta el ejercicio del control aquí mencionado.

Por otra parte, el artículo 115 del Convenio establece la creación de una Autoridad de Control Común (en adelante, ACC-Schengen) encargada del control de la unidad de apoyo técnico del SIS; esta autoridad está compuesta por dos representantes de cada autoridad nacional de control. También el artículo 10 del Real Decreto mencionado establece que el Director de la Agencia designará a los dos representantes que formarán parte de la Autoridad de Control Común.

La delegación española ha asistido a las cinco sesiones plenarias que ha celebrado la ACC-Schengen durante el año 2000 en la sede del Consejo de la Unión Europea en Bruselas.

* DATOS INTRODUCIDOS POR LAS AUTORIDADES ESPAÑOLAS

El SIS incluye exclusivamente las categorías de datos que proporciona cada uno de los Estados miembros y que son necesarios para los fines previstos en el Convenio. Las categorías de datos introducidos corresponden a personas descritas, vehículos (cilindrada superior a 50 c.c. o remolques y caravanas de peso en vacío superior a 750 Kg. que hayan sido robados, sustraídos u ocultados fraudulentamente) y objetos (armas de fuego, documentos vírgenes y documentos de identidad expedidos que hayan sido robados, sustraídos u ocultados fraudulentamente, así como billetes de banco registrados). En el caso de las personas descritas se distinguen entre otros los siguientes fines por los que dichos datos pueden ser introducidos por las autoridades competentes: personas buscadas para su detención a efectos de extradición, extranjeros incluidos en las listas de no admisibles, datos de personas desaparecidas o que deban ser puestas a salvo provisionalmente (otorgarles protección, prevención de amenazas, menores de edad), datos de testigos o de personas que deban comparecer ante las autoridades judiciales.

Las autoridades españolas habilitadas para consultar el SIS son las siguientes: Cuerpo Nacional de Policía, Guardia Civil, Policías Autonómicas, Policías Locales, Servicio de Vigilancia Aduanera, Autoridades Judiciales, Oficinas Únicas de Extranjería (Administración de extranjeros), Ministerio de Asuntos Exteriores (Misiones Diplomáticas y Oficinas Consulares).

Según los datos disponibles a fecha de 31/12/2000, las autoridades españolas habían introducido en el SIS los datos de 19.226 personas, lo cual representaba el 2'44% del total de datos que se habían introducido relativos a personas (respecto del año anterior supone una disminución de 1.155 personas). Estos datos se distribuían por finalidad de la siguiente forma: 646 (detención a efectos de extradición), 10.604 (no admisibles), 4.347 adultos y 2.956 menores de edad (desaparecidos o que deban ser puestos a salvo provisionalmente), 641 (testigos y personas que deban comparecer ante las autoridades judiciales) y 32 (otras categorías).

* RESPUESTA A LA INSPECCIÓN DEL CSIS

Durante el año 2000 la ACC-Schengen recibió respuesta al informe de la inspección que había realizado en abril de 1999 en la unidad de apoyo técnico central (CSIS) ubicada en Estrasburgo y en la que participó la delegación española. La ACC pudo constatar que diez de las recomendaciones que había emitido en su informe se habían adoptado en el nuevo sistema CSIS1+, así como que al menos cinco de ellas serían estudiadas para su implantación en el futuro; no obstante, lamentaba no se tuvieran en cuenta todas sus recomendaciones en materia de seguridad física, así como alguna otra medida organizativa relacionada con la gestión de los equipos de cifrado, solicitando se revisara el impacto económico y organizativo de la implantación de estas recomendaciones.

* EVALUACIÓN DE LOS PAÍSES NÓRDICOS

Durante el año 2000 se inició el proceso de evaluación del cumplimiento del Acervo de Schengen por parte de los países nórdicos (Noruega, Suecia, Finlandia, Dinamarca e Islandia), los cuales aplicarán dicho Acervo a partir de finales de marzo de 2001, eliminando por ello el control fronterizo con los países del territorio Schengen. La ACC-Schengen analizó las condiciones previas a la puesta en aplicación de dicho Acervo en materia de protección de datos personales y dictaminó que se cumplían las mismas en dichos países. Para ello, la ACC-Schengen dispuso de las legislaciones nacionales sobre protección de datos de cada uno de los países, de las respuestas de cada país a un cuestionario de la ACC-Schengen, de las explicaciones facilitadas por las delegaciones de esos países en el transcurso de las sesiones plenarias y de un informe que elaboró el Grupo de "Protección de Datos" del Grupo "Evaluación de Schengen"; no obstante, la ACC-Schengen lamentaba no haber podido participar más activamente en dicho proceso de evaluación, pudiendo realizar ella misma los controles pertinentes en cada país.

* CUESTIONARIOS DE EVALUACIÓN DE SEGURIDAD

A raíz de una inspección que realizó cada una de las autoridades de control sobre sus propios ficheros nacionales del SIS, la ACC-Schengen observó que los resultados obtenidos eran en algunos casos difícilmente comparables, ya que las inspecciones realizadas en cada país diferían en contenido y profundidad. Por ello, se observó la necesidad de elaborar una lista de controles, en relación con el cumplimiento del artículo 118.1 del Convenio de Schengen relativo al cumplimiento de medidas de seguridad, que pudiera ser utilizada por cada autoridad de control nacional cuando procediera a revisar la seguridad de sus ficheros nacionales del SIS. Esta lista de controles fue elaborada por la delegación española, tomando como referencia los propios estándares de inspección que aplica la Agencia de Protección de Datos, la cual fue aprobada en sesión plenaria por la ACC-Schengen con el fin de que sirviera como referencia a las autoridades nacionales en la realización de las inspecciones sobre los ficheros del SIS.

* USURPACIÓN DE IDENTIDAD

Uno de los problemas que ha analizado la ACC-Schengen en diferentes ocasiones es el caso de aquellas personas cuya identidad es usurpada y cuyos datos son introducidos en el SIS con el fin de localizar o identificar al usurpador; es decir, en estos casos el SIS contiene una descripción de identidad que no se corresponde ni de facto ni de iure con la identidad real de la persona buscada, introduciéndose además los datos de las personas afectadas sin que se les notifique dicha inclusión.

Analizado nuevamente el caso por la ACC-Schengen se completó un dictamen emitido anteriormente, recalcando que en estos casos el tratamiento de datos de los afectados sólo debería permitirse previa autorización libre y explícita de dichas personas o a petición concreta de la persona afectada. También se contemplaba la posibilidad de contar con medidas tales como disponer de un documento aparte del pasaporte, en que constara que su titular no es la persona usurpadora.

* CREACIÓN DE UNA SECRETARÍA COMÚN

El 17 de octubre de 2000 el Consejo de la Unión Europea adoptó una Decisión, que será aplicable a partir del 1 de septiembre de 2001, por la que se crea una Secretaría para las Autoridades comunes de control de protección de datos establecidas por el Convenio Europol, Convenio de Schengen y Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros. Según esta Decisión, la Secretaría desempeñará las funciones asignadas a cada una de las secretarías de las diferentes Autoridades comunes de control.

* PRESENTACIÓN DEL INFORME DE ACTIVIDADES

En la sesión plenaria de la ACC-Schengen celebrada en octubre de 2000, esta Autoridad prestó en conferencia de prensa su cuarto informe de actividades que cubría el periodo comprendido entre marzo de 1999 a febrero de 2000. De entre las actividades que se destacaban en ese informe cabe señalar: la inspección que se había realizado en el CSIS en el año 1999; los dictámenes y recomendaciones emitidos relacionados con la seguridad de las Oficinas SIRENE (encargadas del intercambio de información entre oficinas policiales), con la conservación de los expedientes manuales una vez que las descripciones son eliminadas del SIS y sobre los datos de las personas cuya identidad es usurpada con finalidad delictiva.

La Agencia de Protección de Datos siempre divulgaba el informe de la ACC-Schengen incluyéndolo en su Memoria anual, pero en este caso no fue posible debido al retraso que sufrió su publicación, por ello esta Agencia lo difundió remitiéndolo a los Ministerios de Justicia, Interior y Exteriores, así como a la Comisión Constitucional del Congreso de los Diputados.

5. AUTORIDAD COMÚN DE CONTROL DE EUROPOL

El Convenio basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol), cuya adopción recomienda el Consejo de la Unión Europea en su Acto 95/C 316/01, de 26 de julio de 1995 y que fue ratificado por el Reino de España en el año 1997, tiene como objetivos, según establece su artículo 2, *"(...) mejorar, en el marco de la cooperación entre los Estados miembros de conformidad con el punto 9 del artículo K.1 del Tratado de la Unión Europea, por medio de las actividades que se enumeran en el presente Convenio, la eficacia de los servicios competentes de los Estados miembros y la cooperación entre los mismos con vistas a la prevención y lucha contra el terrorismo, el tráfico ilícito de estupefacientes y otras formas graves de delincuencia inter-*

nacional, en la medida en que existan indicios concretos de una estructura delictiva organizada y que dos o más Estados miembros se vean afectados por las formas de delincuencia antes mencionadas, de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados miembros" .

Para ello, según se describe en el artículo 6, *" 1. Europol gestionará un sistema informatizado de recogida de datos que constará de los siguientes elementos:*

1) El sistema de información contemplado en el artículo 7, de contenido limitado y definido con precisión, que permitirá una rápida consulta de la información existente en los Estados miembros y en Europol.

2) Los ficheros de trabajo contemplados en el artículo 10, que se crearán, por un plazo variable, a efectos de análisis y contendrán información pormenorizada.

3) Un sistema de índice que contendrá entradas de los ficheros de análisis a que se refiere el punto 2, según lo dispuesto en el artículo 11.

2. El sistema informatizado de recogida de datos empleados por Europol no deberán en ningún caso conectarse a otros sistemas de tratamiento automatizado, exceptuado el sistema de tratamiento automatizado de las unidades nacionales ".

Por ello, el Convenio Europol también establece unos requisitos mínimos en materia de protección de datos personales que deberán cumplir los Estados Miembros que sean parte del mismo. En concreto, cada parte deberá adoptar las disposiciones nacionales necesarias para conseguir un nivel de protección de datos que sea, como mínimo, equivalente al resultante de los principios del Convenio del Consejo de Europa de 28 de enero de 1981 (Convenio 108), teniendo en cuenta la Recomendación R(87) 15, de 17 de septiembre de 1987, del Comité de ministros del Consejo de Europa encaminada a regular la utilización de datos de carácter personal en el sector de la policía (Articulo 14 del Convenio Europol).

Además, en el artículo 24, se crea una Autoridad Común de Control independiente cuyo cometido será vigilar la actividad de Europol, con el objeto de garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que dispongan los servicios de Europol no vulneren los derechos de las personas y controlar la licitud de la transmisión de los datos que procedan de Europol. Esta Autoridad Común de Control estará integrada, como máximo, por dos miembros o representantes de las autoridades nacionales de control (la Agencia de Protección de Datos en el caso español).

Si tuviéramos que elegir un hecho que caracterizara la actividad de la Autoridad Común de Control de Europol (en adelante, ACC-Europol), durante el año 2000, podríamos decir que este fue el año en que por primera vez se realizó una inspección, una auditoría, a los sistemas de información de Europol.

Para ello, la ACC-Europol otorgó un mandato a un Grupo de Inspección en el que participaron expertos de las autoridades de control alemana, británica, española, griega y neerlandesa para que planificaran y, posteriormente, realizaran dicha visita de control a la sede de Europol en La Haya.

El objetivo de la inspección era auditar, con carácter general, las medidas globales de seguridad implantadas por Europol y, de manera más específica, la adecuación del Sistema de Ficheros de Trabajo con fines de Análisis a los requerimientos que para el mismo marca el Convenio Europol.

Con esta finalidad, el Grupo de Inspección celebró tres reuniones preparatorias en las que se diseñó el enfoque del trabajo de auditoría y se desarrollaron los documentos de trabajo que se utilizarían durante el control en La Haya, realizándose la inspección durante los días 8, 9 y 10 de noviembre.

Como resultado de la misma, se elaboró un informe provisional de inspección en el que se hacían constar los resultados de la auditoría. Dicho informe se presentó el 12 de diciembre al plenario de la ACC-Europol quien decidió, a propuesta del Grupo de Inspección, remitirlo a Europol para que dicho organismo realizara los comentarios que creyera oportunos y, de esta manera, garantizar la correcta interpretación de los hechos que en el mismo se reflejaban. Una vez que se reciban dichos comentarios, el Grupo de Inspección confeccionará el informe definitivo en el que se harán constar las recomendaciones que se juzguen necesarias y que elevará a la ACC-Europol para su aprobación definitiva y para que decida, a la vista de su contenido, las siguientes actuaciones que se deban realizar.

No obstante, dado que, por un lado, se prevé la puesta en marcha de nuevos sistemas de información por parte de Europol y, por otro lado, se hará necesario comprobar la implantación de las recomendaciones que se efectúen, está previsto realizar una nueva auditoría en el segundo semestre del año 2001.

Por lo que respecta a la actividad de la ACC-Europol en otros campos, a finales del año 1999 se constituyó por un periodo limitado de tiempo un Grupo de Trabajo para diseñar y proponer una planificación de la actividad de la ACC-Europol para el bienio 2000-2001. El resultado de los trabajos de dicho grupo (en el que participaban representantes de las delegaciones alemana, británica, española y neerlandesa), se plasmó en un informe que fue presentado a la ACC-Europol en su reunión de 3 de febrero y que, tras recoger los comentarios realizados en dicha reunión por las distintas delegaciones, se presentó a la ACC-Europol en su versión definitiva en la reunión de 12 de abril, en la que fue aprobado por la misma, disolviéndose el Grupo de Trabajo de Planificación.

El objetivo de la planificación delineada en el documento confeccionado por el Grupo de Planificación y aprobado por la ACC-Europol es establecer un sistema eficaz de protección de datos que permita hacer valer suficientemente los

derechos de las personas cuyos datos obran en los sistemas de Europol. Sobre la base de este planteamiento, se trazó un sistema que permitiera a la ACC-Europol desarrollar su trabajo de forma eficiente. El sistema elegido es la constitución, cuando las circunstancias así lo requieran, de grupos de trabajo de entre tres y cinco miembros, ya sea con carácter temporal o permanente, que prepararían el trabajo haciendo las propuestas que creyeran oportunas o preparando los borradores de diversos documentos que, posteriormente, se presentarían a la ACC-Europol para su discusión y, en su caso, aprobación.

Una vez aprobado este sistema de trabajo, se constituyeron diversos Grupos de Trabajo para abordar las distintas áreas en las que la ACC-Europol debía actuar. A continuación se detallan las actividades más relevantes de cada uno de ellos, de las que se fueron dando cuenta en las cinco reuniones (febrero, abril, junio, octubre y diciembre) celebradas por la ACC-Europol en el año 2000, a excepción de las ya referidas del Grupo de Planificación y del Grupo de Inspección.

El Grupo de Trabajo de Ficheros de Análisis fue el primero que se constituyó, habiendo iniciado su actividad ya en 1999, y su misión es examinar las Órdenes de Creación de Ficheros de Trabajo con Fines de Análisis que, conforme al artículo 12.1 del Convenio, Europol debe remitir a la ACC-Europol para recibir su dictamen. A lo largo del año 2000 este Grupo de Trabajo ha informado a la ACC-Europol de todas aquellas dificultades que observaba en las distintas Órdenes y, a raíz de estas observaciones y de las realizadas por el resto de las delegaciones en las reuniones de la ACC-Europol, se han ido formulando los distintos dictámenes y, en su caso, solicitando a Europol las aclaraciones que se han considerado oportunas.

El Grupo de Trabajo de Publicidad tiene como misión fomentar el conocimiento de los derechos que el Convenio Europol otorga a los ciudadanos en relación con el derecho fundamental a la protección de datos personales que son tratados en los sistemas de información creados en el marco de dicho Convenio. Para ello, intenta difundir, de la manera más amplia posible, la existencia de la ACC-Europol como garante de dichos derechos y de las actividades que la misma realiza en defensa de los mismos. Durante el año 2000 sus esfuerzos han ido encaminados a la consecución del objetivo de que la ACC-Europol pueda disponer de un espacio propio en Internet y al diseño del logotipo de la misma para resaltar su carácter independiente y no vinculado a Europol.

El Grupo de Trabajo de Procedimientos se encarga de todos aquellos asuntos relacionados con las normas y procedimientos que Europol debe aplicar en materia de consulta de datos personales, comunicación con terceros Estados y organizaciones y el ejercicio del derecho de acceso, entre otros temas relevantes. No obstante, el trabajo de este grupo se centró, a lo largo del año 2000, en la confección de los borradores de los dictámenes preceptivos no vinculantes que la ACC-Europol debe elaborar con carácter previo al establecimiento de negociaciones entre Europol y estados y organismos terceros.

En efecto, el artículo 18.2 del Convenio Europol, al tratar de la transmisión de datos a estados y organismos terceros, establece: *"El Consejo, de conformidad con el procedimiento previsto en el Título VI del Tratado de la Unión Europea y habida cuenta de las circunstancias contempladas en el apartado 3, fijará por unanimidad las normas generales para la transmisión por Europol de datos personales a terceros Estados y organismos a tenor del apartado 4 del artículo 10. El Consejo de Administración preparará la decisión del Consejo y consultará a la autoridad común de control contemplada en el artículo 24"*. Posteriormente, en el artículo 2.1 del Acto del Consejo 1999/C 88/01, de 12 de marzo, por el que se fijan las normas para la transmisión por Europol de datos personales a Estados y organismos terceros, se dispone que *"En las condiciones establecidas en el artículo 18 del Convenio Europol, Europol podrá transmitir datos personales a un Estado u organismo tercero cuando medie alguna de las circunstancias siguientes: a) Un acuerdo entre Europol y un tercer Estado u organismo tal como se contempla en el artículo 3 del presente acto; b) excepcionalmente, en caso de que el director considere que la transmisión de datos resulta absolutamente necesaria para salvaguardar los intereses fundamentales de los Estados miembros de que se trate dentro del ámbito de los objetivos de Europol o a fin de prevenir un peligro inminente de comisión de delito"*. Además, en el apartado 4 del artículo 3 de este mismo Acto, se establece la obligatoriedad de consultar a la ACC-Europol previamente a la aprobación de cualquier acuerdo con un Estado u Organismo tercero.

Finalmente, la Decisión del Consejo 2000/C 106/01, de 27 de marzo de 2000, por la que se autoriza al Director de Europol a entablar negociaciones sobre acuerdos con terceros Estados y organismos no relacionados con la Unión Europea, dispone, en el apartado 5 del artículo 1, que *"No obstante, cuando se trate de un acuerdo que incluya la transmisión de datos personales por parte de Europol a Estados y organismos terceros, el Director de Europol podrá entablar negociaciones únicamente después de que el Consejo decida, por unanimidad, basándose en un informe que le presentará el Consejo de administración de Europol, que no existe ningún obstáculo para dar comienzo dichas negociaciones. El Consejo de administración consultará al órgano común de control sobre estos informes (...)"*.

Por ello, la ACC-Europol ha debido pronunciarse sobre la existencia de obstáculos insalvables para el comienzo de las negociaciones con diversos Estados y organismos terceros, señalando, al mismo tiempo, aquellos puntos en los que no parecía que existiera una protección adecuada a la vista de la legislación y práctica en materia de protección de datos en los mismos y en los que, por lo tanto, sería conveniente introducir las necesarias garantías cuando se negociaran los acuerdos pertinentes entre Europol y la tercera parte.

Durante el año 2000, la ACC-Europol ha evacuado dictámenes en relación con el comienzo de las negociaciones con la Organización Internacional de Policía Criminal (Interpol), Noruega, Islandia, Polonia, Hungría, Eslovenia y Eslovaquia, en los cuales, aparte de realizar alguna de las puntualizaciones mencionadas en el párrafo anterior y señalar las condiciones generales que deberían regir los intercambios de datos con dichos terceros, la ACC-Europol no ha objetado el comienzo de negociaciones con dichos Estados y organismos terceros.

En otro orden de cosas, también se constituyó un Grupo de Trabajo sobre Tecnologías de la Información -del que forma parte la delegación española-, cuya misión consiste en el seguimiento de los desarrollos tecnológicos que se vayan produciendo en Europol para que, de esta manera, la ACC-Europol pueda dar una opinión temprana sobre si se ajustan o no a las disposiciones sobre protección de datos del Convenio Europol y, en caso de no ser así, formular las observaciones oportunas que ayuden a resolver las deficiencias observadas. También es función del mismo prepara los borradores de dictamen que sobre esta materia le sean solicitados a la ACC-Europol por parte de Europol.

La actividad de este subgrupo se centró en la obtención de información en el marco de la inspección realizada a Europol puesto que se consideró la forma más adecuada de proceder, dado que la mayor parte de la información técnica relevante está contenida en documentos a los que se les ha asignado una marca de nivel de seguridad, lo que dificulta su consulta y distribución fuera de la sede de Europol. En este sentido, se produjo una entrevista con representantes de Europol que informaron de los planes para los próximos meses, entre los que se encontraba la puesta en marcha de un Sistema de Información Provisional (en el marco de lo establecido en los artículos 7 a 9 del Convenio), sobre el cual se solicitó el dictamen de la ACC-Europol mediante una carta de 8 de diciembre de 2000, del Presidente del Consejo de Administración de Europol al Presidente de la ACC-Europol, borrador de dictamen que será presentado en la primera reunión de la ACC-Europol del año 2001 por el Grupo de Tecnologías de la Información.

Igualmente, en la misma carta, se solicitaba otro dictamen relativo a un Proyecto de Decisión de Europol respecto a los informes sobre las consultas realizadas al Sistema de Información Provisional, según se prevé en el artículo 16 del Convenio. Este proyecto de dictamen también será presentado al plenario de la ACC-Europol en su primera reunión del año 2001.

Por otra parte, el Grupo de Tecnologías de la Información también presentó al plenario de la ACC-Europol otro proyecto de dictamen, que fue aprobado por unanimidad, sobre las reglas que debían regir el acceso de las Autoridades Nacionales de Control a los ficheros en los que se registran los accesos de los Funcionarios de Enlace destacados en Europol por los Estados Miembros y que se basaba en el hecho de que la comprobación de la licitud de la introducción de un dato personal en el Sistema de Información debería correr a cargo de la Autoridad de Control del Estado Miembro que lo introdujo y la verificación de la legalidad del tratamiento de un dato personal por una fuerza policial de un determinado Estado Miembro, debería correr a cargo de la Autoridad de Control de dicho Estado, independientemente del Estado que haya introducido el dato en el sistema.

Por lo que respecta a la actividad del Comité de Recursos establecido en el apartado 7 del artículo 24 del Convenio Europol para tramitar y decidir sobre los posibles recursos presentados por los afectados frente a decisiones de Europol en las que se les deniegue el acceso, rectificación o supresión de sus datos personales, dado que no se han presentado recursos de este tipo ante la ACC-Europol durante el año 2000, ésta se ha limitado a terminar de redactar el documento que debe regir determinados aspectos procedimentales de la tramitación de dichos recursos.

6. SISTEMA DE INFORMACIÓN ADUANERO

El Convenio establecido sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la tecnología de la información a efectos aduaneros (en adelante Convenio SIA), establecido por el Acto del Consejo 95/C 316/02, de 26 de julio de 1995, crea, en su artículo 2, un sistema común automatizado de información a efectos aduaneros, denominado Sistema de Información Aduanero. La gestión de la infraestructura técnica del SIA será garantizada por la Comisión de las Comunidades Europeas *"(...) de conformidad con las normas que establecen las disposiciones de aplicación adoptadas por el Consejo" (Artículo 3.2 del Convenio SIA)* .

El apartado 2 de dicho artículo 2 establece como objetivo del SIA *"(...) contribuir a prevenir, investigar y perseguir las infracciones graves de las leyes nacionales, aumentando, mediante la rápida difusión de información, la eficacia de los procedimientos de cooperación y control de las administraciones aduaneras de los Estados miembros".*

Asimismo, en su Capítulo VI establece las normas por las que se debe regir la protección de datos personales en el ámbito del Convenio. Concretamente, en el artículo 13 se establece que *"El Estado miembro que quiera obtener o introducir datos personales en el Sistema de Información Aduanero deberá adoptar, antes de la fecha de entrada en vigor del presente Convenio, las disposiciones legales nacionales que se precisen para alcanzar un nivel de protección de los datos personales equivalente, como mínimo, al que resulta de los principios rectores del Convenio de Estrasburgo de 1981".* Esta previsión es similar a las establecidas en los Convenios de Schengen y Europol.

Además, se garantiza el ejercicio de los derechos de acceso, rectificación y cancelación de acuerdo con la normativa vigente en el Estado miembro en que se invoque el derecho así como a obtener una compensación por los posibles perjuicios achacables a la utilización del SIA (artículos 15 y 21 del Convenio).

Adicionalmente, el apartado 3 del artículo 13 dispone que *"A fin de garantizar la correcta aplicación de las disposiciones del presente Convenio en materia de protección de datos personales, el Sistema de Información Aduanero se considerará en cada Estado miembro como un fichero nacional de datos, sujeto a las disposiciones nacionales mencionadas en el apartado 1 y a cualquiera otra más estricta contenida en el presente Convenio"* .

Igualmente, siguiendo la estructura del resto de instrumentos legales existentes en el marco del III Pilar, se constituye una Autoridad de Supervisión Común, *"(...) compuesta por dos representantes de cada Estado miembro elegidos entre la autoridad o autoridades nacionales de supervisión independientes" (artículo 18.1 Convenio SIA)*, en el caso español,

la Agencia de Protección de Datos. Dicha Autoridad de Supervisión Común *" (...) estará facultada para supervisar el funcionamiento del Sistema de Información Aduanero, examinar todas las dificultades de aplicación o interpretación que puedan surgir en su funcionamiento, estudiar los problemas que puedan platearse en el ejercicio de la supervisión independiente por parte de las autoridades nacionales de supervisión de los Estados miembros o en el ejercicio del derecho de acceso de las personas al Sistema y elaborar propuestas de solución común a los problemas"* .

Por lo que respecta a la situación actual, España ratificó el Convenio SIA en julio de 1999, al igual que el Protocolo Adicional por el que los Estados miembro acuerdan que el Convenio pueda empezar a aplicarse de forma provisional a partir del primer día del tercer mes siguiente al depósito del instrumento de aprobación, aceptación o ratificación del Acuerdo por parte del octavo Estado miembro parte del mismo. Esta situación se produjo el día 1 de noviembre de 2000, lo que implica que ha de constituirse la Autoridad de Supervisión Común prevista en el artículo 18.

En previsión de esta situación y como ya se informó en la anterior edición de esta Memoria, en 1998, la Presidencia Británica se dirigió al Grupo de Trabajo de Ficheros Policiales para que, teniendo en cuenta que la Autoridad de Supervisión Común estaría formada, con toda probabilidad, por representantes de las Autoridades Nacionales de Control en materia de protección de datos existentes en los Estados miembros, elaborara un borrador de Reglamento Interno para la futura autoridad común. Dichos trabajos se finalizaron en el mes de marzo de 1999, en el que se produjo el acuerdo de todas las delegaciones participantes en el Grupo de Trabajo sobre una Posición Común para dicho Reglamento, texto que deberá ser adoptado por la nueva Autoridad de Supervisión Común, cuya constitución está previsto se produzca en los primeros meses del año 2001.

7. GRUPO DE PROTECCIÓN DE DATOS EN TELECOMUNICA-CIONES (GRUPO DE BERLÍN)

En el año 2000 ha habido dos reuniones del Grupo de Berlín. La primera reunión se celebró en el mes de mayo en Grecia y la segunda tuvo lugar en el mes de septiembre en Berlín. En ambas participaron representantes de autoridades de control de países de la Unión Europea, de Europa Central y Oriental y de Nueva Zelanda.

En la reunión de Grecia se aprobaron seis documentos de posiciones comunes (ver Anexo) que llevan por títulos:

- "Posición Común relativa a aspectos de Privacidad y Protección de Datos en la Publicación de Datos Personales contenidos en documentos públicamente disponibles en Internet".

- "Posición Común relativa a aspectos de Privacidad y Protección de Datos en el Registro de Nombres de Dominios en Internet"

- "Posición Común sobre el establecimiento de perfiles on-line en Internet"

- "Posición Común sobre Privacidad y gestión de los Derechos de Autor (Copyright)"

- "Posición Común sobre los Intermediarios de la Información (Infomediarios) - un modelo de negocio respetuoso con la de "

- "Posición Común sobre la de detección del fraude en las telecomunicaciones"

En la reunión de Berlín se aprobaron dos documentos (ver anexo) de posiciones comunes que llevan por título:

- "Posición Común relativa a aspectos de protección de datos en el borrador de Convenio sobre cibercrimen del Consejo de Europa"

- "Posición Común sobre la incorporación de principios específicos de telecomunicaciones en acuerdos de privacidad multilateral".

Además de las posiciones comunes aprobadas se trataron otros temas de interés que se resumen a continuación.

Se realizó un seguimiento de los trabajos que se están desarrollando en el marco del Consejo de Europa con el fin de elaborar un documento que recoja una serie de medidas para luchar contra el *cibercrimen* en el también denominado *ciberespacio*. El objetivo de este documento, que se encuentra en fase de elaboración, es armonizar las diferentes normativas nacionales sobre crimen informático y fomentar la cooperación entre las autoridades nacionales para luchar contra este tipo de delitos. Desde el punto de vista de protección de datos se quiere seguir los desarrollos de los trabajos con el fin de que el documento final no recoja aspectos que supongan un detrimento de los principios y garantías de protección de la intimidad, especialmente con los aspectos relativos al trazado, registro y periodos de retención de las operaciones realizadas por los usuarios. Estos trabajos dieron lugar a una posición común del grupo aprobada en la reunión de Berlín.

Respecto de los registro públicos, el representante de Nueva Zelanda informó del proyecto del gobierno de su país de fomentar la administración electrónica, proyecto que tiene una de sus bases en permitir el acceso a determinados registros públicos a través de Internet. A este respecto la autorid de control de Nueva Zelanda ha manifestado su preocupación al respecto estableciendo cuatro recomendaciones:

* que los principios de privacidad de los registros públicos se reformen en el sentido de que el acceso a dichos registros

sea consistente con el principio de finalidad;

* que se restrinjan los accesos masivos a la información personal de los registros públicos.

* que cualquier decisión sobre la puesta en Internet de cualquier registro público esté amparada en una decisión del Parlamento y no en una mera decisión de la Administración.

* que se realice una valoración acerca del impacto en la privacidad de los principales proyectos tecnológicos que se desarrollen.

Respecto a problemas relativos a la publicación de datos personales en Internet, se ha informado al resto del grupo del caso acaecido en España donde una ONG publicaba una lista de funcionarios de las fuerzas y cuerpos de seguridad del estado implicados en denuncias relativas a torturas, dándose la circunstancia de que en determinados casos los funcionarios implicados habían sido declarados inocentes por los tribunales. En este caso, el Director de la Agencia ordenó la cesación del tratamiento consistente en la comunicación de dicha lista a través de Internet, ya que la LOPD establece, en el apartado 5 de su artículo 7 que los datos relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros mantenidos a tal efecto por las Administraciones Públicas competentes.

Se ha puesto en conocimiento del resto del Grupo que en virtud de lo establecido en los artículos 3.j), 28, 30, 31 y Disposición Transitoria Segunda de la LOPD se posibilita la creación de un nuevo fichero, llamada Censo Promocional, formado únicamente por los datos de nombre y domicilio obrantes en el Censo Electoral, que, una vez se proceda a su regulación por medio del no reglamento, podrá ser utilizado con fines comerciales. No obstante, la norma recoge el derecho del ciudadano, ejercitable de forma completamente gratuita, a no figurar en dicha lista.

También, se ha puesto en conocimiento del grupo lo recogido en la LOPD sobre las fuentes accesibles al público. Un aspecto sobre el que se hizo una mención especial fue el periodo máximo de validez para las distintas ediciones y versiones de las fuentes accesibles al público establecido en el artículo 28 de la LOPD. En virtud del mismo, se limita a un año el carácter de fuente accesible al público de aquellas obtenidas por vía telemática en formato electrónico y a la última edición de la misma en el caso de las que se editen en un soporte que haga imposible su modificación (papel, CD-ROM, etc.).

En relación con el acceso a datos personales por las fuerzas y cuerpos de seguridad, el representante noruego planteó el litigio habido en su país entre el principal proveedor de acceso a Internet y las autoridades policiales que reivindicaban el acceso a los datos asociados a los número IP, entre ellos el número de teléfono. El litigio ha sido resulto por el Tribunal Supremo que ha sentenciado que este tipo de información debe ser entregada a las autoridades policiales que la requieran, aunque no se disponga del consentimiento previo del afectado y sin necesidad de mandamiento judicial.

Respecto de desarrollos normativos relativos a la interceptación de comunicaciones, el Parlamento del Reino Unido ha aprobado una normativa al respecto. Esta normativa permite la interceptación de comunicaciones en las redes públicas y extiende su ámbito de aplicación a Internet. En este caso, la interceptación se realiza a través de un dispositivo denominado *"caja negra"* que el proveedor de acceso debe instalar en sus sistemas, si es requerido para ello, y sin necesidad de mandamiento judicial.

La norma sobre interceptación en el Reino Unido contempla también aspectos de cifrado, incluyendo la potestad de acceder a la información sin cifrar o bien a las claves utilizadas en el cifrado. La Autoridad de Control del Reino Unido ha expresado su preocupación sobre el impacto que esta potestad puede tener en la privacidad y en la seguridad, preocupación que se acrecienta por el hecho de que la norma recoge que cuando un empleado sea requerido para facilitar las claves utilizadas en su empresa, el empleado no puede ponerlo en conocimiento de la misma.

Respecto al periodo de retención asociado a los datos de tráfico y facturación el representante alemán expuso que según la legislación actualmente en vigor en su país dicho plazo es de 80 días, desde la emisión de la factura, pero que previsiblemente se ampliará a 6 meses según el borrador de la nueva Ley de Protección de Datos en Telecomunicaciones que se está tramitando actualmente.

Respecto a la situación en el Reino Unido, su representante expuso que no existe ninguna obligación legal que permita a los PSI (proveedores de acceso a Internet) retener los datos de tráfico para simplemente atender las solicitudes realizadas por las fuerzas y cuerpos de seguridad. No obstante, desde dichas instituciones, se está intentando que el gobierno introduzca una previsión legal que obligue a los PSI a retener los datos de tráfico por un periodo de 7 años. Según el representante británico, el gobierno de su país está desempeñando una actitud activa en este terreno mediante la participación en el grupo G8, fomentando el llegar a un consenso sobre el periodo de retención de la información con fines policiales.

En esta materia el representante noruego expuso que recientemente las autoridades de telecomunicaciones han distribuido una propuesta para ser comentada por las autoridades policiales y los operadores. Uno de los puntos de la propuesta es el relativo al periodo de retención de los datos de tráfico donde parece perfilarse que no será superior a tres meses a contar desde el momento en que se produce la llamada.

Respecto a nuevos desarrollos normativos el representante noruego informó que el Ministerio de Justicia se encuentra elaborando una regulación específica en materia de seguridad que se espera esté aprobada en los primeros meses de 2001.

Respecto de la seguridad, el representante sueco informó que la autoridad de control de protección de datos sueca ha elaborado unas recomendaciones al respecto.

A continuación se incluyen los textos completos de las Posiciones Comunes aprobados por el Grupo durante el año 2000.

Posición Común relativa a aspectos de Privacidad y Protección de Datos en la Publicación de Datos Personales contenidos en documentos disponibles al público en Internet

Con la creciente utilización de Internet, la publicación de datos personales en documentos (oficiales) disponibles al público en la red se ha incrementado de forma espectacular en los últimos años como por ejemplo: sentencias judiciales, información de registros públicos y otros documentos oficiales.

El hecho de que estos documentos se encuentren actualmente disponibles al público a nivel global y de forma electrónica hace que surjan nuevas y específicas amenazas para la intimidad de las personas afectadas.

El Grupo de Trabajo quiere poner de manifiesto que las Autoridades de Protección de Datos, a través del "Grupo del artículo 29", han mantenido una "Reunión de Trabajo sobre la protección de las personas en relación con el tratamiento de datos personales", en la que se han tratado con profundidad estos temas y cuyas conclusiones han quedado recogidas en la Opinión 3/99 sobre Protección de Datos Personales e Información en el Sector Público, respaldando este Grupo de Trabajo la totalidad de su contenido.

Posición Común relativa a la Protección de la Intimidad y los Datos Personales en los Registros de Nombres de Dominio de Internet Con la creciente utilización de Internet, cada vez más personas están empezando a registrar sus propios nombres de domino en los diferentes Centros de Información de Red nacionales e internacionales (NIC en inglés). En el procedimiento de registro de un nombre de dominio, los NICs recogen datos personales de los solicitantes (tales como nombre, dirección y número de teléfono), que de forma regular quedan disponibles al público en las bases de datos denominadas "WhoIs-databases" de la Red. En la mayoría de los países, la recogida y publicación de estos datos es imprescindible para registrar un nombre de dominio debido a las condiciones de servicio impuestas por los respectivos NICs.

Originariamente, la finalidad de estas bases de datos era facilitar el mantenimiento técnico de la Red, (por ejemplo para contactar con la persona que administra un dominio cuando se producían errores y se obstaculizaba el funcionamiento de la red). No obstante, el desarrollo de la Red, que se ha convertido en la columna vertebral de la emergente "Sociedad de la Información", ha creado nuevos intereses en la utilización de estos datos por parte de las diferentes partes implicadas:

Así por ejemplo, diversas Autoridades Públicas utilizan estas bases de datos para combatir el fraude y la publicación de contenidos ilegales en la Red.

Más recientemente, la Organización Mundial de la Propiedad Intelectual (WIPO en inglés) ha publicado un informe para la "Organización de Internet para la Asignación de Nombres y Números" (ICANN) sobre los derechos de propiedad intelectual en la gestión de nombres y direcciones de Internet. Este organismo ha sugerido, entre otras cuestiones, recoger en la lista de dominios genéricos de primer nivel (en inglés generic Top Level Domains o gTLD), los nombres de dominio de segundo nivel con sus datos personales asociados y su publicación en una base de datos accesible al público en Internet, con el fin de posibilitar a los titulares de derechos de propiedad intelectual encontrar y contactar con los titulares de un dominio en caso de violación de sus derechos.

Este enfoque también se refleja en la Declaración sobre Políticas de Acreditación de Registros del ICANN, que exige haber registrado los nombres de dominio genérico de primer nivel (gTLD) con el fin de disponer de información precisa de contacto de sus solicitantes y proporcionar acceso público a esos datos en tiempo real (de igual manera que en el servicio WhoIs).

Al mismo tiempo, la publicación del nombre y dirección del titular de un nombre de dominio puede ser útil para cualquier usuario de Internet que considere vulnerada su intimidad, ya sea por la publicación de sus datos personales en una página web o por el uso indebido de dichos datos personales por parte del titular del nombre de dominio. Por otro lado, al no existir obligación en todos los países de publicar el nombre y dirección del titular del servicio en su página Web, la publicación de estos datos por los NICs nacionales podría ser un prerequisito, con el fin de que los usuarios pudieran ejercer sus derechos de privacidad ante el proveedor del servicio.

No obstante, la recogida y publicación de datos personales de los titulares del nombre de dominio origina en si misma problemas de privacidad y de protección de datos.

La necesidad de proteger a las personas ha sido reconocida desde hace más de veinte años por las legislaciones nacionales de protección de datos, al igual que por la comunidad internacional (por ejemplo, en las directrices de la OCDE de 1980 sobre Protección de la Intimidad, en el Convenio 108 del Consejo de Europa y, más recientemente, en la Directiva 95/46/EC del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre protección de las personas en relación con el tratamiento de datos personales y su libre circulación). Estas regulaciones recogen principios básicos comunes sobre el correcto tratamiento de la información personal. Entre estos principios se encuentra la obligación de informar a las personas sobre el tratamiento de sus datos personales, y la limitación de la recogida y uso de los datos personales a las finalidades informadas así como la protección contra usos distintos.

La importancia de la protección de la intimidad para el desarrollo fructífero de la Sociedad Global de la Información ha sido reconocida en los documentos de desarrollo del Comercio Electrónico; por ejemplo, en el denominado "Estructura para el Comercio Electrónico Global" elaborado por Estados Unidos, o en la declaración conjunta de Estados Unidos y Europa sobre Comercio Electrónico, en la Iniciativa Europea sobre Comercio Electrónico y en la Conferencia Ministerial de la OECD de octubre de 1998, celebrada en Ottawa.

El actual Acuerdo para la Acreditación de Registros (AAR) desarrollado por ICANN no refleja de una forma suficientemente clara el objetivo de la protección de los datos personales de los titulares de nombres de dominio. Por este motivo, el Grupo de Trabajo ha elaborado las siguientes recomendaciones para que sean tenidas en cuenta en futuras versiones de dicho Acuerdo:

Se considera esencial que se especifiquen las finalidades por las que se recaban y se publican los datos personales de los titulares de nombres de dominio.

Se deben de restringir a lo estrictamente necesarios, de acuerdo con su finalidad, los datos personales recabados y publicados en el proceso de registro de un nombre de dominio. A este respecto, el Grupo de Trabajo manifiesta sus reservas sobre la publicación obligatoria de cualquier dato a excepción del nombre (que puede ser también el nombre de una compañía y no el de una persona física), dirección y dirección de correo electrónico, en aquellos casos donde el titular del nombre de dominio no sea responsable del mantenimiento técnico del dominio, por ser éste realizado por un proveedor de servicio (como es el caso de la mayoría de personas que han registrado nombres de dominio).

Cualquier otro dato (especialmente el número de teléfono o de fax), aunque el registro considere necesario recogerlo para su finalidad, debería referirse al proveedor del servicio respectivo o publicarlo si se dispone del consentimiento explícito del afectado. La publicación obligatoria de los números de teléfono y de fax, de los titulares de nombres de dominio puede ocasionar problemas cuando los solicitantes son personas físicas, al obligarles a proporcionar el número de teléfono de su domicilio particular. El derecho a la no publicación del número de teléfono, reconocido en la mayoría de las legislaciones nacionales en materia de protección de datos en las telecomunicaciones, debería respetarse también en estos casos.

Al mismo tiempo, cualquier uso subsiguiente incompatible con la finalidad inicialmente especificada (por ejemplo, marketing) debería disponer del consentimiento informado del afectado. Bajo estas consideraciones, el nivel de protección a la intimidad garantizado por el presente acuerdo AAR (punto II.F.6.f) no parece suficiente.

Cualquier mecanismo técnico que pueda ser introducido para acceder a los datos recogidos debe disponer de las salvaguardas necesarias para satisfacer el principio de sujeción a la finalidad con la que se recogieron y evitar la posibilidad de un uso posterior no autorizado de los datos del afectado. Este requisito no se satisface por ninguna de las bases de datos del tipo *"Whols"*, disponibles al público, donde las búsquedas no están sujetas a ninguna restricción. Bajo esta consideración, el Grupo de Trabajo da la bienvenida a las iniciativas que sobre la materia ha elaborado WIPO, que en su informe sobre Tratamientos de Nombres de Dominio en Internet, recoge que los datos de contacto de los titulares de dominios permanezcan disponibles únicamente para los fines marcados, así como tomar las medidas oportunas para disuadir de la utilización con fines no autorizados, como por ejemplo, con fines comerciales. El Grupo de Trabajo subraya la necesidad de desarrollar mecanismos de filtrado en las interfaces de acceso a la base de datos para garantizar la sujeción a la finalidad.

El Grupo de Trabajo recomienda además que, en ausencia de una legislación a nivel internacional de protección de datos, los registros desarrollen un estándar para la recogida y uso de los datos personales de los titulares de nombres de dominio, que incluyan procedimientos para informar a los afectados acerca de la finalidad y usos posteriores de los datos personales recogidos, así como del derecho de acceso y rectificación sobre dichos datos. La adhesión a estos estándares debería quedar garantizada a través de mecanismos de certificación.

El Grupo de Trabajo resalta que cualquier registro que opere bajo la jurisdicción de una norma de protección de datos existente y que lleve a cabo un procedimiento de registro de nombres de dominio a nivel nacional, está sujeto a la legislación existente en materia de protección de datos y privacidad y al control de la correspondiente autoridad nacional de Protección de Datos.

Al mismo tiempo, el Grupo de Trabajo apoya los esfuerzos de la Comisión Europea para fortalecer la protección de la privacidad y de los datos personales, en el sistema de gestión de nombres de dominio de Internet para beneficio de todos los ciudadanos y anima a la Comisión Europea a continuar sus conversaciones con ICANN, el Gobierno estadounidense y las demás partes implicadas.

Posición Común relativa a la obtención de Perfiles en las conexiones a Internet

- Los proveedores de servicio de Internet deberán informar a los usuarios sobre el tipo, alcance, lugar, duración del almacenamiento, finalidad de la recogida, tratamiento y uso de sus datos cuando se recaben con fines de realizar perfiles. Esta información debería ser proporcionada incluso en el caso de que los datos sean recogidos utilizando seudónimos o números de identificación antes de que sean personalizados.

- Los usuarios deberán ser informados, por quienes realicen perfiles, con anterioridad a la activación de los mecanismos o "cookies" utilizados al efecto.

- Los usuarios deberán tener el derecho a elegir sobre el tratamiento que se de a sus datos, al menos la opción a oponerse. En este caso los proveedores deberán garantizar a los usuarios que los datos acerca de sus últimos movimientos en Internet no van a ser utilizados para la definición de perfiles.

- Los usuarios deben disponer del derecho a revocar su consentimiento en cualquier momento sin efectos retroactivos.

- La personalización de perfiles de usuario requiere el consentimiento previo e informado del afectado.

- El Grupo de Trabajo considera esencial que terceras partes independientes verifiquen que quienes realicen perfiles cumplen con los principios de privacidad y protección de datos.

- Los usuarios deben tener derecho a comprobar en cualquier momento, y de forma gratuita, los perfiles que sobre ellos se hayan elaborado. Los Servicios de creación de Perfiles tendrán que proporcionar acceso directo a los datos almacenados sobre los usuarios. Si el perfil es recogido utilizando seudónimos, los usuarios deben tener la oportunidad de acceder, rectificar y cancelar sus datos sin revelar su verdadera identidad.

- Los proveedores de servicios que realicen perfiles deberán implantar las medidas de seguridad adecuadas.

Posición Común relativa a Privacidad y Gestión de los derechos de Propiedad Intelectual (Copyright)

Siempre se había considerado que el derecho a la propiedad intelectual (Copyright) y el derecho a la privacidad presentaban un origen común. Así, Warren y Brandeis se refirieron al derecho consuetudinario en la protección de la propiedad intelectua establecieron los fundamentos del "derecho a la privacidad" de las personas. Sin embargo, en el marco del comercio electrónico a través de Internet, el derecho a la propiedad intelectual y el derecho a la privacidad parecen entrar en conflicto.

Mientras que en mundo analógico, o tradicional, la regulación sobre la propiedad intelectual proporcionó exenciones a la utilización no comercial de la privacidad, en el mundo digital, o *on-line*, la normativa de propiedad intelectual cubre cada acto de reproducción temporal y cada transferencia a la memoria RAM del ordenador con el fin de lectura, escucha o visualización. El autor de una obra digital (incluyendo programas de ordenador y bases de datos) tiene el derecho a prohibir o a cobrar por cualquiera de estos fines.

En parte, el problema en la práctica tiene relación con la escasez de mecanismos fiables de pago, que garanticen la privacidad y que estén disponibles en Internet. Se podrían ofrecer mecanismos de pago anónimo que permitirían la descarga o utilización de la obra digital justo después del pago.

Con la finalidad legítima de proteger la propiedad intelectual en el ciberespacio y prevenir la piratería informática, las tecnologías de protección de los derechos de propiedad intelectual, tales como los robots ("web spiders"), pueden identificar obras digitales y otros elementos protegidos, pudiendo remitir informes a servidores centrales acerca de la obra que es utilizada o copiada, o bien, solicitar los correspondientes permisos o el pago de los derechos. Se están diseñando Sistemas de Gestión del Copyright Electrónico (SGCE o ECMS en inglés) que podrían conducir a una vigilancia completa de los usuarios a través del seguimiento en la utilización de las obras digitales. Algunos SGCE registran cada vez que cualquier persona lee, escucha o visualiza algo en Internet, recogiendo información muy personal sobre los usuarios de la Red..

Los SGCE no se utilizarán en gran medida por las personas que tengan derechos de propiedad intelectual, sino por grandes editoriales e intermediarios (representantes de titulares de derechos) con un gran interés en vigilar el comportamiento de los usuarios con otros fines no relacionados con la protección de los derechos de propiedad intelectual (por ejemplo, para marketing directo). Como contraste, en el mundo analógico, nadie almacena datos personales sobre quién está leyendo un libro y cuántas veces lo hace. En este sentido, no sólo está en juego la intimidad, sino también la libertad de expresión y de información.

Cada vez se utiliza más información relativa a la gestión de derechos con el fin de proteger la propiedad intelectual. Entre esta información se encuentran las marcas de agua digitales y otras técnicas que identifican la propiedad intelectual de la obra. Esta información se encuentra protegida por las disposiciones que sobre la materia recoge el Tratado de 1996 de la Organización Mundial de la Propiedad Intelectual (WIPO), que tiene como objetivo prevenir la vulneración de la propiedad intelectual. No obstante, la información de gestión de derechos puede constituir por si misma información personal, como por ejemplo si contiene la identidad del comprador o usuario o las condiciones de licencia personalizada. Por lo tanto puede ser utilizada para recoger y distribuir información de identificación personal sobre las actividades que realizan las personas en la red.

Las actuaciones tendentes al borrado de esta información o para evitar que los robots ("web spiders") busquen dicha información, incluso para fines de publicidad directa, podrían ser consideradas como una vulneración ilegal de las tecnologías de protección de los derechos de propiedad intelectual.

El control sobre la circulación de una obra digital puede crear un rastro de una persona identificable. Bajo estas condiciones es preferible, desde una perspectiva de protección de la intimidad, bloquear el acceso a las obras sujetas a derechos de propiedad intelectual mediante, por ejemplo, el uso de cifrado, ya que no se necesita registrar el comportamiento del usuario.

Los sistemas nacionales utilizados para bloquear ciertos contenidos ilegales que siguen el modelo de búsqueda e

incautación, podrían ser utilizados no sólo para la prevención de infracciones a los derechos de propiedad intelectual, sino también para prevenir el acceso a material disponible en la red y cuyo contenido puede ser ilegal bajo determinadas legislaciones nacionales. No obstante, estos sistemas que están siendo considerados actualmente, puede dar lugar a vulneraciones en el secreto de las comunicaciones y serían de escasa efectividad debido a la arquitectura de Internet.

Con el fin de encontrar un equilibrio justo entre los titulares de derechos de propiedad intelectual y la privacidad de los usuarios, el Grupo de Trabajo quiere hacer una llamada a los diseñadores, productores y proveedores de SGCE para:

1. Diseñar, producir y proporcionar SGCE que no recojan información personal y que permitan las transacciones anónimas o mediante seudónimo. El Grupo de Trabajo reafirma en este contexto, que en su opinión, los usuarios deberían tener la opción de acceder a Internet sin tener que revelar su identidad, cuando los datos personales no sean necesarios para proporcionar determinados servicios. Bajo determinadas condiciones, la utilización de seudónimos podría proteger la privacidad del usuario y, al mismo tiempo, preservar los intereses económicos de los titulares de derechos de propiedad intelectual: las marcas de agua digitales podrían contener códigos de transacción por los cuales se numerarían las copias individualizadas, enlazándose éstos números con usuarios individuales en una base de datos segura, por ejemplo, bajo la titularidad de un tercero de confianza. Esta base de datos sólo se consultaría para proteger los derechos de propiedad intelectual como por ejemplo, ante la solicitud de un juez.

2. Informar con la mayor transparencia posible a los usuarios sobre los tratamientos de los datos personales (incluidos los seudónimos), relacionados con las obras digitales y los sistemas de gestión de sus derechos de propiedad intelectual. El Grupo de Trabajo se adhiere a la Recomendación 1/99 sobre el *"Tratamiento Automatizado e Invisible de Datos Personales en Internet realizado mediante programas de ordenador y equipos especializados",* adoptada por el Grupo de Trabajo Europeo sobre la Protección de las Personas en relación con el Tratamiento de los Datos Personales. Lo anterior es de aplicación también al tratamiento de datos personales en relación con la obra digital.

Las técnicas de filtrado y de exploración utilizadas para vigilar los contenidos conducen a intrusiones en la privacidad y en el secreto de las telecomunicaciones. El Grupo de Trabajo no las considera, por lo tanto, adecuadas para prevenir vulneraciones de los derechos de propiedad intelectual.

La protección de la propiedad intelectual por medios que respeten la intimidad del individuo es esencial para el desarrollo del comercio electrónico global. Por lo tanto, se hace necesario un acuerdo internacional, bien dentro del marco de trabajo de WIPO, o mediante la definición de estándares, que resuelva los problemas de la protección internacional de los derechos de propiedad intelectual mediante la utilización de tecnologías avanzadas de privacidad.

Posición Común relativa a

Los "Informediarios" -¨ un modelo de negocio respetuoso con la intimidad?

Desde 1996 el Grupo de Trabajo ha remarcado la necesidad de desarrollar medios técnicos que mejoren la privacidad de los usuarios en Internet, especialmente facilitándoles opciones de acceso a Internet sin tener que revelar su identidad, allí donde los datos personales no son necesarios para proporcionar el servicio. El Grupo también ha recomendado medidas para que se diseñen agentes de software inteligentes y respetuosos con la intimidad. En paralelo con lo anterior ha surgido un modelo de negocios que consiste en proporcionar a los usuarios la opción de "enmascarar" su identidad mientras navega por la Web.

John Hagel y Marc Singer han definido los *infomediarios* como *"agentes o intermediarios que ayudan a los clientes a maximizar el valor de sus datos".* Bajo su punto de vista, los infomediarios están mejor equipados que los agentes de software para servir los intereses de los usuarios o clientes. También afirman que *"Muchos consumidores son reticentes a divulgar detalles privados de sus vidas y permitir que cualquier entidad electrónica pueda exponer su información de una forma inadecuada, mientras se mueven por la Web ".* Los vendedores que estaban insatisfechos con los agentes de software que sólo comparaban precios descubrieron maneras de bloquearlos en sus sitios Web. Por otro lado, un infomediario actuaría como un agente o guardián, en nombre de sus clientes, representando encarecidamente sus intereses y ayudándoles a optimizar el valor que reciben de los vendedores. Mediante la agregación de información y utilizando el poder de compra de un conjunto numeroso de clientes, reunidos en un "club de compra virtual", los infomediarios podrían crear un "mercado inverso".

Al mismo tiempo los infomediarios recogerían información detallada de sus clientes sobre sus preferencias con el fin de encontrar los sitios Web que más les convengan. Un infomediario - según Hagel/Singer - sólo conseguiría un perfil de información extenso y profundo del cliente con la garantía de proteger esta información frente al abuso, y realizar cesiones de los datos personales únicamente con el consentimiento expreso del cliente ("consentimiento para marketing"). Para este fin, el infomediario ofrecería dos herramientas: una herramientas de privacidad y una herramienta de establecimiento de perfiles. La herramienta de privacidad incluiría direcciones de correo electrónico anónimas junto con software de filtrado que impediría los ataques de correos no solicitados ("spams"); también podría proporcionar facilidades para la supresión de "cookies" tales como los "cortadores de cookies". Respecto de la herramienta de establecimiento de perfiles, el infomediario ofrecería la posibilidad de utilizar cookies para que los clientes mantuvieran un rastro de sus propios comportamientos o de sus compras cuando están conectados a la Red ("cookies inversas"). En definitiva, el infomediario ofrecería una facilidad tecnológica para proteger la privacidad de sus clientes y para "envolverlos en el anonimato"".

Por otro lado, la facilidad de establecimiento de perfiles permitiría construir una visión más completa e integrada de las

transacciones y preferencias de los clientes. Los infomediarios serían capaces incluso de unir la información sobre actividades "on-line" en la red con informaciones relativas a transacciones convencionales efectuadas fuera de la red (por ejemplo, utilizando una tarjeta de crédito). Estos perfiles pueden ser dinámicos, por ejemplo, si se crean utilizando datos sobre actividades que realizan otros clientes con similares perfiles y preferencias. Del mismo modo, los perfiles sobre los vendedores pueden ponerse a disposición de los clientes, dándoles información sobre el número de transacciones realizadas a través de servicios de infomediarios (por ejemplo, ordenadores vendidos de un cierto tipo) y el número de reclamaciones y de devoluciones del producto al vendedor.

El cliente de un infomediario tiene la opción de permanecer anónimo o de permitir que su perfil y sus datos personales se entreguen a los vendedores o empresas de marketing directo. En el último caso, el cliente recibirá pequeños reembolsos en efectivo, un descuento en el precio del producto, acceso libre o más barato a Internet u otros beneficios. Los clientes que elijan permanecer totalmente en el anonimato no recibirán estos pagos o beneficios pero asegurarían su privacidad.

Algunos infomediarios ya están operando en la Web siguiendo este modelo de negocio con algunas modificaciones. Ofrecen servicios que van desde la protección de los niños en la Web (PrivaSeek) hasta las agencias matrimoniales y de contacto personal en la red (yenta.com; flirtmaschine.de). Algunas ofrecen monederos electrónicos que permiten al usuario rellenar formularios con información personal y controlar el uso de esta información.

Recomendaciones:

- En principio, hay que recibir con agrado el hecho de que la privacidad esté ganando terreno en el mercado y que sea tomada por algunos creadores de negocios en Internet como una fuente de negocio. No obstante, el consumidor necesita recursos legales efectivos en caso de que el infomediario utilice los datos de forma desleal. Un modelo de negocio no puede reemplazar los derechos legales de los afectados, si bien, es un ejemplo positivo de cómo las fuerzas del mercado pueden acogerse a un marco legal existente.

- Debe permanecer la libertad de decisión del afectado acerca de si desea vender o no el derecho a la utilización de sus datos de carácter personal. Algunos infomediarios (por ejemplo las agencias matrimoniales) manejan información extremadamente sensible. Además, los afectados no siempre son consumidores; pueden participar por ejemplo, en actividades políticas en la web y tener que considerar cuidadosamente si contratan un agente para tales funciones.

- La capacidad de creación de perfiles de los infomediarios apunta a la importancia de confianza en las relaciones con el cliente. Se asemeja a la relación cliente-abogado o a la relación de confianza entre médico y paciente. El legislador debería considerar proteger de forma adecuada dicha relación.

- Finalmente, los infomediarios, en tanto crean perfiles personales, debrían respetar los principios acordados por el Grupo de Trabajo en su "Posición Común relativa a la creación de perfiles en las conexiones a Internet" de fecha 5 de mayo de 2000.

Posición Común relativa a

la detección del fraude en las telecomunicaciones

El Grupo de Trabajo Internacional sobre Protección de Datos en las Telecomunicaciones quiere llamar la atención sobre los aspectos de protección de datos relacionados con la detección del fraude de las telecomunicaciones, en particular los relativos al tratamiento de los datos de tráfico por parte de los operadores de telecomunicaciones.

El término fraude se utiliza en este documento en el sentido de "usos fraudulentos de los servicios de telecomunicaciones" más que en el de "actividades fraudulentas utilizando las redes de telecomunicaciones ("hacking o pirateo informático", etc.). Los tipos de fraude en las telecomunicaciones analizados inciden negativamente en los operadores de telecomunicaciones, pues los servicios utilizados que no son pagados o lo son parcialmente, implican una pérdida de ingresos.

Es difícil de evaluar la magnitud del fenómeno del fraude, en términos de pérdida económica para el operador. No obstante, se estima dicha pérdida entre el 3 y el 6% de los ingresos mundiales. Parece claro que el crecimiento de los niveles del fraude debe preocupar a la mayoría de los operadores, especialmente desde que el margen de los servicios de telecomunicaciones ha decrecido como consecuencia de la liberalización de este mercado. Por esta circunstancia, existe un gran interés entre los operadores de telecomunicaciones en limitar este tipo de fraude.

Tipos generales de fraude

Existen dos tipos generales de fraude:

Fraudes en la tasa de operación por venta de llamadas. Consiste en la reventa de llamadas a terceras personas sin pagar al operador el tasa establecida por las mismas. Existen distintas variantes: a menudo mediante "locutorios telefónicos", llamadas a través de equipos móviles o construidos de forma específica.

Fraudes en Servicios con Tarifas Especiales. Se incluyen algunos tipos de fraudes relacionados con números pertenecientes a tarifas especiales y de elevado coste (los típicos números "novecientos"). Algunas veces se explota el número de tal forma que se hacen las llamadas mediante la utilización fraudulenta de teléfonos que generan ingresos para un

número determinado. Una variante consiste en tener cómplices que participan en el fraude conectando teléfonos, por ejemplo, después de las horas de oficina, a dichos números. Otra opción es "incitar" a que la gente haga llamadas a estos números especiales sin que se den cuenta de ello. El defraudador recoge los ingresos procedentes de todas estas actividades.

Métodos para cometer fraude

Las principales formas de cometer fraude son:

Fraude en la contratación. Se obtiene un alta en el servicio a través del proceso normal bajo una identidad robada o falsa. Es posible también que los empleados de un operador de telecomunicaciones participen en este tipo de fraude, por ejemplo, saltándose deliberadamente los procedimientos para revisar la identidad de los nuevos clientes.

"Surfing". Bajo este término se incluyen varias formas de utilización no autorizada de los servicios:

- Clonación de los terminales. Se duplican identidades, teléfonos y otros atributos.

- Fraude en las tarjetas de llamada. Incluyendo el robo o fraude de los códigos PIN y las tarjetas de recarga.

- Uso incorrecto de equipos. Se incluyen algunas formas de intrusismo en las redes de comunicaciones. Una vez introducidos en la red, se utiliza ésta sin pagar. Se puede acceder a la red mediante puertos que se mantienen abiertos en las centrales telefónicas o PBX, números de entrada, sistemas de correo vocal, etc.

- Utilizando la línea de otro abonado mediante la conexión física a la misma.

Fraude en los teléfonos móviles.

En las comunicaciones móviles aparecen nuevas formas de fraude, entre las que se encuentran las siguientes: la forma más simple consiste en el robo de un teléfono móvil, otra forma de fraude tiene que ver con el servicio de itinerancia (roaming), en este servicio las llamadas de alto coste se hacen desde un país extranjero produciéndose un gran retraso hasta la facturación de esas llamadas en el país donde el teléfono está registrado; también se han detectado casos de recargas y falsificación de tarjetas de prepago, así como diversos tipos de fraude en los servicios a través de las conexiones.

Métodos para detectar el fraude

La lucha contra el fraude implica su detección. En esta sección se darán algunas indicaciones sobre el funcionamiento de los métodos de detección de fraudes y del tipo de datos que se utilizan en estas técnicas.

La mayor parte de los datos utilizados para la detección del fraude utilizan los denominados Registros de Detalle de Llamadas (CDR) y los datos de facturación. Los CDR constituyen una colección de datos enviados por la red a través del sistema de señación. Estos datos contienen el numero llamante y el número llamado, la hora y duración de la llamada y otros datos necesarios para la comunicación. El sistema de facturación evalúa los CDR y a partir de ellos elabora la factura individual de cada cliente.

Aproximadamente, se pueden agrupar los sistemas de detección de fraude en varios tipos:

- Análisis simple de los informes sobre tráfico de datos (CDR) y datos de facturación. Esto implica el análisis de los informes y búsqueda de situaciones atípicas.

- Mediante herramientas automáticas para analizar CDR basadas en un conjunto de reglas prefijadas. Pueden aplicarse mientras la comunicación se mantiene o una vez ésta ha finalizado. Esta técnica ofrece más flexibilidad que el simple análisis, además de contar con la posibilidad de adaptar las reglas. Suelen utilizar típicamente sistemas expertos.

- Sistemas automáticos complejos con algunas capacidades para aprender y crear nuevas reglas de detección por sí mismos. Las técnicas involucradas utilizan redes neuronales, algoritmos genéticos y data warehousing/data mining.

Datos utilizados para la detección de los fraudes

Algunos de los tipos de datos más utilizados por los sistemas de detección de fraude son los siguientes:

* Consumos altos

* Incrementos de consumo

* Consumos sospechosos, como por ejemplo incrementos fuertes de consumo asociados a servicios con tarifas especiales.

* Llamadas de larga duración, como por ejemplo llamadas de más de ocho horas

* Destinos extranjeros sospechosos, en tanto que son habituales en cuanto a fraude

* Utilización de servicios de elevado coste y en los que existe gran incidencia de fraude

* Perfiles de usuario, que se dividen en clases con diferentes valoraciones de riesgo.

* Patrones de llamadas

Los operadores afirman que necesitan recoger datos detallados durante largos periodos de tiempo con el fin de ajustar y configurar sus sistemas de detección de fraude y que cuando aplican técnicas de "data mining" u otras comparables, la calidad de la detección del fraude mejora con el paso del tiempo. Esto les lleva a mantener una historia completa del comportamiento de sus abonados. Como regla general, cuanto más complejo y adaptable sea el sistema de detección de fraudes, más datos deben recogerse y más tiempo deben mantenerse para su análisis.

Aspectos sobre protección de datos La detección de fraudes implica algunos riesgos para la privacidad. Clientes inocentes puede ser tratados como defraudadores potenciales y existe el riesgo de tomar decisiones equivocadas y de que los datos procesados con la finalidad de detección de fraude se utilicen ilegalmente, o que la transferencia y uso de estos datos por terceros (policía y servicios secretos) pueda estar bajo el control de los operadores.

Dadas las actividades de los operadores de telecomunicaciones para la detección de los fraudes cabe preguntarse dónde se debe situar el límite legal. Los métodos de detección se basan en el análisis de los datos de tráfico, que son considerados en un sentido general como datos de carácter personal. Por lo tanto, el procesamiento de los datos de tráfico debería con la normativa sobre protección de datos personales.

Visto desde la perspectiva de los operadores de telecomunicaciones, la letra de las normativas aplicables deja lugar para la interpretación acerca de cuales son los datos que legítimamente puede recoger, tratar y almacenar. Lo mismo aplica respecto al periodo de retención de dichos datos.

Recomendaciones:

- En general, son preferibles los métodos para limitar los riesgos financieros tales como los sistemas de prepago, el acortamiento de los períodos de facturación o las garantías en los pagos a los métodos a-posteriori de control o análisis de los comportamientos personales.

- El uso de sistemas de detección de fraude debería limitarse a aquéllas circunstancias donde se ha demostrado que las medidas preventivas para minimizar los riesgos no han sido eficaces. No puede admitirse la finalidad de detectar el fraude como una justificación general para la retención completa de los datos de tráfico durante períodos prolongados de tiempo.

- Los sistemas de detección de fraudes son muy diversos y los datos considerados como necesarios para su detección varían ampliamente, dependiendo del tipo de fraude y de las tecnologías aplicadas a su detección. Cada tipo de fraude debe tratarse de forma que sea lo más respetuosa posible con la intimidad, por ejemplo, el fraude en la contratación debería de limitarse mejorando los procedimientos para revisar las credenciales del contratante.

- En caso de que los sistemas de detección de fraude tomen decisiones de forma automática, los sujetos afectados por dichas decisiones deberán ser informados de ello y se les debe de facilitar los medios adecuados para su impugnación.

Posición Común relativa al Tratamiento de la Protección de Datos **en el borrador de Convenio sobre Delito Informático (Cyber-crimen) que está elaborando el Consejo de Europa.**

Introducción

El Consejo de Europa está desarrollando una Convención sobre el delito informático o "Cyber-crimen", con el fin de hacer más efectivas las investigaciones y procedimientos relativos a los delitos informáticos y para permitir la recopilación de evidencias electrónicas en dichos delitos. Los principales países no europeos, como EE.UU., Canadá, Japón y Sudáfrica están participando también en la elaboración del borrador. Se espera que la Convención finalice en Diciembre del año 2000 y que se firme en septiembre de 2001. El borrador permite también la incorporación a cualquier otro país que sea invitado por el Comité de Ministros. El Consejo de Europa ha declarado que busca mejorar el proceso de consulta con las partes interesadas, ya sean públicas o privadas.

El Grupo de Trabajo reconoce que existe una necesidad de luchar contra el crimen informático a nivel internacional, y que se necesita un reforzamiento de la cooperación internacional en la era de las redes de comunicación globales, así como que las diferentes fuerzas y cuerpos de seguridad de cada país necesitan disponer de los medios apropiados de lucha contra este tipo de delitos. Por otro lado, dichas medidas deben ser equilibradas con otros derechos ya establecidos, como el derecho a la privacidad y al secreto de las telecomunicaciones.

Si bien la Convención sobre Asistencia Mutua en Asuntos Penales entre los Estados Miembros de la Unión Europea regula expresamente la protección de datos personales (art. 23), el presente borrador sobre delito informático no contiene ninguna referencia a la normativa sobre Protección de Datos. Así, no se contempla, de una manera clara y sin ambigüedad, como vulneración a dicha normativa el acceso injustificado a los sistemas de información.

El Consejo de Europa tiene una larga tradición en el desarrollo de normas de protección de datos. Parece, por tanto, apropiado que el nuevo convenio expresamente se refiera al Convenio 108 para la Protección de las Personas en relación con el Tratamiento de Datos Personales de 1981; y a la Recomendación número R(95) 4 de la protección de datos personales en el área de los servicios de telecomunicación. El Grupo de Trabajo considera necesario que el Comité de Expertos en Protección de Datos participe en las reuniones posteriores de elaboración del borrador.

Nuevos Procedimientos

La Convención sobre delito informático trata de introducir nuevos procedimientos que permitan la persecución de crímenes relacionados con la utilización de Internet, incluyendo medidas que obliguen a los proveedores de servicios de telecomunicaciones, a almacenar datos personales de las comunicaciones realizadas por las redes (tanto datos de tráfico como de contenido), y a que dichos datos estén disponibles para las autoridades nacionales y extranjeras involucradas en procesos e investigaciones criminales.

Ha sido objeto de discusión en el pasado, y en diferentes contextos, el que los Proveedores de Servicio de Internet y de Telecomunicaciones deban almacenar datos sobre el tráfico de Telecomunicaciones y de Internet, durante un amplio período de tiempo, con el fin de que dicha información se encuentre disponible para el caso de que se produjera un delito durante dicho periodo. El Grupo de Trabajo considera estas medidas desproporcionadas y por lo tanto inaceptables y subraya que los datos de tráfico están protegidos por el principio de confidencialidad, de la misma forma que los datos de contenido (Artículo 8 de la Convención Europea de los Derechos Humanos). En este sentido, el Grupo de Trabajo apoya completamente las declaraciones de la Conferencia Europea de Autoridades de Protección de Datos, que en su reunión celebrada en Estocolmo los días 6 y 7 de abril de 2000, establecieron que la recopilación de datos de tráfico por parte de los Proveedores de Servicio de Internet puede suponer una vulneración de los derechos fundamentales de la persona garantizados por la Convención Europea de los Derechos Humanos. También, iría en contra de la Recomendación 3/99 sobre la conservación de los datos de tráfico por parte de los Proveedores de Servicio de Internet, para fines policiales adoptada por el Grupo de Trabajo del Artículo 29 de Autoridades Europeas de Protección de Datos.

Lo expuesto en el párrafo anterior también se aplicaría respecto al almacenamiento de datos que revelen el uso que cada persona realiza de Internet.

El Grupo de Trabajo considera que no debería de extenderse la utilización de mecanismos de rastreo de delitos de forma que invada la privacidad, hasta que la utilidad de tales mecanismos no haya sido demostrada de forma fehaciente.

El Grupo de Trabajo ha declarado con anterioridad que cualquier interceptación de una comunicación privada debería estar sujeta a las debidas garantías (Posición Común sobre la responsabilidad pública en relación con la interceptación de comunicaciones privadas; adoptada en la vigesimotercera Reunión en Hong Kong SAR, China, el día 15 de abril de 1998). También desea expresar que se deben respetar las condiciones y garantías proporcionadas por las legislaciones nacionales y por la Convención sobre Asistencia Mutua en Asuntos Penales de los Estados Miembros de la Unión Europea (Art. 23). Tales condiciones y garantías deberían al menos incluir:

* autorización judicial previa,

* (posterior) notificación a los afectados,

* limitación en los usos,

* almacenamiento de los registros sujeto a condiciones,

* control y auditoría

* informe público de las actuaciones practicadas.

Por lo tanto, tales garantías deberían también ser incorporadas en el Borrador de Convenio sobre Delito Informático. En particular, la cooperación de las autoridades nacionales con los operadores de redes públicas y privadas debería basarse preferentemente, sobre obligaciones legales más que sobre acuerdos voluntarios que son muy difíciles de controlar.

Nuevos Delitos

Al mismo tiempo, el Convenio trata de cubrir nuevos tipos delictivos que todavía no han sido incorporados por la mayoría de los países miembros del Consejo de Europa en sus respectivas legislaciones penales.

La incorporación de nuevos delitos en la legislación penal tiene que realizarse de forma extremadamente cuidadosa, pues una excesiva proliferación de estos nuevos delitos, así como la penalización de los intentos y colaboraciones en ellos, podría conducir a un detrimento considerable de los estándares de primera para todos los usuarios de las redes de telecomunicaciones, produciendo una enorme cantidad de datos personalizados relativos a la utilización de las redes de telecomunicaciones e Internet, y la consiguiente supresión del derecho a la utilización anónima de tales servicios. Podría considerarse que las regulaciones previstas pueden llevar a la necesidad de personalizar cada acción individualizada de cada usuario en la red global, lo que claramente resulta desproporcionado.

En relación con los delitos informáticos que son tratados en los Artículos 1 al 13, especialmente los de penalización de los *"dispositivos ilegales"* (artículo 6), los de *"Intromisión en los datos"* y de *"Intromisión en los sistemas"* (artículos 4 y 5), el Grupo de Trabajo considera que las obligaciones que se imponen a los proveedores de servicio al exigirles la adopción de ciertas medidas de seguridad cuando conecten sus sistemas a la red pública, con el fin de incrementar el nivel de seguridad de Internet, serán, en general, más adecuadas para luchar contra el Delito Informático, que la simple introducción de nuevos delitos que se relacionan con un amplio conjunto de actividades de Internet y que podrían incluso ir en detrimento de las medidas que intentan mejorar la seguridad de la red.

Posición Común relativa a Los principios básicos de privacidad en las telecomunicaciones para su incorporación en acuerdos multilaterales en la materia.

Entre las principales ideas expuestas en el discurso que Michael Kirby, Juez del Tribunal Supremo Australiano y miembro del Grupo de Expertos en Privacidad de la OCDE, dirigió a los asistentes a la Conferencia de Autoridades de Protección de Datos celebrada en 1999 en Hong Kong, se incidía en la necesidad de establecer nuevos principios de privacidad en consonancia con la tecnología actual. Estas consideraciones sirvieron de incentivo para que el Grupo de Trabajo Internacional estudiara cuales serían los principios fundamentales relativos a la privacidad en las telecomunicaciones dentro de la actual sociedad de la información, con vistas a su incorporación en acuerdos nacionales o internacionales sobre la materia.

El siguiente texto constituye una primera aproximación a la cuestión planteada y resume sus resultados en principios que pueden ser integrados en acuerdos ya existentes o ser adoptados como anexos a los mismos. El texto recoge las ideas que el juez Kirby planteaba en su discurso.

Diez mandamientos para proteger la privacidad en el mundo de Internet

- **División de poderes en el mundo de la información:** Los Proveedores de Servicios y los proveedores de Red no deben interferir con el contenido de la información, salvo cuando una Ley explícitamente lo indique. En la medida en que los Proveedores de Red y los de Servicio proporcionen contenidos por si mismos, las responsabilidades por sus respectivas funciones se deberán tener en cuenta por separado.

- **Secreto en las Telecomunicaciones:** Los Proveedores de Servicio y de Red no deben revelar ninguna información sobre el contenido o sobre los datos de tráfico excepto en los casos en que la Ley explícitamente lo indique.

- **Austeridad de Datos:** Las infraestructuras de Telecomunicaciones deben ser diseñadas de forma que su utilización requiera de la mínima cantidad de datos personales posible en la medida en que técnicamente pueda hacerse.

- **Derecho al anonimato:** Los Proveedores de Servicios y de Red deben de ofrecer a cualquier usuario la opción de utilizar la red o los accesos a los servicios de forma anónima o bien utilizando seudónimos, o caso no deben ser revelados salvo en aquellos casos en que una Ley explícitamente lo determine.

- **Derecho virtual a la no injerencia (virtual right to be alone):** Nadie debe ser obligado a que sus datos personales sean publicados en directorios u otros repertorios. Todo usuario debe tener el derecho de impedir que sus datos sean recogidos por algún motor de búsqueda o por cualquier otro tipo de agentes. Todo usuario debe tener el derecho y los medios técnicos precisos para impedir la intrusión de software externo dentro de sus propios equipos.

- **Derecho a la seguridad:** Todo usuario debe disponer del derecho y de los medios técnicos necesarios para comunicar sus contenidos de forma confidencial mediante la utilización de métodos efectivos como el cifrado.

- **Restricción de usos secundarios:** Los datos de tráfico no deben ser utilizados para otros fines distintos de los necesarios para el funcionamiento de la red o de los servicios sin el consentimiento explícito del usuario.

- **Transparencia:** Los Proveedores de Servicio y de Red deben de publicar, de forma comprensible, la información que permita a los usuarios conocer la estructura de la red o del servicio, las respectivas responsabilidades, la cantidad de datos personales que vayan a ser tratados y las cesiones previstas.

- **Acceso a los datos personales:** Todo usuario debe disponer del derecho a ser informado de todos los datos personales que vayan a ser tratados sobre su persona para la prestación por la red del servicio.

- **Resolución de reclamaciones internacionales:** De cara a los aspectos internacionales de las redes y servicios, todo usuario debe disponer del derecho a presentar sus reclamaciones ante un que disponga de competencias de investigación y sanción internacional si la normativa nacional no garantiza suficientemente sus derechos.

El Grupo de Trabajo hace un llamamiento a las organizaciones internacionales y a las agencias públicas y privadas para incorporar estos principios en sus políticas y en sus normativas reguladoras.

8. GRUPO DE TRABAJO SOBRE FICHEROS POLICIALES DE LOS COMISIONADOS EUROPEOS DE PROTECCIÓN DE DATOS

Tras la gran actividad desarrollada por este Grupo de Trabajo en los años anteriores, fundamentalmente estructurada en torno a los debates sobre el Reglamento Interno de las Autoridades Comunes de Control de Europol y Sistema de Información Aduanero, durante el año 2000 sólo se produjo una reunión del mismo. Ello se debió, fundamentalmente, a que muchos de los temas de debate en el seno del Grupo se han ido trasladando a los órganos formales de control establecidos por los Convenios relativos a materias del III Pilar, esto es, las Autoridades Comunes de Control de Schengen, Europol y, en un futuro cercano, Sistema de Información Aduanero, por lo que no ha resultado necesario utilizar el Grupo de Ficheros Policiales con vistas a adoptar posturas armonizadas por parte de las Autoridades de Control nacionales. Es de prever que esta tendencia continúe en el futuro por lo que, de no aparecer nuevas áreas de interés en estos sectores, es posible que el mismo Grupo decida su disolución.

No obstante lo anterior, el Grupo se encontró una vez en el año 2000 en una reunión que resultó de tremendo interés y que sirvió de base para la preparación de un informe que se presentó en la Conferencia de Primavera de Autoridades de Control Europeas, celebrada en Estocolmo, y que, a su vez, fue el fundamento para la Declaración de Estocolmo sobre la retención de datos de tráfico por parte de los Proveedores de Acceso a Internet, que se reproduce en el apartado dedicado a dicha Conferencia dentro de este documento.

De hecho, durante la misma se estudiaron las distintas iniciativas que en aquellos momentos se estaban llevando a cabo para proporcionar nuevos instrumentos para luchar contra lo que se ha dado en llamar "cibercrimen" o "ciberdelitos", esto es, aquellos delitos tradicionales que utilizan las modernas redes de telecomunicaciones y las facilidades de las nuevas tecnologías de la información para la comisión de los mismos o aquellas nuevas formas de delincuencia aparecidas como consecuencia de la existencia de las susodichas capacidades tecnológicas.

Estos ciberdelitos se pueden categorizar en cuatro tipos principales: la intrusión en sistemas de información para la obtención de información sensible o valiosa, el uso de las nuevas tecnologías para facilitar la comisión de delitos, publicación de material ilegal en la Red (por ejemplo, pornografía infantil) y la puesta en marcha de planes financieros fraudulentos a través de Internet.

Puesto que aunque es evidente que el Derecho nacional de cada país es aplicable para castigar estas formas de criminalidad, la mayor parte de estos delitos tienen, hoy en día, una naturaleza internacional por el desarrollo global de Internet y otras redes de telecomunicaciones, lo que hace imposible que un país sólo pueda obtener resultados positivos en la lucha contra los crímenes de alta tecnologías, por lo que se están desarrollando aproximaciones internacionales para luchar contra estos ciberdelitos.

En concreto, en la reunión del Grupo de Ficheros Policiales, se discutieron las iniciativas, en gran medida convergentes, existentes dentro del G8 (Principios y Plan de Acción), el Consejo de Europa (Convenio sobre Cibercrimen) y la Unión Europea (Plan ENFOPOL), todas ellas coincidentes en armonizar y dotar de nuevos instrumentos legales a las fuerzas de seguridad de los países incluidos en estos foros (G8, UE, Noruega, Australia y Nueva Zelanda, fundamentalmente).

Las principales novedades que aparecían en los planes antes mencionados se pueden concretar en las llamadas "Órdenes de Preservación", que permitirían a las fuerzas de seguridad solicitar a un Proveedor de Servicios de Internet (PSI) la conservación de datos que pudieran servir como evidencia hasta que se consiguiera la orden judicial que permitiera el acceso a los mismos; la posibilidad de un rastreo rápido de los enlaces entre ordenadores situados en distintos países (conocido por "Trap and Trace") contando con la colaboración de los distintos PSI implicados en la comunicación; la "Preservación Futura", que permitiría solicitar a un PSI que, a partir de un determinado momento, se almacenaran todos los datos relativos a las comunicaciones de una persona específica, para que, una vez se produjeran dichas comunicaciones se enviara al PSI una Orden de Preservación; la "Preservación Rutinaria" que impondría a los PSI la obligación de conservar, con carácter general, los datos de tráfico de las personas por un periodo mayor del necesario para la facturación de los servicios por si fueran necesarios en una investigación policial posterior y la posibilidad de dotar a las fuerzas de seguridad con las llamadas "Interfaces de Interceptación" en los locales de los PSI o, incluso, "Interfaces de Interceptación Virtuales" en las oficinas de las propias fuerzas de seguridad, permitiéndoles un acceso completo en tiempo real al tráfico de Internet que sucediera en dichos PSI, que debería ser únicamente utilizado con las debidas garantías pero que, por su propia naturaleza, resultaría muy difícil de controlar.

Aunque, como no podía ser de otra manera, los Comisionados Europeos de Protección de Datos coinciden plenamente en la necesidad de luchar contra cualquier forma de delito, sí que han puesto de manifiesto en repetidas ocasiones en que los instrumentos que se utilicen en dicha lucha deben guardar un equilibrio y proporcionalidad con el fin perseguido, debiendo respetar, en todo caso, los derechos humanos recogidos en los diversos instrumentos internacionales y, en concreto, en el Convenio Europeo de Derechos Humanos y, particularmente, lo referido al respeto a la intimidad y al secreto de las comunicaciones, postura que sirvió de base para el informe presentado en la Conferencia de Estocolmo.

Aparte de los temas referidos al cibercrimen, se tomó nota de las observaciones remitidas por el Grupo de Cooperación Aduanera respecto del Reglamento Interno de la Autoridad de Supervisión Común del Sistema de Información Aduanero, decidiéndose que serían estudiadas cuando se constituyera formalmente la Autoridad y tuviera que tomar la decisión definitiva sobre dicho Reglamento.

9. PROYECTO HISPANO-HOLANDÉS SOBRE ESTÁNDA-RES DE INSPECCIÓN.

Ya en anteriores ediciones de esta Memoria, se dio cuenta de la existencia de un proyecto conjunto entre los autoridades de control de España (Agencia de Protección de Datos) y los Países Bajos (Registratiekamer) para el desarrollo

de metodologías y procedimientos comunes o armonizados para la realización de inspecciones o auditorías de privacidad. El motivo principal de este proyecto era la previsión de que, una vez que se haya establecido una legislación armonizada en materia de protección de datos en toda la Unión Europea mediante la transposición de la Directiva 95/46/CE, las competencias e instrumentos legales y tecnológicos que tendrían a su disposición las autoridades de control para llevar a cabo su misión serían similares. Y una de estas herramientas son las inspecciones o auditorías de los distintos trata mientos de datos personales realizados en cada Estado miembro de la UE, siendo previsible que, dada la cada vez mayor extensión de los tratamientos de datos de ámbito internacional, cada vez se hará más necesaria la cooperación en esta materia. Por lo tanto, para que dicha colaboración sea efectiva, es absolutamente necesario, como se ha dicho, el desarrollo de estándares y métodos comunes.

En el año 1998 se dio el primer paso en este proyecto, mediante un seminario que tuvo lugar en Madrid y en el que dos equipos de inspectores de ambas autoridades intercambiaron ideas y experiencias, planificándose los pasos posteriores del proyecto.

El primer resultado fue la presentación, en la Conferencia de Primavera de Autoridades de Control, celebrada en Helsinki en abril de 1999, de un informe conjunto de ambas delegaciones en el que se daba cuenta de los resultados del seminario celebrado durante dos días en Madrid, se delineaban las líneas generales que se pensaban seguir y se invitaba a otras delegaciones a unirse al proyecto.

Posteriormente, tal como se había acordado en la reunión de Madrid, se planificó y se llevó a cabo la primera inspección utilizando métodos comunes, en gran parte derivados de los sistemas de trabajo de la Inspección de Datos española, que cuenta con una gran experiencia en este tipo de trabajo. El sector elegido para esta primera experiencia fue el de proveedores de servicios de Internet (PSI), por considerarse que los servicios que prestan estas compañías son idénticos en cualquier parte del mundo.

Para estudiar los resultados de esta primera inspección en ambos países y confirmar que el método seguido ofrecía los resultados apetecidos, se celebró un nuevo seminario de dos días, en el mes de noviembre de 1999, en La Haya. En el primer día y en una sesión cerrada, ambas delegaciones compararon los resultados obtenidos y decidieron seguir utilizando el mismo modelo puesto que había dado los frutos esperados. Por lo tanto, se tomó el acuerdo de realizar dos nuevas auditorías a otros dos PSI para tener, de esta manera, un conocimiento del sector que permita extraer conclusiones respecto a sus prácticas en el campo de protección de datos personales.

Pues bien, en los primeros meses del año 2000 se llevaron a cabo las dos auditorías restantes en cada uno de los países, lo que permitió presentar el informe de conclusiones en la Conferencia de Primavera de Autoridades de Control, que se celebró en Estocolmo el mes de abril de 2000.

En dichas conclusiones se ponía de manifiesto la existencia de similitudes y diferencias detectadas durante las inspecciones en ambos países, que fue uno de los objetivos fundamentales del uso de una metodología común. A continuación se presenta un resumen de las mismas:

* PRINCIPALES SIMILITUDES

1. Los datos conservados por los PSI de cada país son similares, aunque existen diferencias en el periodo de retención de dichos datos.

2. Todos los PSI almacenan datos relativos a las visitas a sus páginas web que son posteriormente agregados y guardados para uso estadístico. De nuevo, aparecen diferencias sobre los plazos de conservación.

3. Todos los proveedores la base contractual para el tratamiento de los datos de sus clientes.

4. No se han obtenido evidencias de tratamiento de datos especialmente protegidos.

5. Sería necesario incrementar el conocimiento de la existencia de la legislación sobre protección de datos en este sector en ambos países.

* PRINCIPALES DIFERENCIAS

1. La diferencia más importante estribaba en la información dada a los afectados. Los PSI españoles daban una información mucha más detallada y exacta sobre su política de privacidad a los afectados. También es interesante señalar que los tres PSI españoles inspeccionados contaban con dicha política de privacidad definida.

2. Los PSI españoles también habían establecido y desarrollado un procedimiento más integral para facilitar el ejercicio de los derechos de los ciudadanos. Alguno de ellos incluso tramitaba las peticiones que le llegaban vía correo electrónico o a través de transacciones *on-line*.

3. Los PSI españoles utilizaban el correo electrónico de forma habitual para comunicarse con sus clientes mientras que los holandeses eran reticentes a su uso por miedo a ser acusados de practicar el "spam".

4. Respecto de las prácticas de comunicación de datos a terceros, es interesante mencionar que los PSI españoles admitieron haber solicitado el consentimiento de sus clientes para comunicar sus datos a terceros (generalmente, socios comerciales) mientras que los PSI holandeses negaron comunicar datos a terceros o, incluso, tener la intención

de hacerlo. Esta diferencia puede estar causada por el hecho de que los PSI españoles tenían planes para poner en marcha, en el futuro, plataformas de comercio electrónico.

5. Todos los PSI españoles inspeccionados almacenaban similares tipos de datos, sin que aquellos que prestaban el servicio de forma gratuita o diferentes categorías de datos que aquellos otros que lo prestaban a cambio de una contraprestación económica. En cambio, en los Países Bajos había una diferenciación mucho más clara en la información almacenada en relación con este hecho.

10. GRUPO DE PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL

En el pasado año 2000 tuvieron lugar dos reuniones -en junio y en noviembre- del Grupo de trabajo de protección de datos en el ámbito laboral. Dicho Grupo había mantenido en el año 1997 dos encuentros informales, si bien ha sido en el transcurso del pasado año cuando se ha fomentado esta iniciativa y ha adquirido una mayor relevancia.

El Grupo se convocó a iniciativa de la Comisión Europea, Dirección General de Empleo y Asuntos Sociales, y contó con la participación de la Dirección General de Mercado Interior -Unidad de Protección de Datos- en ambas reuniones, a las que fueron invitados representantes tanto de los Departamentos de Trabajo como de las Autoridades de Protección de Datos de los Estados miembros de la Unión Europea.

El objetivo de dichas reuniones era intercambiar información acerca de la normativa y tendencias nacionales en este ámbito así como el de estudiar posibles acciones comunitarias futuras dirigidas específicamente a la protección de datos en el campo laboral, todo ello teniendo en cuenta y partiendo de la protección otorgada por parte de la Directiva 95/46/CE.

En el transcurso de dichas reuniones se analizaron diferentes puntos y principios propuestos en los documentos de trabajo presentados por la Dirección General de Empleo, a la luz de la Directiva, la normativa y la jurisprudencia existente en los distintos Estados miembros.

Entre ellos podemos citar la precisión del alcance, desde el punto de vista de la protección de datos personales, de diferentes conceptos como "interesado", "empleador", "tra tamiento de datos de carácter personal" y "consentimiento", buscando el modo de compatibilizar los intereses de los trabajadores con los del empresario teniendo en cuenta el artículo 8.2.b) de la Directiva, que establece una derogación al principio general del consentimiento en los casos en los que el tratamiento sea necesario para *respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral* de conformidad con la legislación nacional y la extensión a ciertos datos laborales de la consideración de datos especialmente protegidos.

En relación con este último punto, respecto del que el Grupo manifestó especial interés, se abordó la protección otorgada por los distintos Estados a los datos de salud, incluyendo en este apartado los tests genéticos y sobre drogodependencia.

Otro asunto de especial relevancia para el Grupo es el de la protección de los trabajadores en lo relativo a la vigilancia de su comportamiento, de su correspondencia -fundamentalmente correo electrónico e Internet-, así como las implicaciones existentes con el ejercicio de la libertad sindical y el papel que deben desempeñar los representantes de los trabajadores en relación con un posible enfoque colectivo del derecho a la protección de datos personales, que podrá extenderse a cuestiones relacionadas con la introducción o modificación de sistemas automatizados de tratamiento de datos laborales, vigilancia electrónica del comportamiento de los trabajadores, contenido y modo de gestión e interpretación de cuestionarios y tests relativos a sus datos personales, etc.

Otro punto que se trató fue protección otorgada a los datos personales de los trabajadores en relación con posibles transferencias a terceros países y la posible aplicación en este ámbito del contenido del proyecto de Decisión de la Comisión sobre Cláusulas contractuales tipo del artículo 26.4 de la Directiva.

En la segunda reunión, se solicitó a los distintos países la remisión de información legislativa y jurisprudencial respecto a dicha materia, decidiéndose trasladar al Grupo de Trabajo del Artículo 29 un documento de propuesta con inclusión de la información recabada, sometiendo a su consideración los puntos anteriormente mencionados.

11. CONFERENCIA DE PRIMAVERA DE AUTORIDADES DE PROTECCIÓN DE DATOS (ESTOCOLMO, 6 Y 7 DE ABRIL DE 2000)

La Conferencia de Primavera de los Comisionados Europeos de Protección de Datos la forman los Comisionados de la Unión Europea además de los representantes de las Autoridades de Control de Noruega, Islandia, Suiza y Hungría y una representación de la Comisión de las Comunidades Europeas. Se celebra anualmente en un país distinto y se ocupa del análisis de aquellos desarrollos legislativos o tecnológicos que pueden afectar a la privacidad de los ciudadanos europeos en aras de buscar soluciones armonizadas en dicho ámbito.

En la Conferencia del año 2000 se trataron los siguientes temas:

- Desarrollos desde la última Conferencia de Primavera: seguimiento de las discusiones de Helsinki y seguimiento del cuestionario estadístico de actividades de las autoridades nacionales.

- El proyecto de inspección de la Agencia sueca de protección de datos sobre datos genéticos. La situación en otros países.

- Reforma de la sanidad y la protección de datos.

- Así se lleva a cabo una inspección de la Agencia sueca de protección de datos

- Tramitación de quejas

- Implantación de la Directiva relativa a la protección de datos: la situación en los diferentes países de la UE

- La Ley sobre la libertad de imprenta y la ley de secreto - el sistema sueco. Situación en los diferentes países de la UE

- Informe del Grupo Operativo Internet

- Comunicación de datos obtenidos por Internet

- Artículo 4 de la Directiva relativa a la protección de datos

- Jurisdicción y ley aplicable

- Iniciativas relativas al crimen en el ciberespacio

- La experiencia española en la implantación de la Directiva de Telecomunicaciones

- Videovigilancia por razones de seguridad

- Servicios telefónicos gratuitos

La delegación española, aparte de participar en todas las actividades y debates de la Conferencia, expuso tres ponencias durante la misma.

D. Juan Manuel Fernández López, Director de la Agencia de Protección de Datos, expuso una ponencia sobre "La experiencia española en la implantación de la Directiva de Telecomunicaciones".

"Dicha ponencia se centró en tres aspectos diferenciados: el tratamiento de los datos personales y protección de la intimidad en el sector de las telecomunicaciones, los aspectos concretos de la transposición en materia de datos personales en la prestación de los servicios de telecomunicaciones al Derecho nacional español y las actuaciones más relevantes realizadas por la Agencia de Protección de Datos en el sector de las telecomunicaciones durante el año 1999.

En primer lugar, pues, se pasaba revista a la normativa reguladora, haciendo especial hincapié en las disposiciones de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que ha sido incorporada al ordenamiento jurídico español por la Ley 11/1998, de 24 de abril, General de Telecomunicaciones -LGT- (arts. 49 a 54) y el Título V del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo.

La materia de protección de datos personales en el ámbito de las telecomunicaciones afecta de lleno a un derecho fundamental como es el derecho a la intimidad, protegido por la Constitución Española en su artículo 18, con dos garantías: por un lado, el secreto de las comunicaciones (art. 18.3 C.E.) y, por otro, la limitación en el uso de la informática (art. 18.4 C.E.)

Estas dos garantías constitucionales, aparecen contempladas a su vez en sendos artículos de la citada Ley General de Telecomunicaciones: El artículo 49 que impone a los operadores de servicios de telecomunicaciones la obligación de garantizar el secreto de las comunicaciones mediante la adopción de las medidas técnicas oportunas, y el artículo 50 que impone a los mismos operadores la obligación de garantizar, en el ejercicio de su actividad, la protección de datos de carácter personal de acuerdo con la hoy vigente Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

Por lo que respecta a los aspectos concretos de la transposición en materia de protección de datos personales en la prestación de los servicios de telecomunicaciones se examinaron las disposiciones relativas al derecho de información, a los datos personales sobre el tráfico y facturación, la facturación desglosada, la identificación de líneas, el desvío automático de llamadas, la confección de guías, las garantías frente a llamadas no solicitadas para fines de venta directa (marketing directo y llamadas anónimas), la seguridad de los servicios de telecomunicación y la confidencialidad de las comunicaciones.

Entrando ya en las actuaciones más relevantes de la Agencia de Protección de Datos durante el año 1999, se analizaban éstas en una doble vertiente. De un lado, los Planes Sectoriales de Inspección de Oficio y, de otro, las derivadas de la atención de las denuncias de los ciudadanos relacionados con el uso de sus datos personales en el marco de la provisión de servicios de telecomunicaciones.

En el primer apartado, se resaltaban las inspecciones llevadas a cabo en los principales operadores de telefonía fija de cara a conocer su grado de adecuación a la legislación sobre protección de datos, tanto en lo referente a la Ley de Protección de Datos, como en lo relativo a la norma que incorpora la Directiva de Telecomunicaciones.

Como uno de los resultados más importante del primer conjunto de actuaciones se constató que un operador de tele - comunicaciones disponía de un fichero automatizado cuyo objeto es el tratamiento automatizado de los datos de tráfico y facturación telefónica de sus clientes con fines comerciales propios.

El sistema recogía, grababa y almacenaba también los datos de detalle de las llamadas de todos los abonados, manteniendo actualizado el detalle de entre 100 y 110 millones de llamadas diarias durante los últimas 5 o 6 semanas y les añade la facturación de los últimos 12 meses, datos referidos a millones de abonados.

Igualmente, el sistema permitía obtener información sobre el nombre, apellidos y domicilio tanto de los titulares de telé - fono que realizan la llamada como el nombre, apellidos y domicilio de los titulares de teléfono que la reciben.

Este Sistema de Información no tiene en cuenta ningún tipo de selección o filtración de datos, por lo que se incorporan a él datos de todos los titulares existentes en los demás ficheros de la compañía de los que se nutre (Fichero Integrado de Abonados, solicitudes, órdenes de servicio, ficha de cliente y Fichero de Facturación) y de todas sus llamadas. En consecuencia, en el fichero se recogen y tratan los datos de las personas que han manifestado su oposición al trata - miento automatizado de sus datos para fines de promoción comercial de los servicios de telecomunicaciones del operador y los datos personales de tráfico y facturación telefónica de los abonados que han adquirido tal condición con posterioridad al mes de enero de 1999, fecha en la que el operador remitió el encarte solicitando el consentimiento de los afectados.

La eliminación de los datos de abonados que han rechazado el tratamiento de sus datos personales, así como la de aquéllos a los que no les ha sido solicitado el consentimiento, se realiza al definir cada una de las consultas que los usuarios realizan al sistema. Esto quiere decir que el operador, después de incorporar los datos de todos sus abonados en el fichero, de tratarlos automatizadamente y de seleccionar el perfil del colectivo al que desea remitir encartes publi - citarios, elimina a aquellos que se han opuesto al tratamiento de sus datos con fines comerciales y a aquellos abona - dos que aún no han prestado su consentimiento, no remitiéndoles promociones comerciales de dichos productos.

Ello ha supuesto la incoación al citado operador de un procedimiento sancionador por tratamiento automatizado de datos de carácter personal sin consentimiento de los afectados y con incumplimiento de los preceptos de protección de datos que imponen las disposiciones reglamentarias de desarrollo.

Dentro de este procedimiento sancionador y mediante Acuerdo del Director de la Agencia de Protección de Datos se adoptó la medida cautelar consistente en que, por parte del operador se cesara, de manera inmediata, en el tratamiento automatizado, de datos de carácter personal relativos al tráfico y a la facturación telefónica de los abonados que se han opuesto expresamente a que sus datos personales sean tratados automatizadamente, así como de los abonados que no han prestado el consentimiento. Dicha medida cautelar fue inmediatamente cumplida por el operador.

Este procedimiento terminó con una Resolución confirmatoria de los hechos imputados que sancionó al operador en los términos expuestos con una multa de 50 millones de pesetas.

Otro de los aspectos más relevantes de la referida inspección centra los hechos en el procedimiento utilizado por un operador para recabar el consentimiento para tratar los datos de tráfico telefónico. Durante las actuaciones realizadas se ha constatado que el operador ha realizado tratamiento de datos personales de sus abonados con fines de promo - ción comercial de sus propios productos, y para ello ha tratado conjuntamente en un mismo fichero, diferentes tipolo - gías de datos procedentes de otros ficheros, entre los que se encuentran datos de tráfico telefónico, facturación, ficha de clientes, etc.

Cuando un abonado no está suficientemente informado del uso y finalidad que sus datos van a tener durante ese tratamiento, entiende que las relaciones entre la empresa y él son exclusivamente las necesarias para que reciba el servicio de telecomunicaciones y para abonar el dinero que en contraprestación le corresponda. Por lo tanto, sus datos personales no deben ser incluidos en otro fichero distinto del específicamente destinado al tráfico, al pago o la factura - ción telefónica, máxime cuando ese fichero está destinado esencialmente a la promoción comercial y se utiliza para crear perfiles y categorías de clientes.

Para pedir el consentimiento al tratamiento anterior, el operador ha remitido varios encartes a sus abonados. Dichas notificaciones únicamente hacen referencia a los datos de tráfico sin especificar cuáles y, por otra parte, tampoco hacen referencia a los datos de facturación, cuando estos últimos son objeto de tratamiento en el fichero. No se especifica el plazo conforme al cual la falta de contestación por el abonado supone el otorgamiento de consentimiento tácito y tampoco se informa de que el tratamiento de los datos de tráfico se va a realizar conjuntamente con otras tipologías de datos, lo cual permite establecer perfiles, categorías de clientes y hábitos de uso de los servicios de telecomunicaciones.

Esta situación ha supuesto el inicio de un procedimiento sancionador al operador por tratamiento de datos personales sin consentimiento con arreglo a lo dispuesto en nuestra Ley nacional. Esta infracción está tipificada como grave, pudiendo ser sancionada con una multa de 10.000.001 a 50.000.000 de pesetas.

Un tercer aspecto analizado en la inspección sectorial de oficio realizada por la Agencia de Protección de Datos durante 1999, ha sido la comprobación del grado de adecuación de los principales operadores de telefonía fija a las prescripciones relativas a la prestación de servicios avanzados de telecomunicaciones.

En el curso de las inspecciones realizadas a estos operadores se han detectado evidencias de varios incumplimientos.

Así, por ejemplo, se ha detectado una carencia de información de los operadores hacia sus abonados sobre el riesgo concreto de violación de la seguridad en la red; las guías actuales no recogen lo previsto en la normativa para que un abonado pueda solicitar figurar con la marca de no utilización para fines de venta; los operadores no prestan el servicio de que cualquier abonado pueda suprimir de forma automática en todas sus llamadas la identificación de la línea llamante; ni, en fin, se encuentra aún disponible una solución para ofrecer a los abonados la posibilidad de poner fin al servicio de desvío automático de llamadas a su terminal por parte de un tercero.

Sin embargo, hay que señalar que algunas de las obligaciones legales impuestas por el Reglamento a los operadores requieren del oportuno desarrollo reglamentario por parte del organismo regulador o autoridad administrativa competente, desarrollo que aún no se ha producido en su totalidad, por lo que el incumplimiento de dichas obligaciones no es imputable a los operadores en aquellos puntos que exigen de tal desarrollo reglamentario.

Finalmente, cabe destacar también las inspecciones sectoriales practicadas en relación con los denominados procedimientos de "scoring". Consisten en esencia estos procedimientos en que un operador facilita a otra entidad una relación de sus propios clientes o potenciales clientes, la cual le es posteriormente devuelta por ésta, pero ampliada con una clasificación con información sobre la aptitud crediticia de cada uno de esos clientes, lo cual le sirve al operador para rechazar o no la solicitud de servicio realizada por el potencial cliente. Esta operación de "scoring" puede suponer una cesión inconsentida de datos personales a efectos de la Ley española de Protección de Datos, razón por la que se han abierto dos procedimientos sancionadores a otros tantos operadores.

Por lo que respecta a las actuaciones de la Agencia realizadas en virtud de denuncias de los ciudadanos podemos destacar como más significativas las que afectan a la difusión de datos personales que un importante operador de telefonía realiza a través de Internet, la obligatoriedad de facilitar los datos de una cuenta corriente o tarjeta de crédito para conectarse al servicio Internet, cuando el pago del mismo se ha realizado por anticipado con la compra de un kit contra reembolso, así como algún tema relacionado con las búsquedas inversas en directorios, esto es, obtener la identidad y/o dirección de una persona a partir de su número de teléfono, fax o correo electrónico" .

Igualmente, D. Jesús Rubí Navarrete, Adjunto al Director, realizó una intervención sobre "Comunicación de datos obtenidos por Internet", cuyos aspectos fundamentales se resumen a continuación.

"La Directiva 95/46/CE ha sido definitivamente incorporada al derecho español a través de la reciente Ley Orgánica 15/1999, de 13 de diciembre, que entró en vigor el 14 de enero pasado, disposición que permitirá abordar los problemas de protección de datos en Internet. Sin embargo, la hoy derogada Ley Orgánica 5/1992, que continúa siendo aplicable a los hechos producidos con anterioridad a la entrada en vigor de la nueva Ley, también ha sido un instrumento adecuado para llevar a cabo la protección de datos personales en Internet. Confío en que la experiencia obtenida con su aplicación resulte útil para conseguir una mejor protección de la privacidad en el futuro.

El objeto de la presente comunicación es, precisamente, el de analizar algunos de los problemas prácticos que se han planteado en esta materia así como los criterios interpretativos que ha mantenido la Agencia de Protección de Datos española en aplicación de la Ley Orgánica 5/1992, de 29 de octubre.

Los supuestos prácticos que se han seleccionado para la presente comunicación se refieren a dos cuestiones diversas relacionadas con el tratamiento y la obtención de datos personales en Internet.

El primero de ellos es un caso de recepción de correo publicitario no deseado a través de la dirección de correo electrónico y el segundo se refiere a la obtención de datos a través de páginas web en Internet y a las posteriores cesión y tratamiento de los datos.

Los hechos relativos al primero de los supuestos son sencillos: un usuario de Internet recibe mensajes publicitarios en su dirección de correo electrónico remitidos desde la dirección de correo electrónico de una empresa que se dedica a esta actividad. El usuario solicitó información sobre la procedencia de su dirección de correo electrónico y pidió la baja en la lista de distribución, ejercitando sus derechos de acceso y cancelación. Inmediatamente volvió a recibir mensajes publicitarios en su dirección de correo electrónico. Asimismo, recibió un mensaje amenazante desde la dirección de correo electrónico de la empresa remitente, que permitió acreditar una vinculación entre la dirección de correo electrónico del usuario de Internet y su propia persona.

La cuestión relevante en el presente caso consiste en determinar si la dirección de correo electrónico del usuario puede ser considerada o no como un dato personal.

El concepto de dato personal, según la definición de la Ley Orgánica 5/1992, de 29 de octubre, comprende cualquier información concerniente a persona física identificada o identificable, de donde se requiere la concurrencia de un doble elemento: por una parte la existencia de una información o dato y de otra, que dicho dato pueda vincularse a una persona física identificada o identificable. En el supuesto de direcciones electrónicas la información está constituida por un conjunto de signos que cuando permiten la vinculación directa o indirecta con una persona física la convierte en un dato de carácter personal.

En el caso examinado resulta evidente que la dirección de correo electrónico ha quedado vinculada a su persona, como se desprende de que se le envíe un posterior correo electrónico a dicha dirección y personalizado con un nombre y apellido.

El hecho de que una dirección electrónica se exteriorice de forma voluntaria por el afectado, no quiere decir que ese dato esté disponible para cualquiera, sino que únicamente, y por regla general, estará disponible y será conocido por aquellos a quienes voluntariamente se lo indique el titular de dicha dirección. En consecuencia, las empresas que obtienen direcciones electrónicas para enviar publicidad, deben cerciorarse de que el afectado ha manifestado su consentimiento para tratar sus datos referidos a esa dirección.

El segundo de los supuestos prácticos seleccionado para la presente comunicación se refiere al tratamiento y cesión de datos personales obtenidos a través de accesos a páginas web.

Los hechos objeto de consideración son, sintéticamente, los que se exponen a continuación.

Usuarios de Internet residentes en España acceden a las páginas web de empresas ubicadas en un país que no dispone de niveles de protección adecuados o equivalentes, en este caso, los Estados Unidos de Norteamérica (USA). Los usuarios consultan la información contenida en las páginas web de empresa norteamericana interesándose por los nuevos productos y servicios que ofrecen. Para ello, registran sus datos personales que se incorporan a las base de datos de dichas empresas. Las empresas mantienen una política propia de protección de la privacidad que se traduce en posibilitar el acceso a determinadas páginas web en las que se informa de una doble posibilidad: excluir el consentimiento respecto de la remisión por parte de las empresas de correo postal o electrónico o de recibir llamadas telefónicas con fines de marketing o excluir el consentimiento para que las empresas titulares de las páginas web puedan ceder los datos a otras empresas colaboradoras.

El acceso a dichas páginas web no es obligatorio, ni se advierte al usuario de la necesidad o conveniencia de acceder a ellas ni de las consecuencias de la falta de acceso. Estas consecuencias consisten en que la empresa que recaba los datos estima que, aunque no se haya accedido a las páginas sobre privacidad, el usuario ha manifestado tácitamente su consentimiento sobre el contenido de las mismas.

Una vez incorporados los datos a los sistemas informáticos de las empresas, éstas permiten que sus filiales accedan a las bases de datos y los transfieran telemáticamente, incorporándolos a sus propios ficheros informáticos ubicados en España y procediendo a su tratamiento posterior.

En resumen, se obtienen datos a través de Internet en ficheros ubicados en un país sin nivel de protección adecuado y, posteriormente, son cedidos y tratados en España.

Los principales problemas que, desde la perspectiva de la protección de datos personales, se han planteado son los siguientes: el ámbito de aplicación y, por tanto, de protección de la Directiva 95/46/CE y de las normas de derecho nacional que la incorporan en España; la información que se facilita a los usuarios a través de las páginas web, que se limita a ofrecer la posibilidad de rechazar envíos de correo postal o electrónico, llamadas telefónicas o cesiones de datos a otras empresas colaboradoras. En este punto las partes imputadas han alegado que, habiéndose obtenido los datos USA conforme al derecho norteamericano, por encontrarse allí ubicadas las bases de datos, la cesión y el tratamiento ulterior por parte de las filiales en Europa es, también, conforme a derecho y la cesión de datos a empresas filiales que forma parte del mismo grupo empresarial ubicadas en España.

La postura de la Agencia de Protección de Datos española se resume en que la normativa española debe aplicarse atendiendo al principio de territorialidad, de forma que aunque la ley española no puede aplicarse a la conducta de las empresas ubicadas en USA, si se produce una cesión o tratamiento de datos en España, éstos deberán ser conformes con la ley española de protección de datos, principio que debe ser mantenido, aunque los datos se obtuvieran en origen en USA conforme a la legislación norteamericana,

La consecuencia de lo expuesto es que si están previstas cesiones de datos a empresas filiales, el usuario debe ser informado previamente y disponer de la opción de excluir la cesión para que esta sea lícita según la Ley española.

Admitir tales prácticas en el derecho interno supondría permitir la obtención de datos por una entidad cedente interpuesta, excluyendo la responsabilidad del cesionario que, en su propio interés, no ha obtenido lícitamente datos relativos a potenciales clientes.

Para analizar si dicho tratamiento es conforme con la normativa española de protección de datos, es preciso considerar las circunstancias relacionadas con los principios de información y consentimiento que se produjeron al recabar los datos en origen, es decir, en las páginas web ubicadas en USA.

A este respecto, la información que figura en las páginas web no resulta conforme con dicha norma. En primer lugar, porque se facilitan los datos y se ceden aunque el usuario no acceda a las páginas que contienen la política de privacidad de las empresas norteamericana, sin que se le informe previamente de la necesidad de acceder a las mismas ni de las consecuencias de la falta de acceso.

En segundo lugar, porque, aunque acceda, las posibilidades de excluir el consentimiento resultan limitadas y no comprenden la opción de excluir otras modalidades de tratamiento de datos como exige la LORTAD.

En tercer lugar, porque no se informa previamente ni se exige el consentimiento para la cesión de datos a las empresas filiales de, ni para su posterior tratamiento por éstas.

Y, en cuarto lugar, porque no existe relación negocial con la filial sino sólo con la matriz norteamericana a la que pertenece la página web ubicada en USA.

La falta de información adecuada, conforme a la normativa española de protección de datos determina que el consentimiento prestado por el usuario al registrarse en las páginas web resulte insuficiente ya que, al menos, no incluye la cesión de datos a las empresas filiales ni al tratamiento posterior que éstas realicen.

Por ello, a juicio de la Agencia de Protección de Datos infringen la Ley española de protección de datos, incurriendo en responsabilidad.

De acuerdo con este criterio, el sistema de protección de datos de los ciudadanos residentes en España resulta completo".

Además, D. Emilio Aced FÚlez, de la Inspección de Datos de la Agencia, presentó conjuntamente con Dña. Dia na Alonso Blas, de la Autoridad de Control de los Países Bajos, el informe "Auditorías de la privacidad: informe del proyecto Hispanoholandés", de cuyas principales conclusiones ya se ha dado cuenta en otro apartado de esta Memoria.

Además, como uno de los resultados más importantes de la Conferencia, se debe mencionar la Resolución de los Comisionados Europeos de Protección de Datos sobre la retención de datos de tráfico por parte de los Proveedores de Acceso a Internet, que a continuación se reproduce:

Resolución de la Conferencia Europea de Autoridades de Control de Protección de Datos Estocolmo, 6 y 7 de abril de 2000

Conservación de datos de tráfico por parte de los Proveedores de Servicios de Internet (PSI)

La Conferencia Europea de Autoridades de Control de Protección de Datos observa con preocupación que los PSI estarían obligados, según ciertos proyectos encaminados a combatir los delitos informáticos puestos en marcha por el G8, el Consejo de Europa y el Consejo de Ministros de la Unión Europea, a conservar los datos de tráfico durante más tiempo del requerido para la facturación de sus servicios, con el fin de permitir posibles accesos a dichos datos de tráfico por parte de las Fuerzas y Cuerpos de Seguridad.

La Conferencia hace hincapié en que tal conservación podría suponer una invasión indebida de los derechos fundamentales garantizados a las personas por el Artículo 8 del Convenio Europeo de Derechos Humanos. Cuando los datos de tráfico tengan que ser conservados en casos específicos, debe existir una necesidad demostrable para ello, el periodo de conservación debe ser tan corto como sea posible y dicha práctica debe estar claramente regulada por la Ley.

El Director de la Agencia de Protección de Datos, en base a lo acordado en la Conferencia, remitió copia de dicha Resolución a los Ministros de Justicia, Interior y Ciencia y Tecnología; al Presidente del Consejo General del Poder Judicial, al Fiscal General del Estado, a los Presidentes de los principales operadores de telecomunicaciones, al Presidente de la Asociación Nacional de Industrias Eléctricas y de Telecomunicaciones y a los Presidentes de la Asociación de Usuarios de Internet y de la Asociación de Internautas.

12. CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS (VENECIA, 28 A 30 DE SEPTIEMBRE DE 2000)

Como un medio para, al menos una vez al año, estudiar desde una perspectiva global los desarrollos más importantes habidos en el mundo en el ámbito de la privacidad y en la defensa de los derechos fundamentales de la persona humana en todo aquello relativo al tratamiento de datos personales, se celebra la Conferencia Internacional de Autoridades de Protección de Datos.

En el año 2000, dicha conferencia fue organizada por la Autoridad de Control italiana y se celebró en la ciudad de Venecia. El lema de la Conferencia fue "Un mundo, una privacidad" y se centró en el impacto de las nuevas tecnologías para la privacidad, resaltando el carácter global de las mismas.

La delegación española participó activamente en todos los trabajos de la Conferencia y el Director de la Agencia de Protección de Datos pronunció una conferencia sobre el tema "Protección de datos en los ámbitos judicial y policial", que tenía como objeto analizar el modo en que los ficheros que existen en los distintos órganos jurisdiccionales deben someterse a las normas reguladoras de la protección de datos de carácter personal. A continuación se incluye un resumen de la misma.

"Los ficheros de los órganos jurisdiccionales tienen unas características muy especiales derivadas de su propia naturaleza. Se trata de ficheros que se crean por la autoridad judicial en el ejercicio de sus funciones, funciones que a la defensa del Estado de Derecho y en particular a la tutela de los derechos de los ciudadanos. Consecuentemente van a contener datos que en muchos casos se obtienen sin el consentimiento del afectado, que en muchos casos serán datos

sensibles, que van a ser conocidos por las partes que intervienen en el proceso y por otros terceros interesados en el mismo y que podrán en determinados supuestos ser comunicados a otros órganos jurisdiccionales tanto nacionales como internacionales. Además, la resolución judicial que ponga fin al proceso deberá comunicarse a las partes que han intervenido en el mismo, a otras administraciones para su ejecución, darle la publicidad general que requiere toda resolución judicial en un Estado de Derecho e incluirse en colecciones jurisprudenciales para atender la necesidad de que se conozca la interpretación que los Tribunales establecen respecto de la legislación y su aplicación a supuestos diferenciados. Una vez establecidas las características fundamentales de dichos ficheros, se analizaban los aspectos de las normas internacionales (fundamentalmente la Directiva 95/46/CE y el marco legal establecido por el Consejo de Europa: Convenio 108, Recomendación R (73) 23, Recomendación R (83) 3 y Recomendación R (95) 11) de las que se desprende una limitación a la divulgación de las resoluciones judiciales en cuanto contengan datos de carácter personal, dado que en ese caso, deberán tomarse en consideración los principios contenidos en el Convenio 108, entre los que cabe destacar los de consentimiento, finalidad, información, calidad de los datos, proporcionalidad y seguridad. En este punto, y en relación con el principio de finalidad, debe recalcarse que la propia Recomendación R (95) 11 indica, en el apartado II de su Anexo I,
las finalidades que fundamentan la divulgación en repertorios de las sentencias, haciendo referencia, entre otras, a "facilitar el trabajo a las profesiones jurídicas", "informar a toda persona interesada en una cuestión de jurisprudencia", "contribuir a la coherencia de la jurisprudencia" o "permitir al legislador hacer análisis de la aplicación de las leyes".

Todo ello sin olvidar la jurisprudencia del Tribunal Europeo de Derechos Humanos, que ha puesto de manifiesto la necesidad de preservar la intimidad de las personas intervinientes en un determinado procedimiento, garantizando la confidencialidad de los datos identificativos de las personas cuando la revelación de su identidad puede causarles un serio perjuicio.

Por lo que se refiere al ámbito nacional la vigente Ley española de protección de datos sólo contiene una previsión respecto de los ficheros jurisdiccionales para no exigir el consentimiento del afectado respecto de la comunicación de datos cuando tenga por destinatarios "... a los Jueces y Tribunales en el ejercicio de las funciones que tienen atribuidas". Obsérvese que en estos supuestos se exige que la cesión tenga lugar en el contexto de las funciones jurisdiccionales, esto es, en la investigación que en el marco de un expediente estén llevando a cabo, o los que se comuniquen dentro de un proceso jurisdiccional.

Acorde con el respeto a los principios de protección de datos en los ficheros jurisdiccionales el artículo 230 de la Ley Orgánica del Poder Judicial establece al respecto que los Juzgados y Tribunales podrán utilizar medios informáticos y telemáticos en sus funciones con las limitaciones que establece la Ley de Protección de Datos (art. 230.1) de tal manera que los procesos que se tramiten en soporte informático garantizarán ... la confidencialidad, privacidad y seguridad de datos personales en los términos que establece la Ley (art.230.3).

En el ejercicio de su función reglamentaria, el órgano rector de los Jueces ha dictado el Reglamento 5/1995, de 7 de junio, en el que concreta aspectos prácticos relativos a la creación de los ficheros, garantías de confidencialidad y forma de ejercer sus derechos por parte de los afectados. Las previsiones más destacables son las siguientes: los ficheros de Juzgados y Tribunales se crearán, modificarán y suprimirán mediante acuerdo del Consejo General del Poder Judicial (órgano rector de los Jueces) que se publicará en el Diario Oficial (B.O.E.) y se notificará a la Agencia de Protección de Datos; los datos serán conservados en tanto su supresión no sea ordenada por decisión judicial; la cesión de datos se limita a supuestos de cooperación jurisdiccional nacional o internacional, a las normas y supuestos de competencia territorial u organización de servicios y el nombramiento del Secretario del Juzgado o Tribunal como responsable del fichero o tratamiento.

Por lo que respecta al ejercicio de los derechos de acceso, rectificación y cancelación el Reglamento se remite a la normativa reglamentaria de la Ley de Protección de Datos en la que se desarrolla la forma de ejercer aquellos derechos. Además, concreta que el afectado es quien podrá ejercer tales derechos en la sede del órgano judicial y ante el responsable del mismo (Secretario) y prevé la denegación del acceso, en los supuestos generales del Reglamento que desarrolla la Ley de Protección de Datos y en el supuesto de unas diligencias judiciales penales que hayan sido declaradas secretas. Asimismo el derecho de acceso no podrá ejercerse en perjuicio del derecho a la intimidad de otra persona distinta del afectado.

Igualmente, los datos que reflejen hechos constatados en un procedimiento jurisdiccional no podrán ser modificados o cancelados por el ejercicio de estos derechos, lo que resulta lógico toda vez que los procedimientos jurisdiccionales informatizados constituyen auténticos documentos judiciales sujetos a las normas generales de conservación y custodia. Las denegaciones al ejercicio de los derechos de acceso, rectificación y cancelación podrán recurrirse por el afectado ante el Juez o Tribunal.

Por otro lado, una cuestión de especial relevancia es el establecer los límites de acceso al texto completo de las resoluciones judiciales.

Partiendo del principio de publicidad de las actuaciones judiciales, que la Constitución Española consagra en su art. 120.1, deben considerarse las circunstancias en que los intereses de los afectados justifiquen una restricción o limitación a este principio de publicidad.

Por ello, el órgano de gobierno de los jueces señaló en su Acuerdo de 6 de marzo de 1991 que las partes interesadas en el proceso, en el sentido técnico jurídico, tendrán el derecho de acceso sin limitaciones.

Los demás interesados, terceros ajenos al proceso judicial, deberán justificar el interés y finalidad que persiguen y

comprometerse a respetar los derechos y garantías reconocidos por la Ley de Protección de Datos, lo que supondrá en muchos casos la despersonalización de la información. Será el Juez o Tribunal, en cada caso, quienes deban apreciar el interés del solicitante y la finalidad que persigue, valorando los intereses en conflicto mediante la ponderación motivada del derecho a recibir información y la garantía de la intimidad de los afectados.

Por lo que respecta, finalmente, a las sentencias incluidas en colecciones legislativas y jurisprudenciales accesibles al público, cabe señalar que la anterior Ley de Protección de Datos de 1992 (LORTAD) excluía a las mismas del ámbito de aplicación de dicha Ley en tanto se limitaran a reproducir resoluciones judiciales publicadas en diarios oficiales. Dicha previsión ha desaparecido de la reciente Ley de Protección de Datos 15/99 por lo que se consideran sometidos a los principios que sobre protección de datos establece la propia Ley. En todo caso tanto antes como ahora se publican con los datos anonimizados de las personas físicas".

Aparte de ello, los principales asuntos tratados en la Conferencia de Venecia fueron:

- Ciudadanía electrónica

- Videovigilancia

- Nuevas tecnologías, seguridad y libertad

- Contratos y flujos de datos

- Coste de la privacidad y soluciones basadas en software

- Tarjetas inteligentes y bancos de datos centralizados

- Intranets y servicios globales

- Privacidad y medios de comunicación

- Transparencia electrónica

- El estado actual de la privacidad

- Integración de distintas herramientas desde una perspectiva global

- Actividades policiales y judiciales

- Datos genéticos

- Nuevos retos

- ¨Hacia un Convenio Internacional sobre privacidad?

Como colofón de la Conferencia, se aprobó la Resolución que se incluye a continuación.

Resolución de la Conferencia Internacional de

Autoridades de Control de Protección de Datos

Venecia, 28, 29 y 30 de septiembre de 2000

Los Comisionados de Protección de Datos de los países reunidos en Venecia con ocasión de la 22¦ Conferencia Internacional sobre Privacidad y Protección de Datos Personales están de acuerdo afirmar los principios y estándares comunes de protección de datos a la vista de la creciente penetración de las tecnologías de tratamiento de los datos, el número creciente de usuarios de tales tecnologías y la intensificación del intercambio mundial de datos.

Muchos instrumentos internacionales están ya disponibles en este sector: desde las Directrices sobre Privacidad de la OCDE hasta el Convenio 108 del Consejo de Europa, las directivas de la Unión Europea, resoluciones y recomendaciones de organizaciones internacionales.

Estos instrumentos ya representan un núcleo significativo de principios de referencia apoyados por un amplio consenso; ellos forman lo esencial de un ejercicio común con vistas a asegurar su aplicación mundial tomando debida nota de los muchos cambios tecnológicos y sociales.

A la luz del reconocimiento de la privacidad como un derecho fundamental de las personas y como un elemento constitutivo de la libertad de los ciudadanos, nuestro trabajo debería dirigirse hacia el reconocimiento global de directrices para el tratamiento de datos personales

- reafirmando el carácter legalmente vinculante de estos principios, con particular atención a la finalidad de la recogida de datos, la necesidad de operaciones de proceso leales y transparentes (especialmente respecto a los llamadas

operaciones invisibles de tratamiento), proporcionalidad, calidad de los datos, tiempo durante el cual se guardan los datos, el derecho de acceso y el resto de los derechos de los afectados;

- proporcionando a los afectados una protección más efectiva a través de una supervisión independiente de las operaciones de tratamiento y la disponibilidad de vías de recurso fáciles de utilizar;

- reforzando las salvaguardias aplicables a deteminadas categorías de datos tales como los datos genéticos o los relativos a los distintos tipos de vigilancia electrónica.

Este debería permitir a los ciudadanos de todo el mundo alcanzar un nivel de protección adecuado y más ampliamente compartido, independientemente del lugar en el que tenga lugar el tratamiento o de los instrumentos usados para implantar esta protección en los foros nacionales e internacionales.

Los Comisionados de Privacidad y Protección de Datos trabajarán con otros para elaborar e implantar los principios globalmente reconocidos.

13. PRIMER ENCUENTRO IBÉRICO DE PROTECCIÓN DE DATOS

Las Autoridades de Control de Protección de Datos de España y Portugal han mantenido siempre una fluida y amistosa relación de trabajo y cooperación mutua. Como consecuencia de esta estrecha colaboración, el Presidente de la Comisio Nacional de Protecteccio de Dados de Portugal, el Sr. D. Joao Labescat, y el Director de la Agencia de Protección de Datos, el Sr. D. Juan Manuel Fernández López, acordaron celebrar anualmente un encuentro entre representantes de ambas autoridades para intercambiar experiencias prácticas y armonizar sus posturas respecto de los problemas que más preocupan a ambas.

Con este motivo, se celebró en la ciudad portuguesa de Évora, durante los días 14 y 15 de noviembre, el Primer Encuentro Ibérico de Autoridades de Protección de Datos.

Durante el mismo se celebraron sesiones monográficas dedicadas a diversos temas, como los problemas del sector de las telecomunicaciones, el comercio electrónico, los ficheros de solvencia patrimonial y crédito, a la utilización de cláusulas contractuales tipo para permitir el intercambio de datos personales con aquellos países que no gozaran de un nivel de protección adecuado en este campo y a la situación de la protección de datos personales en Iberoamérica, celebrándose también una rueda de prensa a la que acudieron los principales medios de comunicación de Portugal.

Como colofón de los trabajos se decidió la continuación de estos encuentros dado lo fructífero de la reunión y se redactó un informe final que se distribuyó a los medios de comunicación y que se reproduce a continuación.

PRIMER ENCUENTRO IBÉRICO DE AUTORIDADES DE PROTECCIÓN DE DATOS

Évora, 14 y 15 de noviembre de 2000

Las Autoridades portuguesa y española de Protección de Datos, reunidas los días 14 y 15 de noviembre en la ciudad de Évora, realizaron un balance de varios aspectos relevantes en el ámbito del derecho a la vida privada y discutieron las perspectivas de este derecho de cara a la evolución de las tecnologías de la información.

La Comisión Nacional de Protección de Datos (Portugal) y la Agencia de Protección de Datos (España), en este Primer Encuentro Ibérico, subrayan la importancia de la cooperación mutua, como forma de anticiparse y responder a los nuevos desafíos de la sociedad de la información, en especial en el marco ibérico, donde existen relaciones comerciales crecientes que afectan al tratamiento de datos personales de empresas establecidas en uno y otro país.

En el ámbito europeo e internacional, las dos Autoridades constataron la existencia de puntos de vista comunes y consideraron urgente la adopción de medidas para una efectiva armonización práctica que, incluso en el espacio europeo, se encuentra lejos de ser alcanzada.

Durante la reunión, fueron abordados aspectos ligados a las telecomunicaciones, al comercio electrónico, a los flujos transfonterizos de datos, al crédito y solvencia y a las relaciones con América Latina.

En particular, fueron debatidos varios casos concretos que permiten estudiar la aplicación de las leyes de protección de datos en ambos países.

En cuanto al sector de las telecomunicaciones, fueron abordadas las materias relativas a la forma de disponibilidad y recogida de datos de directorios y listas de abonados, al tratamiento de datos de tráfico y facturación y al consentimiento de los abonados, la existencia de mecanismos que permiten realizar perfiles de usuarios, los sistemas de información que permiten combatir el fraude en las comunicaciones, los nuevos sistemas de localización espacial de los teléfonos móviles y al tiempo de conservación de los datos.

En relación con el comercio electrónico, se analizó el papel de los Servicios de Proveedores de Internet, las garantías de seguridad y confidencialidad de los datos, la posibilidad de trazar perfiles de consumidores y de los internautas en general, las transferencias para la UE de datos obtenidos a través de páginas web publicadas fuera de Europa y las comunicaciones comerciales no solicitadas. Fueron debatidos los aspectos ligados a la firma y certificación digital, a la

necesidad de transposición de la Directiva de Comercio Electrónico, así como a la cuestión de ley aplicable. Los fenómenos de concentración empresarial, con la posible centralización de información personal procedente de varias empresas, constituye un problema adicional a la luz de la transparencia y de la información que deben marcar el tratamiento de datos personales.

En cuanto a los flujos de datos transfonterizos, fue evaluada la situación de los regímenes de protección adecuada de los Estados fuera de la UE y la importancia de la existencia de cláusulas contractuales tipo para varios sectores de actividad -financiero, seguros, compañías aéreas, recursos humanos-. Las Autoridades reconocieron, en el momento actual, la dificultad y la indeterminación jurídica y práctica de la aplicación del Safe Harbor, Puerto Seguro, que facilita la transferencia de datos hacia los Estados Unidos de América.

En cuanto al crédito y solvencia, fueron destacados aspectos relativos al tratamiento de datos por parte de las entidades financieras y otras empresas de informaciones comerciales, habiendo sido resaltada la necesidad de armonización de procedimientos relativos a la apreciación de los riesgos de crédito, a los ficheros de información positiva y negativa, a los plazos de conservación de la información "negativa" y de la información sobre "saldo cero" y los parámetros de concesión de crédito de acuerdo con las decisiones individuales automatizadas -credit scoring-.

En relación con América Latina, las dos Autoridades acordaron dar un nuevo impulso para promover un régimen de protección de datos de los países iberoamericanos, teniendo en cuenta las relaciones privilegiadas que España y Portugal tienen con esta zona.

La Comisión Nacional de Protección de Datos y la Agencia de Protección de Datos manifiestan su pleno apoyo y consagración de una Carta de Derechos Fundamentales de la Unión Europea, del derecho a la privacidad.

Las dos Autoridades acordaron mantener una estrecha colaboración en el futuro, mejorando la información mutua en cuanto a las decisiones adoptadas.

La Autoridad de Control Portuguesa y la Autoridad de Control Española señalan que la privacidad es un derecho fundamental que la tecnología debe respetar.

14. COOPERACIÓN CON LOS PAÍSES DEL CENTRO Y ESTE DE EUROPA

La Agencia de Protección de Datos considera de la mayor importancia la consolidación de un espacio europeo de respeto a la intimidad de las personas, siendo particularmente sensible al desarrollo de la misma en los países candidatos a la integración como miembros de pleno derecho de la Unión Europea.

Fruto de este interés son los proyectos de colaboración que se han mantenido con diversos países del Centro y Este de Europa, revistiendo especial importancia los llevados a cabo con la República Checa y Polonia.

En el caso de Chequia y como continuación a los trabajos emprendidos en el año 1999, en el que una delegación de dicho país visitó la Agencia durante tres días para conocer el funcionamiento de la misma de primera mano, con vistas al establecimiento de una Autoridad similar en dicho país.

La creación de la Oficina Checa de Protección de Datos Personales se produjo en el año 2000, nombrándose Presidente de la misma al Dr. Karel Neuwirt. A resultas de estos hechos, dicha Autoridad puso en marcha un Proyecto de Hermanamiento con un organismo similar de alguno de los Estados miembros de la UE, en el marco del programa PHARE.

La Agencia de Protección de Datos se presentó como candidata a este Proyecto de Hermanamiento, resultando adjudicataria del mismo. En virtud de este proyecto, liderado por parte española por el Director de la Agencia de Protección de Datos, un miembro de la misma se desplazará a Praga durante un año en calidad de Consejero Pre-Adhesión. Este Consejero tendrá la misión de colaborar con la nueva Autoridad con un enfoque eminentemente práctico y basado en transmitir la experiencia española en la creación de un organismo similar.

Para ello, coordinará las distintas actividades del proyecto, incluyendo la presencia de varios expertos a corto plazo, en su mayoría miembros de la Agencia de Protección de Datos, que se desplazarán a Chequia para impartir diversos seminarios y responder a todas aquellas cuestiones que se les planteen por parte de las autoridades checas.

En relación con Polonia, este país aprobó en 1997 una Ley de Protección de Datos Personales que pretende establecer un nivel de protección de datos equiparable a los estándares de la Unión Europea (Directiva 95/46/CE), incluyendo la creación de una autoridad independiente (Inspección General) encargada de velar por el cumplimiento de lo establecido en la misma. Además, en el año 1998, el Parlamento Polaco nombró a la Dra. Ewa Kulesza como la primera Inspectora General para la Protección de Datos de Polonia, con rango de Ministra, momento a partir del cual comenzó a organizarse dicha institución

Desde estos tempranos momentos, la Agencia de Protección de Datos ha mantenido estrechos contactos con la Inspección General de Polonia, aportándole su experiencia en todo aquello que pudiera resultarle útil.

Fruto de dicha colaboración, fue la invitación realizada al Director de la Agencia de Protección de Datos para visitar Varsovia con el objeto de dar a conocer, de una manera más directa, nuestro modelo de protección de datos.

Esta visita del Director, acompañado de un grupo de expertos de la Agencia de Protección de Datos, se llevó a cabo en el mes de mayo, y, tras dos intensos días de trabajo, que incluyeron una conferencia del Director de la Agencia sobre la Ley española y nuestra experiencia en la creación de un ente de estas características así como un encuentro con los principales medios de comunicación polacos, se invitó a la Dra. Kulesza a visitar España para que pudiera comprobar in situ la labor y los métodos de la Agencia española.

La Sra. Kulesza visitó España durante los días 16 y 17 de octubre acompañada de una delegación de la Inspección General. En el transcurso de la visita, la delegación polaca se reunió con el Director y con las distintas Unidades de la Agencia de Protección de Datos, pronunciando una conferencia en la sede del Consejo Superior de Cámaras de Comercio, Industria y Navegación en la que explicó la experiencia polaca en la implantación de un sistema de protección de datos y ofreciendo a continuación, junto con el Director de la Agencia, una rueda de prensa.

También hay que mencionar la participación de un representante de la Agencia de Protección de Datos en el Seminario celebrado en Varsovia, en el mes de diciembre de 2000, sobre Protección de Datos en el Sector Asegurador, en el que se presentó la normativa y estado de la cuestión en España.

Por otro lado, la Organización No Gubernamental ucraniana Privacy Ukraine, que tiene como objetivo fundamental el promover la adopción de medidas legislativas sobre protección de datos en dicho país acordes con los estándares europeos, le solicitó al Director de la Agencia que prologara un libro editado por ella en el que se incluían todos los textos legales europeos relevantes en la materia y que pretendía fomentar el conocimiento de la misma en Ucrania.

15. OTRAS ACTIVIDADES DE ÁMBITO INTERNACIONAL.

El año 2000 vio la finalización de las negociaciones entre los Estados Unidos de América y la Unión Europea respecto de la declaración de adecuación del sistema de Puerto Seguro. En el transcurso de las mismas, el Director de la Agencia de Protección de Datos recibió, a petición del mismo, al Subsecretario de Comercio de los Estados Unidos, Sr. David Aaron, quien deseaba explicarle personalmente la postura del Gobierno de los Estados Unidos en esta materia y hacerle llegar la seriedad del compromiso del mismo en la defensa de la intimidad de los ciudadanos europeos cuyos datos se transfirieran a los Estados Unidos amparados en dicho estatuto.

El Director de la Agencia manifestó al Sr. Aaron que la adopción de un acuerdo en esta materia es una decisión política que escapa a su ámbito de atribuciones. No obstante, señala que la Agencia ha autorizado muchas transferencias internacionales a empresas ubicadas en los Estados Unidos vía un contrato examinado por la misma para asegurarse de que se ofrecen las garantías necesarias y que, desde su punto de vista, el sistema de Puerto Seguro adolecía de una serie de carencias fundamentales provenientes de la inexistencia de una autoridad de control independiente en los Estados Unidos encargada de hacer cumplir el acuerdo y de la posibilidad de transferencias ulteriores a terceros países sin ninguna garantía.

En este punto, la Sra. Barbara Wellbery, que asistía a la reunión en su calidad de asesora para asuntos de comercio electrónico del Sr. Aaron, garantizó al Director que nunca se permitiría la transferencia ulterior a un tercer país sin que exista un contrato que haya sido aprobado por la Unión Europea.

Como punto final, el Director insistió en la necesidad de contar con un texto final consolidado en el que se aclarasen las dudas existentes y que permitiera la emisión de un dictamen final por parte del Grupo del Artículo 29, señalando que, no obstante, la decisión final está en manos de los representantes de los gobiernos de los Estados miembros en el seno del Comité del Artículo 31, representación que es política y no la ejerce la Agencia de Protección de Datos.

Aparte de esta reunión, el Agregado Comercial de la Embajada de los Estados Unidos de América en España, el Sr. Mark C. Johnson, se mantuvo en contacto con el Director de la Agencia para mantenerle informado de la postura americana según avanzaban las negociaciones y solicitando su opinión en diversas ocasiones.

También es de destacar la visita que realizó a la Agencia el Sr. Bruce Slane, Comisionado de Protección de Datos de Nueva Zelanda, en la que mantuvo una reunión con el Director y el Comité de Dirección de la Agencia, en la que ambas partes tuvieron la oportunidad de intercambiar sus puntos de vista respecto de los temas que más les preocupaban y, en concreto, sobre el marco legal para la transferencia de datos personales a Nueva Zelanda desde la UE, asunto de especial actualidad al estarse produciendo en aquellos momentos las negociaciones que concluyeron en el Acuerdo de Puerto Seguro entre los Estados Unidos de América y la Unión Europea; la colaboración mutua en el asunto de las réplicas del fichero de la Asociación Contra la Tortura existente en servidores neozelandeses y la situación legal y funcionamiento en España de los ficheros de solvencia patrimonial y crédito.

Además, hay que señalar la visita de tres días realizada a la misma por D. Leonardo Cervera, alto funcionario de la Unidad de Protección de Datos de la Comisión de las Comunidades Europeas, durante la que tuvo la oportunidad de comprobar la forma de trabajo y de abordar los distintos problemas de las diferentes unidades de la Agencia, con las que mantuvo fluidas e intensas reuniones de trabajo, haciendo especial hincapié sobre los problemas reales y los procedimientos de trabajo de todas ellas.

De la misma manera, la Agencia de Protección de Datos recibió la visita del Sr. Eric Freysselinard, Inspector de la Administración del Ministerio del Interior de la República Francesa encargado del estudio para la puesta en marcha de un documento de identidad electrónico, interesado en conocer tanto la normativa española como la opinión de la

Agencia sobre esta materia.

Igualmente es digna de mención, la colaboración de la Agencia de Protección de Datos con la Autoridad italiana en el marco del Proyecto Falcone. En efecto, Il Garante per la protezione dei dati personali, puso en marcha un proyecto en el que se pretendía identificar los principales problemas y divergencias existentes para la aplicación de los principios de protección de datos en el ámbito del III Pilar comunitario (Asuntos de Justicia e Interior). Con tal fin, se celebraron sendas reuniones con representantes de las fuerzas de seguridad europeas (La Haya) y del Poder Judicial (París), para, finalmente, realizar una sesión final, en Roma, a la que estuvieron invitadas las autoridades de control europeas y que contó con la asistencia de un representante de la Agencia de Protección de Datos.

Como principales conclusiones de las actividades llevadas a cabo dentro del Proyecto Falcone se pueden citar las siguientes:

1. En los Estados miembros la protección de datos se aplica a los tratamientos llevados a cabo por las fuerzas de seguridad pero, en general, sus reglas y principios no se aplican a la actividad de los servicios secretos

2. Existe una escasa armonización de las reglas en el ámbito de la actividad judicial, lo que nos llevaría a preguntarnos si los derechos de los ciudadanos europeos en este ámbito están mejor o peor protegidos en función del Estado miembro del que sean nacionales

3. Las cuestiones relativas al mantenimiento de las medidas de seguridad adecuadas, a la clara identificación del responsable de los tratamientos, a las etiquetas correspondientes a niveles de confidencialidad y a la fiabilidad de la información no deben de ser problema para ningún servicio de seguridad

4. Existen problemas de armonización y de gestión en la actualización de los datos relativos a ciudadanos absueltos y a los plazos de conservación de la información en función de su tipología o de los delitos a que hacen referencia, siendo el problema más complejo el de la conservación de la información relevante para la resolución de crímenes en serie

5. No existe un enfoque armonizado sobre la utilización de técnicas de vigilancia ni sobre el periodo de retención de los datos así obtenidos, existiendo un problema importante para establecer dicho periodo en relación con la lucha contra el crimen organizado

6. Es importante no transformar la privacidad, el derecho a la protección de datos, en algo que pueda llegar a ser visto por los ciudadanos como un obstáculo para garantizar su seguridad utilizando los medios acordes a la realidad social del momento

7. No se puede esperar que la tecnología resuelva todos los problemas, ya que siempre será necesario un marco jurídico fiable que garantice en último término los derechos de los ciudadano.

En otro orden de cosas, el Director de la Agencia ha mantenido durante el año 2000 diversos contactos con personalidades iberoamericanas con el objeto de promover la adopción de medidas legislativas en dichos países que permitieran la duración de adecuación de los mismos para, de esa manera, evitar que se puedan llegar a dar problemas en los intercambios comerciales entre los mismos y la Unión Europea.

Entre los más relevantes se pueden citar las reuniones mantenidas con Dña. Mariela B. Budiño, Asesora del Senador Nacional de la República Argentina, D. Alcides H. López, que desempeñó un papel relevante en la posterior adopción de la Ley de Habeas Data argentina y a la que se proporcionó abundante información y documentación sobre la legislación española al igual que a D. Adrián Vargas, Magistrado de la Corte Suprema de Costa Rica, que había manifestado un gran interés por conocer la legislación española, ya que el derecho a la protección de la intimidad está también recogido en la Constitución costarricense.

Igualmente se mantuvieron contactos con el entonces Embajador de México en España, D. Juan José BrÚmer y con D. Eugenio Marulanda Gómez, Presidente de la Confederación de Cámaras de Colombia (CONFECÁMARAS), en las que, de nuevo, se puso de manifiesto la necesidad de que en ambos casos se adoptaran las necesarias medidas legislativas para alcanzar un nivel adecuado de protección de datos.

Y ya para finalizar, citar la participación de representantes de la Agencia de Protección de Datos en Conferencia Internacional sobre Sistemas de Información de Crédito, celebrada en los Estados Unidos de América durante los días 23 y 24 de junio, en la que, además de moderar la sesión dedicada a la "Construcción de mejores sistemas de información de crédito", impartió una ponencia con el título "El régimen de los ficheros relacionados con la solvencia patrimonial y crédito en el Derecho español" y en el Seminario organizado por CEN/ISSS, en Bruselas, con el lema "Estandarización - Una herramienta de negocio para la protección de datos", en el que desarrolló el tema "Por qué es importante la privacidad".

MEMORIA DE 2000 - OTRAS ACTIVIDADES

1. COLABORACION CON OTRAS ENTIDADES

De las relaciones que la Agencia de Protección de Datos mantiene con otras entidades deben destacarse dos: La Agencia de Protección de Datos de la Comunidad de Madrid y el Defensor del Pueblo.

Durante el año 2000 han continuado desarrollándose las relaciones con la Agencia de Protección de Datos de la Comunidad de Madrid en el marco de la estrecha colaboración existente entre ambas entidades.

La entrada en vigor el 14 de enero de 2000 de la Ley Orgánica 15 /1999, de Protección de Datos de Carácter Personal, ha determinado que ambas Instituciones hayan intensificado el intercambio de información sobre las novedades de la norma y los criterios para su mejor aplicación.

Adicionalmente, las dos entidades han colaborado en la difusión de la LOPD mediante la participación directa en seminarios públicos organizados por cada una de ellas.

Fruto de esta colaboración ha sido, asimismo, la emisión por parte de la APD de un informe sobre el borrador de ante - proyecto de Ley de Protección de Datos de la Comunidad Autónoma de Madrid.

En lo que se refiere al Defensor del Pueblo, la Agencia debe comunicar a esta Institución las resoluciones en las que se declara una infracción por parte de responsables de ficheros de titularidad pública. En estos casos la Agencia debe efectuar el seguimiento de las medidas adoptadas para evitar la infracción informando de ello al Defensor del Pueblo.

Durante el año 2000 el Director de la Agencia se reunió con el Defensor del Pueblo en funciones, con objeto de cambiar impresiones sobre el seguimiento de los expedientes tramitados por la Agencia y remitidos al Defensor del Pueblo.

Junto con el cumplimiento de tales obligaciones y del espíritu de colaboración que presiden las relaciones entre las dos Instituciones, el Director de la Agencia presentó personalmente la Memoria anual al Defensor del Pueblo propiciando un intercambio directo de opiniones sobre respectivas competencias.

Mención específica merecen, también, las actividades de la Agencia con las Universidades tanto públicas como priva - das.

Estas actuaciones se han dirigido a tres objetivos distintos.

En primer lugar se han abordado los problemas de las propias Universidades como responsables de ficheros.

En segundo lugar la Agencia ha participado en "masters" programados por las Universidades para facilitar una forma - ción especializada a estudiantes nacionales y extranjeros.

Finalmente, la Agencia ha suscrito convenios de colaboración con las Instituciones docentes dirigidas a facilitar la realización de prácticas por parte de sus alumnos que les permitieran acceder a un conocimiento directo de las actua - ciones realizadas en materia de protección de datos.

Los Convenios de formación se han suscrito con las Universidades de Pau (Francia) en colaboración con el Centro de Estudios Europeos de la Universidad de Alcalá de Henares y Universidad Complutense de Madrid.

La Agencia ha sido particularmente sensible a la necesidad de participar conjuntamente con los sectores afectados en la resolución de los problemas que la aplicación de la normativa de protección de datos ha planteado a colectivos específicos.

A este respecto debe destacarse la complejidad que la aplicación de la LOPD y sus normas de desarrollo han produ - cido en el ámbito de Corporaciones en las que confluyen el ejercicio de funciones administrativas delegadas con la representación de intereses corporativos.

Es el caso de los Colegios Profesionales y Consejos Generales de las distintas profesiones, de las Cámaras Oficiales de Comercio, Industria y Navegación y del Consejo General del Notariado.

Para analizar estas cuestiones la Agencia ha suscrito Protocolos de colaboración con las mismas que contemplan la creación de grupos de trabajo cuya actividad posibilita aclarar el carácter público o privado de los ficheros de los que son titulares y, ulteriormente, informar de las medidas que, en cada caso, permitan un mejor cumplimiento de la Ley.

En términos generales, dados los recursos humanos disponibles, la Agencia ha tratado de estimular las relaciones con entidades que agrupen a numerosos responsables de ficheros tales como el Consejo General del Notariado, la Unión Profesional, el Consejo Superior de Cámaras Oficiales de Comercio, Industria o Navegación y asociaciones empresa - riales o de consumidores y usuarios. El objetivo de estas relaciones ha sido el de permitir una síntesis de los principales problemas que afectan a una colectividad de responsables de ficheros y el de dar una respuesta unificada respecto de

la aplicación de la Ley que sea posteriormente difundida entre la colectividad de sus miembros por parte de sus organizaciones representativas.

Por último, debe reseñarse la presentación pública de la Memoria anual de la Agencia, que tuvo lugar el 15 de junio de 2000.

La presentación de la última Memoria había sido realizada en la sede del Consejo Superior de Cámaras de Comercio, Industria y Navegación con el objetivo de aproximar el conocimiento de la normativa de protección de datos a los sectores empresariales. La presentación de la Memoria de 1999 pretendió que tal aproximación se produjera respecto de otros sectores afectados eligiéndose, a tal efecto, el Consejo General de Consumidores y Usuarios. Además del Director de la Agencia intervinieron en la presentación miembros del Consejo. La presentación contó con una nutrida representación de medios de comunicación.

2. PARTICIPACION DEL DIRECTOR DE LA AGENCIA EN CONFERENCIAS, SEMINARIOS, JORNADAS Y REUNIONES INSTITUCIONALES.

Durante el año 2000 se han intensificado las actividades del Director de la Agencia dirigidas a facilitar el conocimiento de la normativa española de protección de datos mediante la participación en foros públicos y la celebración de reuniones específicas con responsables de ficheros.

El objetivo de estas actividades es de carácter preventivo dado que tratan de impulsar un conocimiento directo por parte de los sectores afectados por la norma, permitiendo la resolución de los temas que les afectan concretamente.

Tales actuaciones han sido impulsadas desde el primer momento por el Director de la Agencia y han sido requeridas expresamente por los Portavoces de los Grupos Parlamentarios en las comparecencias celebradas, en las que han resaltado la necesidad de desarrollar actuaciones preventivas que traten de limitar la iniciación de procedimientos sancionadores.

La entrada en vigor de la Ley Orgánica 15/1999, de 13 de diciembre, el 14 de enero de 2000 ha determinado que un número muy relevante de las intervenciones del Director haya tenido como objeto la explicación de las novedades que esta norma implica respecto de la derogada LORTAD.

El principal grupo de intervenciones realizadas por el Director de la Agencia se ha dirigido a operadores económicos responsables de los ficheros.

En este sentido, el Director de la Agencia ha intervenido en multitud de foros públicos con participación de aquéllos. Estas intervenciones se han referido, como antes se señaló, a las novedades más relevantes introducidas por la LOPD, con especial referencia a los ficheros de entidades financieras, ficheros de información sobre solvencia patrimonial y crédito, publicidad, distribución comercial, telecomunicaciones y medidas de seguridad.

La relación directa con los responsables de ficheros se ha completado con las numerosas reuniones mantenidas a solicitud de aquéllos en los sectores antes citados a los que se añaden otros tales como los de transferencias internacionales de datos vinculadas a servicios en Internet, correo electrónico, cobro de deudas, medios de comunicación, construcción, energía, publicaciones y salud.

Las intervenciones del Director de la Agencia se han dirigido, asimismo, de forma específica a los representantes de consumidores y usuarios.

En relación con las asociaciones de consumidores y usuarios la Agencia tanto ha participado en foros públicos organizados por aquellas asociaciones, como ha mantenido reuniones específicas para abordar los temas que se han planteado. Pueden destacarse, en este ámbito, las mantenidas con Oficinas de Información al Consumidor, así como las relacionadas con servicios financieros y con usuarios de Internet.

ACTIVIDADES DIRECTOR: CONFERENCIAS, PONENCIAS Y JORNADAS		
FECHA	**LUGAR**	**ACTIVIDAD**
17/1/00	MADRID	**Curso Monográfico sobre "La Protección de Datos en España", organizado por la Universidad Carlos III Título ponencia: El derecho a la intimidad y su consideración por la Declaración de las NNUU, el Convenio Europeo de Derechos Humanos de 1950, la Constitución Española y otros instrumentos internacionales**
27/1/00	MADRID	Seminario sobre la Ley Orgánica de Protección de Datos, organizado por ASNEFTítulo Ponencia: **La nueva Ley de Protección de Datos de Carácter Personal.**
9/2/00	MADRID	II JORNADAS DE PROTECCIÓN DE DATOS SANITARIOS EN LA COMUNIDAD DE MADRIDTítulo Ponencia: **La nueva Ley de Protección de Datos.**
14/2/00	BARCELONA	Curso sobre Protección de Datos en la Escuela de Derecho Cuatrecasas
15/2/00	MADRID	Jornadas de Protección de Datos organizadas por el Instituto de Europeos Expertos (IEE) Apertura de Honor
25/2/00	MADRID	Master de Psiquiatría Legal, Hospital Gregorio MarañónTítulo Ponencia: **Funciones de la Agencia de Protección de Datos**
29/2/00	MADRID	Apertura de Honor Jornadas organizadas por el Institute for International ReseachTítulo Ponencia: **Nueva Ley de Protección de Datos**
2/3/00	MADRID	Master de Informática y Derecho de la Universidad Complutense Título Ponencia: Ley de Protección de Datos, Funciones de la Agencia.

6/3/00	BARCELONA	Segundo curso de iniciación al derecho de la publicidad organizado por la Asociación de Autocontrol de la Publicidad Título Ponencia: Marketing Directo y protección de datos personales.
20/3/00	MADRID	Curso especializado de Derecho Informático y de las Telecomunicaciones, organizado por GRUPO RECOLETOS Título Ponencia: Principales Novedades de la Ley de Protección de Datos Personales y Funciones APD
22/3/00	MADRID	Curso Superior de Seguridad de la Información, organizado por Belt Ibérica y la Universidad Autónoma de Madrid Título ponencia: Exigencias de la nueva ley de protección de datos.
23 y 24/3/00	BALEARES	Jornadas De Protección De Datos, organizadas por la Asociación de Usuarios de Banca (AUSBANC)Título Ponencia: **Principales aportaciones de la nueva Ley 15/99 de protección de datos de carácter personal**
29/3/00	MADRID	Presentación del INFORME SEIS de la Sociedad Española de Informática de la Salud.
29/3/00	MADRID	Clausura I Jornadas de Bioética de la UNED
25/4/00	MADRID	Apertura del Congreso SECURMÁTICA 2000 Título Ponencia: Nuevos horizontes legislativos de la Protección de Datos Personales en España.
11/05/00	HUELVA	Ciclo de Conferencias "Derecho y Nuevas Tecnologías" organizado por la Universidad de Huelva. Titulo Ponencia: La nueva Ley de Protección de Datos. Funciones de la APD.
25/05/00	BILBAO	Seminario "La nueva Ley de Protección de Datos y el Reglamento de Medidas de Seguridad", organizado por Cuatrecasas Abogados y la Asociación para el Progreso de la Dirección. Título Ponencia: Principales novedades introducidas por la nueva Ley Orgánica de Protección de Datos y el Reglamento de Medidas de Seguridad.
31/5/00	BARCELONA	ESADE (Programa de Doctorado) Conferencia sobre la Agencia de Protección de Datos
01/06/00	MADRID	Jornadas sobre Derechos Fundamentales organizadas por la revista "La Ley" Título Ponencia: La Protección del derecho de la intimidad
15/06/00	MADRID	Jornadas sobre la Protección de Datos de Carácter Personal y los Colegios Profesionales, organizadas por el Consejo General de Enfermería y Patrocinadas por Unión Profesional. Título Ponencia: Principales aportaciones de la nueva ley orgánica 15/99, de 13 de diciembre, de Protección de Datos de carácter personal.
22 y 23/6/00	NAVARRA	Jornadas Conjuntas APD-Universidad de Navarra sobre Protección de la Privacidad.Título Ponencia: **Aspectos principales de la legislación española de protección de la intimidad en las telecomunicaciones**
07/07/00	SALAMANCA	Jornadas sobre Derecho e Informática, organizadas por la Universidad de Salamanca. Título Ponencia: La Agencia de Protección de Datos: Funciones. Novedades de la Ley 15/99.
12/07/00	LA CORUÑA	IV Escuela de Verano del Poder Judicial Título Ponencia: Regulación del tratamiento automatizado de los datos de carácter personal. El secreto bancario. Comunicaciones Judiciales y Administrativas.
14/07/00	RONDA	Curso de Verano de la Universidad Rey Juan Carlos sobre Derecho y Nuevas Tecnologías Título Ponencia: Las bases de datos judiciales en la nueva LOPD
18/07/00	MADRID	Jornadas Internet y Derecho - Curso de Verano de la Universidad Autónoma de Madrid Título Ponencia: Protección de Datos
22-23/09/00	MADRID	Sesión de expertos sobre "La Justicia ante el Reto de la Sociedad de la Información" organizada por la Federación Iberoamericana de Asociación de Derecho e Informática.
10/10/00	MADRID	IV Master en Informática y Derecho Conferencia de Apertura
23/10/00	LEON	Jornadas X Aniversario de la Oficina Móvil de Información al Consumidor de León.Título Ponencia: **La seguridad de los datos personales**

24/10/00	MADRID	II Jornadas LOPD'2000. La Ley de Protección de Datos Personales y el Reglamento de Medidas de Seguridad, organizadas por Informáticos Europeos Expertos (IEE) Conferencia de Apertura
27/10/00	MADRID	Foro de Recursos Humanos, organizado por la Asociación Española de Directores de Personal, Grupo Recursos Humanos Farmacia. Título Ponencia: **Protección y Seguridad de Datos**
23-24/11/00	ZARAGOZA	Jornadas sobre Internet, Registros de Morosos y Derecho al Honor, Concentración Empresarial y Registros Públicos, organizada por AUSBANCTítulo Ponencia: **Experiencia práctica de la APD ante la nueva Ley 15/99.**
04/12/00	MADRID	Jornadas Protección de Datos de Carácter Personal, organizadas por la Federación Española de Religiosos de la Enseñanza.Título Ponencia: **Ficheros de Datos Personales: Razones de la Ley. Definición de dato personal. Definición de fichero. Clases de ficheros. Características. Responsable del fichero. Inscripción en el Registro. APD.**
04/12/00	MADRID	Jornada sobre Protección de Datos en el Sector de las Telecomunicaciones, organizadas por la Universidad Pontificia de Comillas. Instituto de Informática Jurídica. Presentación del libro del Profesor Miguel Angel Davara
13/12/00	MADRID	Curso Superior dedicado al Derecho de las Nuevas Tecnologías, organizado por la Universidad San Pablo-CEU Apertura de Honor

3. JORNADAS SOBRE "PROTECCIÓN DE LA PRIVACIDAD TELECOMUNICACIONES E INTERNET" (PAMPLONA, 22 Y 23 DE JUNIO DE 2000)

En el ejercicio de sus competencias, y con el fin de lograr un mejor conocimiento de la ley y tratar en profundidad temas de la mayor actualidad e interés, la Agencia de Protección de Datos ha organizado unas**Jornadas sobre "Protección de la Privacidad, Telecomunicaciones e Internet"** en colaboración con la **Universidad Pública de Navarra**, que tuvieron lugar en **Pamplona** los días**22 y 23** de junio de 2000.

En las Jornadas se abordaron los siguientes temas:

"El derecho a la intimidad como derecho fundamental en la Constitución Española".

Excmo. Sr. D. Rafael de Mendizabal y Allende. Magistrado del Tribunal Constitucional.

"Aspectos principales de la legislación española de protección de la intimidad en las telecomunicaciones".

Ilmo. Sr. D. Juan Manuel Fernández López. Director de la Agencia de Protección de datos.

"La protección de Datos en Internet y en los demás servicios de telecomunicaciones"

Ilmo. Sr. D. José Manuel Villar Uribarri. Abogado del Estado.

"Comercio electrónico, intimidad y derechos de los consumidores"

Dª Mª Angeles Egusquiza. Profesora Titular de Derecho Civil..Universidad Pública de Navarra. Magistrado suplente

"Riesgos para la privacidad derivados de las nuevas tecnologías en Telecomunicaciones e Internet"

D. Javier Rivas Alejandro. Abogado. Responsable del Departamento del Derecho de las Tecnologías de la Información del Landwell (Price Waterhouse Coopers)

" Comunicación de la Administración con los ciudadanos a través de Internet".

Ilmo. Sr. D. Pablo Lucas Murillo de la Cueva. Jefe de Gabinete de la Presidencia del Consejo General del Poder Judicial

"Transacciones electrónicas en Internet"

D. Emilio Aced Félez. Inspector de Datos de la Agencia de Protección de Datos.

"Directiva de telecomunicaciones", especial referencia a Internet.

D. Leonardo Cervera Navas. Funcionario de la Comisión Europea.

4. PREMIOS "PROTECCIÓN DE DATOS PERSONALES"

Se convocó la CUARTA EDICIÓN DEL PREMIO "PROTECCIÓN DATOS PERSONALES", con una dotación de un millón de pesetas, y un accésit dotado de 250.000 pesetas, con la finalidad de profundizar en el estudio del desarrollo del artículo 18.4 de la Constitución. Según las Bases de la Convocatoria el premio se otorgará a la mejor obra científica, original e inédita de autores españoles o extranjeros, que verse sobre la materia de la protección de datos personales informatizados, desde un plano jurídico, ya sea con un enfoque estrictamente teórico o a partir de experiencias concretas basadas en nuestro ordenamiento o en el Derecho Comparado. El Jurado establecido en las Bases de la convocatoria otorgó por unanimidad el Premio a la obra "Regulación Jurídica de los Tratamiento de Datos Personales realizado por el Sector Privado en Internet" de la que es autora Dª Mª de los Reyes Corripio Gil-Delgado. De la referida obra la Agencia ha realizado una edición de 1000 ejemplares para su entrega y difusión institucional.

* En la obra premiada la autora indica en la introducción de su libro la problemática que en la actualidad tienen las autoridades de control en la aplicación de las leyes de protección de datos se produce ante la dispersión y atomización de la información que circula a través de la red de ordenadores a ordenadores interconectados entre sí, entre cualquier país del mundo sin que el interesado pueda llegar a sospechar donde puede haber datos personales de él y el tratamiento que se pueda estar realizando con los mismos.

* El jurado acordó por unanimidad conceder el premio valorando a la hora de decidir el acertado enfoque teórico desde el punto de vista jurídico y también desde el tecnológico dada la claridad con la que se exponen los conceptos y las técnicas usadas en Internet para cualquier persona profana en la materia. Asimismo, es un ejemplo práctico y estructurado de los diferentes escenarios que se producen en Internet con respecto al tratamiento de los datos personales.

El trabajo consta de cinco capítulos, cada uno de ellos con áreas temáticas respecto al tratamiento de los datos personales, así como la política de privacidad que deberán incluir estos tratamiento para cumplir y garantizar a los ciudadanos sus derechos emergentes en la nueva sociedad global.

El libro es una herramienta útil para todos los ciudadanos y especialmente para aquéllos que cada día en mayor número se acercan a navegar por la red por motivos muy diversos. Así se habrá cumplido la doble finalidad que persigue la Agencia de Protección de Datos al convocar anualmente este premio: incentivar el estudio desde el punto de vista jurídico de los diversos problemas que plantea la protección de datos y servir, con la publicación de la obra premiada a una concienciación de los ciudadanos en sus derechos y en las mejores formas de protegerlos.

Se concedió un accésit, dotado con 250.000 pesetas, a la obra titulada "La Transmisión Internacional de Datos Personales y la Protección de la Privacidad en Latinoamérica", de la que es autor D. Pablo Andrés Palazzi, investigador argentino. El autor pone de relieve la situación actual del tratamiento de datos personales en la América Latina, cuestión ésta no sólo poco conocida en nuestro país sino muy poco investigada y tratada en los países del indicado continente.

- Se convocó asimismo el **PRIMER PREMIO DE PERIODISMO DE "PROTECCIÓN DE DATOS PERSONALES"** dotado con 250.000 pesetas, al que podían concurrir los trabajos publicados en medios de comunicación escritos que tengan por tema central la protección de datos personales.

El premio fue concedido, asimismo por unanimidad a D. Bonifacio de la Cuadra Fernández por el miento continuado llevado a cabo de las cuestiones relativas a la protección de datos y a las actividades de la Agencia en un diario de máxima difusión nacional.

El día 15 de diciembre fueron entregados, por el Director de la Agencia, los premios en un acto celebrado en Madrid al que acudieron el Consejo Consultivo de la Agencia de Protección de Datos, invitados, y medios de comunicación.

MEMORIA DE 2000 - ANEXO I - INSTRUCCIÓN 1/2000, DE 1 DE DICIEMBRE, DE LA AGENCIA DE PROTECCIÓN, RELATIVA A LAS NORMAS POR LAS QUE SE RIGEN LOS MOVIMIENTOS INTERNACIONALES DE DATOS

Este documento se encuentra en la Base de Datos de legislación.

MEMORIA DE 2000 - ANEXO II - RESOLUCIÓN DE 30 DE MAYO DE 2000, DE LA AGENCIA DE PROTECCIÓN DE DATOS, POR LA QUE SE APRUEBAN LOS MODELOS NORMALIZADOS EN SOPORTE PAPEL, MAGNÉTICO Y TELEMÁTICO, A TRAVÉS DE LOS QUE DEBERÁN EFECTUARSE LAS SOLICITUDES DE INSCRIPCIÓN EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS.

MEMORIA DE 2000 - ANEXO III - INFORMES PRECEPTIVOS EVACUADOS EN 2000

PROYECTO DE DISPOSICIÓN	SOLICITADO POR	FECHA
Informe al borrador del Proyecto de Real Decreto por el que se establece el plazo para implantar las medidas de seguridad de nivel básico previstas por el Reglamento aprobado por el Real Decreto 994/1999 de 11 de junio.	Secretario General Técnico de Justicia	13/01/00
Informe referido al Proyecto de Real Decreto por el que se crea y regula la Comisión Interministerial para actuar contra las actividades vulneradoras de los derechos de propiedad intelectual e industrial	Vicesecretario General Técnico de Justicia	21/01/00
Informe referido al Proyecto de orden por la que se amplía el anexo de la Orden de 26 de julio de 1994, por la que se regulan los ficheros con datos de carácter personal gestionados por el Ministerio de Agricultura, Pesca y Alimentación.	Subsecretario del Ministerio de Agricultura, Pesca y Alimentación	14/02/00
Informe referido al segundo borrador de Orden Ministerial por la que se crea la Comisión del Ministerio de Sanidad y Consumo para la gestión de un censo de personas con hemofilia y otras coagulopatías congénitas que hayan desarrollado el virus de la hepatitis C como consecuencia de haber recibido tratamiento en el sistema sanitario público.	Secretario General Técnico del Ministerio de Justicia(Se solicita a Justicia por el S.G.T. de Sanidad)	24/02/00
Informe referido al Proyecto de Real Decreto sobre Inscripción de los españoles en los Registros de Matrícula de las Oficinas Consulares en el extranjero.	Secretario General Técnico del Ministerio de Justicia(Se solicita a Justicia por el S.G.T. de Exteriores)	21/03/00
Informe referido al Proyecto de Orden Ministerial por la que se crea un fichero de carácter sanitario relativo al censo de personas con hemofilia y otras coagulopatías congénitas que hayan desarrollado el virus de la hepatitis C como consecuencia de haber recibido tratamiento en el sistema sanitario público.	Secretario General Técnico del Ministerio de Sanidad y Consumo	14/04/00

PROYECTO DE DISPOSICIÓN	SOLICITADO POR	FECHA
Informe referente al Proyecto de Real Decreto por el que se desarrolla el régimen de control interno ejercido por la Intervención General de la Seguridad Social	Secretario General Técnico del Ministerio de Justicia(Se solicita a Justicia por la Intervención de la Seguridad Social)	26/04/00
Informe referido a la propuesta de norma con rango de Ley para la actualización de la regulación de la Central de Información de Riesgos del Banco de España (CIRBE)	Director General del Banco de España	04/05/00
Informe referido al Proyecto de Orden Ministerial por la que se amplía la de 21 de julio de 1994, por la que se regulan los ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo	Secretario General Técnico del Mº de Sanidad y Consumo	11/07/00
Informe referido al Proyecto de Orden Ministerial por la que se actualiza la relación de ficheros automatizados de datos de carácter personal del Ministerio de Fomento	Secretario General Técnico del Mº de Fomento	11/07/00
Informe referente al Proyecto de Orden Ministerial por la que se regulan los ficheros automatizados de datos de carácter personal del Ministerio del Interior sobre ADN	Secretario General Técnico del Ministerio de Justicia (Se solicita a Justicia por el Ministerio del Interior)	27/07/00
Informe referente al Proyecto de Real Decreto por el que se regula el proceso de evaluación para el registro, autorización y comercialización de biocidas.	Secretario General Técnico del Ministerio de Justicia (Se solicita a Justicia por el Mº de Sanidad)	27/07/00
Informe referente al Proyecto de Orden Ministerial por la que se cresa un nuevo fichero de datos de carácter personal del Mº de Sanidad sobre nuevas infecciones del V.I.H	Secretario General Técnico del Ministerio de Justicia (Se solicita a Justicia por el Mº de Sanidad)	18/08/00

PROYECTO DE DISPOSICIÓN	SOLICITADO POR	FECHA
Informe al Borrador de Anteproyecto de Ley de Protección de Datos de la Comunidad de Madrid.	Directora de la APD de la Comunidad de Madrid	08/09/00
Informe sobre la Proposición No de Ley del Grupo Socialista relativa a las actuaciones necesarias para impedir el tratamiento masivo de datos de carácter personal por parte de los Operadores de Telefonía	Directora del Gabinete del Ministro de Justicia	25/09/00
Informe referido al Proyecto de Orden por la que se crea el fichero de agricultores asegurables para la gestión de los seguros de rendimientos incluidos en los planes anuales de seguros agrarios combinados	Secretaria General Técnica del Mº de Agricultura, Pesca y Alimentación	26/09/00
Informe referente al Proyecto de orden Ministerial por la que se actualiza la relación de ficheros automatizados de datos de carácter personal del Ministerio de Fomento a efectos de determinar su conformidad con lo dispuesto en la Ley Orgánica 15/99.	Secretario General Técnico del Mº de Fomento	30/10/00
Informe referente al Proyecto de Orden Ministerial por la que se crea un nuevo fichero de datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información de Nuevas Infecciones (SINIVITH)	Secretario General Técnico del Mº de Sanidad	30/10/00
Informe referente al Proyecto de Real Decreto por el que se aprueba el Reglamento sobre Protección Sanitaria contra Radiaciones Ionizantes	Subdirector General de Coordinación Normativa y Relaciones Institucionales. Mº de Economía	26/12/00
Informe referente al Proyecto de Orden Ministerial por la que se actualiza la relación de ficheros automatizados de datos de carácter personal del Ministerio de Fomento	Secretario General Técnico del Mº de Fomento	26/12/00
Informe referente al Proyecto de Orden Ministerial por la que se crean en la Delegación del Gobierno para el Plan Nacional sobre Drogas diversos ficheros automatizados de datos de carácter personal	Secretario General Técnico del Mº de Justicia (Se solicita a Justicia por el Ministerio del Interior)	26/12/00
TOTAL		**21**

MEMORIA DE 2000 - ANEXO IV - SESIÓN NÚM. 6 CELEBRADA EL JUEVES, 14 DE DICIEMBRE DE 2000

COMISIONES

Año 2000 VII Legislatura Núm. 123

CONSTITUCIONAL

PRESIDENCIA DE LA EXCMA. SRA. D.a MARGARITA MARISCAL DE GANTE

Sesión núm. 6 celebrada el jueves, 14 de diciembre de 2000

ORDEN DEL DÍA:

Comparecencia del señor director de la Agencia de Protección de Datos (Fernández López) para dar cuenta de las actuaciones que está llevando a cabo dicha Agencia ante la reiterada vulneración de la confidencialidad de los datos de carácter personal por parte de algunas entidades financieras y, en especial, por parte de las Administraciones públicas. A solicitud del Grupo Parlamentario Socialista.

(Número de expediente 212/000281.).... 3568

Se abre la sesión a las once y cinco minutos de la

mañana.

La señora **PRESIDENTA:** Se inicia la sesión.

Comparecencia del director de la Agencia de Protección de Datos para dar cuenta de las actuaciones que está llevando a cabo dicha Agencia ante la reiterada vulneración de la confidencialidad de los datos de carácter personal por parte de algunas entidades financieras y, en especial, por parte de las administraciones públicas, a solicitud del Grupo Parlamentario Socialista.

Señor López Garrido.

El señor **LÓPEZ GARRIDO:**

Señor director de la Agencia de Protección de Datos, gracias por su comparecencia ante esta Comisión, que en este periodo de sesiones se ha reunido fundamentalmente para escucharle a usted, es decir, que está convirtiéndose en una de las personas más asiduas a la misma y le agradecemos mucho su disponibilidad para ello. Seguiremos convocándole y si tiene usted esa amabilidad, que seguro que la tendrá, le veremos más a menudo en esta Comisión. El objetivo de la comparecencia, como ha dicho la señora presidenta, es que nos informe sobre las actuaciones que está llevando a cabo la Agencia de Protección de Datos ante la reiterada vulneración de los datos de carácter personal por parte de quienes más pueden, si quieren, vulnerar dichos datos y la intimidad de las personas, como son las grandes entidades financieras y las propias administraciones públicas, que son quienes más poder tienen para hacerlo y quienes cuentan con más datos personales para ello. Por eso es especialmente importante que la Agencia de Protección de Datos informe a esta Comisión sobre qué actuaciones está llevando a cabo, qué instrucciones está impartiendo y qué acciones ha decidido poner en marcha para combatir las vulneraciones ya producidas o la posible vulneración de lo que la reciente sentencia del Tribunal Constitucional de 30 de noviembre de este mismo año, conocida hace muy pocos días, llama el derecho fundamental a la protección de los datos.Precisamente a la luz de esta sentencia resulta particularmente importante su comparecencia hoy, porque, aunque la misma sin duda se discutirá, puesto que todo es discutible, es una sentencia del Tribunal Constitucional, máximo órgano intérprete de la Constitución en este país. Yo me atrevería a decir que constituye un hito hístorico dentro de la jurisprudencia del Tribunal Constitucional y, desde luego, dentro de lo que es la interpretación de ese derecho fundamental a la protección de datos.

El Tribunal Constitucional establece claramente en esta sentencia la existencia de un derecho fundamental a la protección de datos distinto del derecho a la intimidad, definiéndolo como el poder de control de la persona sobre sus datos personales, sobre su uso y destino, con el propósito de impedir el tráfico ilícito y lesivo para la dignidad y derecho del afectado. Por tanto, es un poder de disposición permanente sobre esos datos, lo que significa que cualquiera de los derechos de las personas, no solamente los derechos fundamentales, sino todo tipo de derechos, los que tienen que ver con el honor, con la ideología o con la intimidad personal y familiar, todos los datos relacionados con las personas deben ser protegidos en su ejercicio y como patrimonio personal, de forma que cualquier persona tenga una capacidad de control sobre los mismos y sepa en todo momento son expresiones literales de la sentencia quiénes tienen sus datos y pueda negarse a facilitarlos o bien modificarlos. Nosotros, en la mañana de hoy, nos vamos a referir, sobre todo, a las entidades financieras y a las grandes compañías y a las administraciones públicas.

Desde un principio conviene destacar que su comparecencia adquiere hoy una especial relevancia cuando hemos conocido hace unos días una importantísima sentencia del Tribunal Constitucional, el cual nunca se había pronunciado con esa intensidad, con esa fuerza, con esa amplitud y con un carácter fuertemente creador e innovador sobre lo que llama, que también es una cierta innovación, el derecho fundamental a la protección de los datos.

Esto pone en cuestión muchos de los artículos de la reciente Ley de Protección de Datos, no solamente los dos que se han considerado inconstitucionales, sino algunos otros.

Pero ésta no es la razón de su comparecencia, sino que vamos a pedirle que nos haga una interpretación de la ley, ya que tendremos ocasión de preguntarle al Gobierno la semana que viene, puesto que hay una interpelación planteada a ese respecto.

Lo que queremos es que, a la luz de esa sentencia, nos hable usted sobre las vulneraciones que se han producido, o que se pueden producir, respecto del derecho fundamental a la protección de datos por parte de las entidades financieras, las grandes compañías y las administraciones públicas.

En cuanto a las entidades financieras, quisiéramos destacar algunas cuestiones que nos preocupan, fundamentalmente dos.

Nos preocupa la facilidad con la que las compañías financieras se hacen con los datos personales.

Estas compañías tienen los datos de prácticamente todos los ciudadanos de este país y, además, datos personales de especial relevancia, referidos a la situación económica, al patrimonio personal e incluso a la salud de las personas.

Se ha conocido, y fue una de las razones para pedir su comparecencia, el hecho de que aparecieran en unos contenedores listados de datos personales de gente que provenían de entidades financieras, de instituciones oficiales como el Instituto de la Mujer y otras entidades, como fue destacado por los medios de comunicación, escandalizándose de la falta de seguridad que existe en estas compañías, que tienen que ser especialmente responsables de los datos que custodian; daba la impresión de que no había esa seguridad, ya que aparecieron centenares o miles de datos íntimos sobre personas, nada menos que en contenedores de basura, lo que pone de manifiesto que falta mucho para llegar a un razonable nivel de seguridad en la custodia de esos datos.

Ese es un primer elemento preocupa, el asunto de la seguridad, relacionado también con algunas administraciones públicas, como el de las instituciones sanitarias, pero a eso me referiré después, porque por el momento quiero mantenerme en el ámbito de los que son entidades financieras privadas, grandes compañías financieras o compañías de telecomunicación.

Quería referirme a ese segundo elemento que nos preocupa que es el de la cesión.

Demasiado a menudo, y se ha convertido ya en una práctica habitual, esas grandes compañías trafican con datos personales con poco cuidado por los derechos de los ciudadanos.

Desde luego, a la vista de la sentencia del Tribunal Constitucional se podría decir que son claramente inconstitucionales esas prácticas de cesión de datos con absoluta desenvoltura y sin tener en cuenta los principios elementales que al comienzo de la Ley de protección de datos aparecen, por cierto, respecto del asunto de la cesión.

Permita que le mencione a título de ejemplo, para no situarnos en el plano de la abstracción, algunas cosas que suceden, y nos gustaría saber qué tiene que decir sobre ello la Agencia de Protección de Datos.

Las compañías financieras, pero no solamente ellas, (bancos, cajas de ahorro), sino también otras compañías, por ejemplo, de telecomunicación (Telefónica, Retevisión u otras empresas de servicios públicos, Iberdrola, Repsol), están sistemáticamente enviando cartas a los ciudadanos, a los usuarios, que son millones y millones, todos los ciudadanos de este país, comunicándoles simplemente mediante una carta como otra cualquiera (perdida entre muchas) que si en 30 días o en el plazo que sea no dicen nada en contrario van a utilizar como les parezca sus datos personales.

Es una interpretación, a nuestro juicio la directiva de la Ley de protección de datos y, desde luego, en este caso inconstitucional a la vista de lo que dice la sentencia del Tribunal Constitucional.

Dice claramente que una persona tiene que saber en todo momento dónde están sus datos, que tiene que dar su consentimiento expreso a que esos datos se utilicen.

Las compañías que hacen esto están utilizando sus datos en la inmensa mayoría de los casos, sin saber realmente si las personas a las que mandaron las cartas las recibieron.

Si a alguien le llega una carta en la que le dice que en el plazo de 30 días la compañía en cuestión no sabe si le llegó, porque no se manda por correo certificado con acuse de recibo.

Hay mucha gente que se queja porque no le ha llegado dicha carta y, sin embargo, se encuentra con que sus datos personales figuran en un listado que es vendido, con el que se trafica con él, porque evidentemente los objetivos fundamentales son económicos; es el tráfico mercantil con datos personales sin tener el afectado ni arte ni parte ni saber siquiera que eso se está produciendo.

A la luz de la nueva sentencia del Tribunal Constitucional esta práctica es inaceptable.

Quisiéramos saber también la opinión de la Agencia de Protección de Datos a este respecto, no sólo en cuanto a lo que

ahora ha sucedido, sino también a la vista de esta sentencia, que la Agencia de Protección de Datos, evidentemente como cualquiera en este país, puede desconocer que se ha producido.

Otro elemento, otro ejemplo, que quisiéramos destacar es el de los listados de riesgos de las compañías financieras. Este es un caso muy delicado. En este país hay, fundamentalmente, dos registros de riesgos de solvencia económica, el RAI y el Asnef. El RAI, registro de aceptaciones impagadas, y el Asnef, acrónimo de Asociación nacional de entidades financieras, son listados de riesgos, de insolvencia, que constituyen auténticas cesiones entre las compañías financieras.

Se ceden esos datos entre sí, porque ese registro central, naturalmente, es un registro en el que se produce una cesión de esos datos.

Una compañía financiera que ha tenido un moroso comunica a todas las demás este dato importante, personal y que afecta a la intimidad de la persona.

Lo relevante, desde el punto de vista de las garantías personales, es la forma en que eso se hace.

Cuando un banco que toma una letra y la descuenta la recibe devuelta, automáticamente lo comunica a un organismo, el RAI, que ni siquiera tiene personalidad jurídica, y le proporciona todos los datos de la letra; lo comunica, a su vez, al supuestamente afectado y digo supuestamente porque en muchos casos se falsifican las aceptaciones y le dice que sus datos han ingresado en ese registro.

El problema es que a veces hay nombres iguales de compañías o de personas, que se confunden, y hay con frecuencia aceptaciones falsificadas.

Y la consecuencia es que a esa persona afectada se la pone automáticamente en la picota.

Es la muerte civil para mucha gente aparecer en ese registro de la forma en que se aparece.

La consecuencia es que esa persona no hará operaciones financieras con nadie, será un apestado desde el punto de vista de su solvencia y no le darán créditos; las consecuencias son terribles para esa persona. Sin embargo, lo que no hay es garantía alguna. Si se le dijera a esa persona: hemos recibido esta comunicación de una letra devuelta, o de lo que sea, y usted puede estar en ese registro, díganos algo; en ese caso habría un procedimiento contradictorio y se podría uno defender. Pero no, lo que le comunican es que está ya sin remedio en ese registro, y luego vaya usted a reclamar al maestro armero.

Esa es la gran cuestión del RAI, registro de aceptaciones impagadas, y del Asnef, que es un registro de morosos, por ejemplo, en créditos al consumo, con cantidades muy pequeñas en muchas ocasiones, y en el que puede haber multitud de equivocaciones. Por cierto, si alguien paga la deuda que se le atribuye, esa persona permanece seis años más en ese registro, aunque haya pagado, lo cualpara mucha gente supone realmente una situación tremendamente dramática. Desde luego, ese es un atentado a la protección de los datos personales y es otra de las cuestiones que nos gustaría saber cómo la ve y qué piensa a ese respecto la Agencia de Protección de Datos.

Todo esto va unido a las compañías de seguros y a la sucesión de datos, que en este caso sí que ha sido prevista, desde luego con la oposición del Grupo Socialista y de otros grupos, en la vigente Ley orgánica de protección de datos, en una disposición adicional, como sabe, que permite un registro central de cesión de datos entre compañías de seguros y que, a la luz de la sentencia del Tribunal Constitucional está claramente tocada de inconstitucionalidad a nuestro juicio.

El Defensor del Pueblo no recurrió ese apartado, pero si lo hubiera recurrido ante el Tribunal Constitucional es muy seguro que el Tribunal Constitucional lo hubiera declarado inconstitucional, a la luz de la doctrina que hay a lo largo de todas las sentencias. Con eso pasa como en otros artículo de esa ley.

En segundo lugar, en el otro bloque de cuestiones referidas a las administraciones públicas, no se le oculta al director de la Agencia de Protección de Datos que la sentencia del Tribunal Constitucional ha sido una auténtica bomba al respecto, porque a partir de ese momento queda claro que la recogida de información de datos personales, la cesión entre administraciones públicas de personales, el acceso y la rectificación de los ciudadanos a partir de ahora es algo absolutamente obligado, porque el Tribunal Constitucional ha declarado parcialmente inconstitucionales los artículos 21 y 24 de la Ley orgánica de protección de datos. Esto es lo que permitía a las administraciones públicas, por razones absolutamente abstractas como el interés público y cosas por el estilo, negarse a informar a la gente de los datos que tenían en su poder, negarse a dar información, poder ceder esos datos entre administraciones públicas como le pareciera, sin que nadie lo supiera. Esto no es posible después de la sentencia del Tribunal Constitucional, pero lo ha sido hasta este momento.

Me gustaría saber qué piensa hacer la Agencia de Protección de Datos para arreglar, durante este año en que han estado vigentes esos artículos de la Ley orgánica de protección de datos, los desaguisados que se han producido respecto de este tráfico de datos personales entre administraciones públicas, que se apoyaban en una determinada regulación que hoy ya no existe porque ha sido declarada inconstitucional por el Tribunal Constitucional.

Para terminar el tema de las administraciones públicas, me voy a referir a dos ejemplos.

Me gustaría saber a título informativo qué pasa con el asunto de las multas de tráfico.

Las multas de tráfico significan una cesión de datos en la práctica entre corporaciones municipales y organismos públicos hacendísticos.

¨Qué pasa en este momento con esas cesiones? ¨Qué se va a hacer al respecto a la luz de la sentencia del Tribunal Constitucional? Habrá que elaborar algunas instrucciones para que se conozca dónde están los datos personales de las personas afectadas en todo momento, como dice la sentencia del Tribunal Constitucional. Otro elemento que también quisiéramos destacar, porque nos parece muy relevante, es el de las instituciones sanitarias, la seguridad de los datos que hay en las instituciones sanitarias. A ese respecto, la situación de seguridad en muchos centros sanitarios es realmente lamentable en cuanto a datos de la salud de la gente que ingresa en ellos. En muchos casos en esos centros hay ordenadores cuyas bases de datos contienen una importantísima información de los pacientes, están conectadas a Internet sin las medidas de seguridad necesarias que eviten la entrada en dichos ficheros de personas no autorizadas. No creo que sea el momento de abusar de la Comisión hablando de una cuestión técnica, pero resulta que muchos centros de salud están incorporados a ciertos programas.

Hay uno que se llama OMI, otro que se llama SIAP, pero ninguno de ellos tiene posibilidad de encriptar datos y de tener un registro de acceso donde se deje referencia de quién ha entrado para conocer esos datos, qué ha visto y si ha modificado algo, como aparece en el reglamento de seguridad.

En comunicaciones que recibimos de distintos centros de salud de este país se pone de manifiesto este enorme problema. No hay medidas de seguridad suficientes en los centros de salud.

Los datos sanitarios de esas personas están expuestos a los **hacker**s, en este caso los **hackers** contra esos ficheros; lo hablábamos en su última comparecencia en esta Comisión. Como digo, muchos de esos datos están conectados a Internet sin medidas de seguridad, por lo que se pueden conseguir esos datos.

Estos son algunos de los temas que queremos plantearle, dentro del conjunto de las cuestiones que afectan a la seguridad y a la protección de los datos personales, en relación con actuaciones de grandes compañías o entidades financieras y administraciones públicas, que adquiere especial importancia a los pocos días de que el Tribunal Constitucional haya elevado el nivel de la protección de los datos muy por encima del nivel de protección de la vigente Ley de protección de datos.

Esto tiene que tener algunas consecuencias, porque incluso ha llegado a declarar inconstitucionales artículos fundamentales de la Ley de protección de datos. Me gustaría que el director de la Agencia de Protección de Datos nos informase a ese respecto y, en concreto y específicamente, de los temas que hemos destacado, con objeto de no hacer de esta comparecencia una cuestión excesivamente abstracta o generalista.

La señora **PRESIDENTA:**

Tiene la palabra el señor compareciente, director de la Agencia de Protección de Datos.

El señor **DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS**

(Fernández López): Buenos días a todos.

Como ya les he manifestado en anteriores ocasiones, siempre es una satisfacción para mí estar aquí con ustedes, porque, en definitiva, el control parlamentario de la Agencia de Protección de Datos ayuda a mantener lo que ya establece la Ley sobre la independencia de su director. Por otro lado, me permite poder conocer a través de sus sugerencias las opiniones de los ciudadanos, las deficiencias que pueden existir y que los ciudadanos les transmiten a ustedes como sus representantes, para poder actuar más eficazmente en un futuro. Por ello, repito, es una satisfacción para mí estar aquí y siempre me encontrarán dispuesto a comparecer tantas veces como lo consideren necesario. Voy a ir contestando a las preguntas y consideraciones que S.S. me ha hecho.

En primer lugar, respecto al tema de las entidades financieras y su seguridad, al hilo de una denuncia presentada primero en la prensa y que luego nos llegó materialmente a la Agencia, a raíz de dos trabajos periodísticos, uno, referido a ciertos listados de datos financieros y bancarios de los ciudadanos que aparecieron en contenedores, y otro referido a datos de las administraciones públicas.

Esto ocurrió a finales de septiembre o primeros de octubre de este año. Ante esto, lo primero que hizo la Agencia, como es lógico, fue mandar a sus inspectores a comprobar la realidad de estos documentos y ver si tenían conexión con los ficheros de las entidades bancarias, o si, por el contrario, como se ha demostrado en algunos casos, procedían del simple descuido de los ciudadanos. Todos podemos comprobar como muchos ciudadanos tiran al lado de un cajero del que se puede extraer dinero con tarjeta de plástico los comprobantes en los que figura el número y el saldo de su cuenta; así están dejando un rastro que parece ser que no pertinente.

Pero cada uno, dentro de la libertad que la ley le concede, puede utilizar sus datos como libremente quiera.

Como les decía, empezamos a comprobar estas denuncias, y como consecuencia de las inspecciones, se iniciaron tres procedimientos sancionadores a unas entidades bancarias, concretamente a Caja Madrid, a Banesto y a La Caixa, por presunta infracción del artículo 9, en relación con los artículos 4.2, 8.1 y 20 del reglamento de medidas de seguridad, y

por presunta vulneración del artículo 10 de la Ley de protección de datos, que establece la obligación de guardar el debido secreto.

Respecto de otras entidades bancarias, como consecuencia de la inspección, se ha decretado el archivo de las actuaciones, concretamente en el supuesto del BBVA. También como consecuencia de esas denuncias se han realizado inspecciones a diversas administraciones públicas, concretamente a la Agencia Estatal de Cooperación Internacional del Ministerio de Asuntos Exteriores y a la Dirección General de Asuntos Económicos del Ministerio de Defensa. En estos dos casos también se ha procedido al archivo de las actuaciones de los procedimientos, al comprobar que los datos que circulaban por ahí no eran debidos a datos o documentación procedentes de la Administración, sino de los propios interesados.

En cambio, sí se han abierto procedimientos a la Agencia Estatal de Administración Tributaria y al INSS por apreciar también una posible vulneración del artículo 9 de la Ley de protección de datos, referido a la seguridad, en relación con los anteriores artículos citados del reglamento de medidas de seguridad y del artículo 10 de la propia ley, como vulneración de secreto.

Estos procedimientos están en tramitación. Con respecto a los bancos, coincido absolutamente con S.S. en que además manejan cantidad de datos nuestros muy grande. Yo, lo pongo por ejemplo, cuando tengo que asistir a un curso o seminario para mejor dar a conocer la ley, digo que los bancos tienen más datos de nosotros que los que incluso nosotros conocemos.

Ahí va a estar domiciliado el pago de nuestras nóminas, nuestros ingresos; ahí van a pagarse los recibos que tenemos domiciliados, van a conocer lo que consumimos de energía, en telefonía; si a través de la tarjeta de crédito gastamos mucho o poco en bienes de gran consumo en otros bienes de lujo, etcétera.

Incluso van a conocer nuestra ideología, si nuestros hijos van a colegios religiosos o a colegios laicos, ahí estarán también domiciliados los recibos, o si contribuimos a partidos políticos, a iglesias u otras confesiones religiosas o laicas. El banco va a tener una información extensa y privilegiada de nosotros. Es normal en el mundo en que nos toca vivir, porque hoy día es absurdo pensar que nadie va a ir a pagar el recibo de la compañía de teléfonos a la ventanilla o el de la compañía del gas o de la electricidad y de la misma forma tampoco va con dinero efectivo cuando quiere hacer compras. Lo normal es que se utilice cada día más el llamado dinero de plástico.

Es una realidad y no pasa nada si el banco mantiene estos datos en la relación contractual que tiene establecida con sus clientes. Últimamente han aparecido técnicas que a mi modo de ver son un paso más de invasión a la intimidad como son el **scoring,** el **data mining** y el **data warehous**e, que ya permiten sacar perfiles del individuo, es decir, sabiendo lo que yo gasto en unos determinados bienes, sabiendo lo que gano, sabiendo a quien contribuyo, se pueden llegar a obtener perfiles del ciudadano. Esto es un paso más dentro de la intimidad de los ciudadanos, así tienen numeradas la Agencia estas prácticas. A no ser que estén expresamente consentidas por el ciudadano, están absolutamente prohibidas. Son prácticas graves porque son invasoras de la intimidad del ciudadano.

Con esto le quiero decir que la Agencia es consciente de la problemática que las entidades financieras pueden plantear y es constante vigilante de sus actuaciones. Con respecto a estos listados que aparecían en los contenedores si bien es un hecho lamentable y se estádepurando su responsabilidad, estos bancos sí tenían unas medidas implementadas de seguridad auténticas y del nivel corrrespondiente y tenían su documento de seguridad, como han podido comprobar nuestros inspectores en la realización de sus funciones, pero tuvieron este fallo, llamémoslo así, que habrá que depurar. A mí el asunto me pareció de tal gravedad que no sólo ordené la iniciación de las correspondientes funciones inspectoras y luego consecuentes procedimientos a los que me he referido, sino que me puse inmediatamente en contacto con el presidente de la asociación de la banca privada para poner en su conocimiento esos hechos y sugerir que se tomaran las medidas adecuadas. Me dio pronta respuesta, ha hablado con los presidentes de todos los bancos, están dentro de las posibilidades conscientes de esta situación y han prometido que no volverá a repetirse en ningún caso.

De otro lado, para tratar todos estos temas, hemos mantenido una reunión con los miembros de la Asociación española de la banca privada, concretamente con su secretario general y con dos de sus asesores, yo mismo y con diversos funcionarios de la Agencia, para comprobar también qué es lo que estaba pasando en toda esta materia de los registros de morosos del RAI, de la AsnefEquifax y otros. Como ya he manifestado, todas estas prácticas de un país dentro de la intimidad, a mi modo de ver están absolutamente prohibidas, a no ser que exista consentimiento expreso del ciudadano, aunque en algunos supuestos hemos detectado que estas prácticas se han llevado a cabo sin consentimiento, no en caso concreto de los bancos sino en el caso concreto de compañías dedicadas a la telefonía móvil. Y por supuesto en esos casos hay varias resoluciones de la Agencia sancionando rigurosamente una práctica que, como digo, va más allá de la simple intimidad de los datos generales, si no es entrar ya a conocer incluso nuestros comportamientos. Por lo que respecta a las administraciones públicas, el otro tema objeto de comparecencia, como ya he dicho, se han abierto procedimientos, estamos pendientes de su tramitación y resolución, pero también debo indicar a SS.SS. que a raíz de la publicación en el Boletín Oficial del Estado de los reales decretos 557/2000 y 688/2000, de reestructuración de diversos departamentos ministeriales, me he dirigido por escrito a los diferentes subsecretarios de estos departamentos, al objeto de recordarles la obligación de cada responsable de fichero de titularidad pública de notificar los efectos de inscripción en el Registro General de Protección de Datos de la creación, modificación o supresión de ficheros que tengan datos de carácter personal, con el fin de suministrar al ciudadano la adecuada información de dónde puede practicar sus derechos de acceso, rectificación y cancelación.

Los responsables de estos ficheros de titularidad pública, tengo que decirlo, han dado y están dando cumplida

respuesta a los requeri mientos de la Agencia, están inscribiendo las modificaciones que proceden, en algunos casos dictando las normas habilitantes, si es que hay un cambio de titularidad, y en ese aspecto no se ha ilutrado mayor problemática. Después, si le parece, hablaré de la sentencia del Tribunal Constitucional, porque engloba un poco todos los temas a los que S.S. ha hecho mención. También se ha referido a los listados de riesgos, principalmente los del RAI y AsnefEquifax.

Ahora también hay otros muchos, porque este tema se está desarrollando mucho en nuestro país y las grandes multi - nacionales que trabajan la materia, ahora no sólo está Asnef, está Transunión y está Hesperian, dos grandes multina - cionales que en el resto de Europa se dedican a este tipo de registros de morosos, están funcionando en nuestro país. A este respecto quiero recordar que la sanción más importante, económicamente hablando, que la Agencia de Protec - ción de Datos ha impuesto en toda su historia fue a una empresa dedicada a registros de morosos y fue por importe de 163 millones de pesetas una, como muy grave en su grado máximo, otra como grave en su grado máximo y otra como leve.

Este es un tema que nos preocupa, para lo cual, además, hubo que hacer una investigación compleja, en este caso concreto, porque se había montado toda una estructura de sociedades interpuestas para que, al final, resultara sancionada sólo la que era insolvente, y la que verdaderamente utilizaba los datos y ganaba sustanciales cantidades por ello resultara con multas menores. A base de un estudio completo de todo este grupo y de las actuaciones inspec - toras se pudo levantar el velo jurídico y sancionar a quien considerábamos el auténtico responsable y así se ha hecho, aunque, por supuesto, la resolución está pendiente del recurso que han interpuesto ante la Audiencia Nacional.

También quiero decir, con respecto a estas sociedades que se dedican a la creación de ficheros, que la regulación que ya establecía nuestra entidad, y que ahora lo hace, a mi modo de ver con más rigor, la vigente Ley de protección de datos en su artículo 29, viene a diferenciar dos tipos de actuaciones: por un lado, las sociedades que se dediquen a prestación de servicios de información sobre solvencia patrimonial y crédito dice el artículo 29 sólo podrán tratar datos de carácter personal obtenidos de los registros de las fuentes accesibles al público establecidas al efecto o procedente de la información facilitada por el interesado. En este supuesto no hay problema. Son datos que, en un caso, son públicos y, en otro, es el propio interesado el que los facilita. El problema surge cuando se trate de datos relativos a cumplimiento o incumplimiento de obligaciones dinerarias.

En el caso del incumplimiento, que es el más grave (porque, como bien ha dicho S.S., es meter a alguien en un registro de insolvencia y considerarle ya como alguien que no va a poder obtenercrédito o que le va a ser difícil de obtener), la Agencia de Protección de Datos ya había dictado en el año 1995 una instrucción para posibilitar un mayor rigor en la introducción de estos datos. En el caso, que aquí ya puede ser, de la introducción de datos, no sólo porque los facilite el interesado sino el acreedor o persona que actúe por su cuenta e interés, se va a exigir que la deuda sea líquida y vencida y que exista requerimiento previo, según establece concretamente la instrucción 1/95, norma primera, de la Agencia de Protección de Datos.

Con lo cual el problema indicado, en principio, por S.S. de que pueda introducirse a alguien que no es deudor, porque se le ha falsificado la letra, no debe darse, puesto que tiene que haber requerimiento previo, y si hay requerimiento previo y se tacha de falsedad la firma no se debe estar en ese fichero. También tengo que todo este grupo de empresas, que ha sido uno de los objetivos principales de la Agencia durante mucho tiempo, y si ustedes ojean nuestra memoria verán que hay multitud de ejemplos y de expedientes abiertos a estas empresas, hoy día afortunadamente se han ido disciplinando y las cosas van por mejor camino; y van por mejor camino porque ya no se introduce a nadie sin ser deudor moroso y, además, no se le mantiene por el tiempo que no deba ser incluido. Por otro lado, ha surgido ahora la posibilidad de crear los ficheros positivos, porque el artículo 29, en su párrafo segundo, señala que podrán tratarse datos de carácter personal relativos al cumplimiento o incumplimiento, o sea, también al cumplimiento.

Las entidades dedicadas a proporcionar esta información se han dirigido a la Agencia con la pretensión de poder introducir datos positivos, y un dato positivo es que uno paga. Si yo pago 200.000 pesetas de una hipoteca, el dato positivo es que yo he pagado 200.000 pesetas de una hipoteca, pero no la totalidad de mi crédito. Nadie tiene que saber lo que yo debo, eso no es un dato positivo, y en este sentido se les ha respondido por la Agencia. Los ficheros de solvencia positiva deberán incluir exclusivamente los datos positivos, pero no se podrán extender, porque entendemos que la previsión legal no habilita para ello, a toda la información de la solvencia de un ciudadano.

Por supuesto, esto será posible siempre que el ciudadano consienta, pero este tipo de información no podrá introdu - cirse por cuenta del acreedor. De los dos ficheros que ha señalado S.S., el que menos importancia tiene respecto a la protección de los ciudadanos es el RAI, porque en él se incluye el impago de efectos cambiarios superiores a 500.000 pesetas, y normalmente este tipo de letras no es el que circula entre los ciudadanos. Lo que viene a contener el RAI son máa bien las morosidades de las empresas y, como saben, las empresas no están bajo la protección de la Agencia de Protección de Datos. Hay que reconocer la necesidad de estos registros de morosos, pero hay que utilizar las cosas en los térmi nos en que legalmente están establecidos. Son necesarios no sólo porque están facilitando a los bancos una información que les puede resultar útil o necesaria, sino porque también se la está facilitando a las pequeñas y medianas empresas.

Muchos de los ficheros que gestiona la Asnef son ficheros sectoriales de distintos empresarios, que así conocen si los que intervienen en el sector son cumplidores o no, lo cual les es necesario, porque una pequeña o mediana empresa, en un momento de competencia como el que estamos viviendo ahora, necesita dar crédito a sus clientes y, si ese crédito luego resulta fallido, les puede llevar a situaciones irremediables.

Si a un banco no le pagan, por muy importante que sea el crédito impagado, tendrá un quebranto, pero su estructura no

llegará a tambalearse; la de una pequeña empresa, sí.

A mi modo de ver, estas empresas realizan una función también importante dentro de la economía del país, lo que pasa es que, vuelvo a repetir, tendrán que estar rigurosamente dentro del marco legal y no podrán salirse nunca de él; en ese supuesto, deberán ser sancionadas.

Ha habido ocasiones en las que la Agencia ha utilizado, incluso, la vía de la medida cautelar y ha paralizado estos ficheros cuando ha detectado graves anomalías.

Como les he manifestado, y por las actuaciones que estamos llevando a cabo, aunque seguimos vigilantes sobre el sector, desde el punto de vista de la Agencia hoy día no es de los que nos preocupe especialmente.

Su señoría se ha referido también a los registros comunes de las compañías de seguros.

Efectivamente, se aprovechó la Ley de protección de datos para modificar la Ley de contratación de seguros privados y posibilitar este tipo de cesiones, aunque limitadas a los casos concretos que en ella se establecen.

Hay que recordar que sólo se referirán a datos del tomador del seguro, no tienen que ser necesariamente los conductores, y además tienen que realizar una previa información que habilitará al ciudadano para, si no está de acuerdo, cambiar de compañía de seguros. Afortunadamente, no todo el sector se ha unido a esta práctica. Hay empresas muy importantes que se han quedado fuera, no se han unido a esta posibilidad de trasladar los datos al fichero común de Unespa, con lo cual, los ciudadanos tienen la otra opción, porque si no, la cosa sería verdaderamente más grave. A este respecto, lo que no comparto es el criterio de S.S. de que esto sea inconstitucional, porque está reglado por una ley, y el Tribunal Constitucional precisamente tacha de inconstitucionales los preceptos de la ley orgánica por el cheque en blanco que pretendía dar el legislador a las administraciones públicas a través de normas inferiores a las que tienen rango de ley, y de ahí que, por el principio de reserva de ley del artículo 53 de la Constitución, esto no era posible. Estos ficheros, si quiere usted mi opinión particular, no me gustan expresamente, pero tampoco creo que tengan un problema más serio en tanto en cuanto se va a informar a los ciudadanos antes y van a tener la posibilidad de cambiarse de compañía y, por tanto, no entrar en esos ficheros.

Un asunto importante que ha suscitado es el de las medidas de seguridad, al hilo del tema de los bancos y, en definitiva, de las grandes compañías. Esto, como saben, ha tenido un importante desarrollo este, porque es cuando ha entrado en vigor el reglamento de medidas de seguridad. En esta materia, la Agencia ha sido muy activa. A través del gabinete jurídico, ha evacuado más de cien consultas a titulares de los ficheros, a entidades y a administraciones para ayudarles al cumplimiento de la ley.

Por otro lado, desde el área de atención al ciudadano, que se ocupa expresamente de atender las preguntas, sugerencias o quejas de los ciudadanos, se han hecho un total de 282 informes exclusivamente referidos a medidas de seguridad. Además, con el fin de dar a conocer las novedades legislativas y promover su implantación por parte de las empresas y de las administraciones, tanto el personal directivo de la Agencia como yo mismo hemos participado en variedad de cursos y seminarios por toda la geografía española dando a conocer este reglamento. Especial significación tiene uno realizado, creo, en el mes de junio, aquí, en Madrid, y que trató sobre los datos de los colegios profesionales, donde, por supuesto, los datos médicos estaban en primera línea; y otro, en Toledo, sobre datos de enfermería. Por otra parte, en los diversos planes de inspección de oficio realizados por la Agencia tanto en el sector público como en el privado, para ver la adecuación de los sectores al cumplimiento de la ley, se ha investigado siempre el cumplimiento de lo relativo a las medidas de seguridad.

Igualmente, se han investigado e incoado las correspondientes actas o procedimientos sancionadores cuando, en virtud de denuncia de los afectados, se ha detectado infracción de medidas de seguridad.

En este caso, es importante la sanción impuesta a un operador de telecomunicaciones, concretamente a Telefónica de España, por infracción del artículo 9, de medidas de seguridad, en relación con los correlativos del reglamento de medidas de seguridad, infraccion tipificada como grave, por haber creado un sistema de información que no disponía de las medidas de seguridad establecidas en el reglamento, al permitir que se produjeran más de 7.000 accesos no autorizados, a través de Internet, a los datos de facturación de los abonados al citado operador. Está terminado el procedimiento y sancionada la conducta. También se ha iniciado un procedimiento sancionador a otro operador, concretamente a Telefónica Servicios y Contenidos por la Red, que explota la marca comercial Terra, por infracción del reglamento de medidas de seguridad, al no tener la contraseña o **password** de acceso de sus clientes de forma ininteligible. Como consecuencia de ello, al estar la contraseña de forma inteligible, se podía acceder a través de Internet a los datos personales de correo electrónico y otros de los clientes de la citada compañía. El procedimiento está en marcha y aún no está concluido.

También tendrán ustedes conocimiento de que la agencia ha abierto procedimientos sancionadores a diversas empresas que han participado en el concurso televisivo de **Gran Herman**o, ya que después de realizar las correspondientes actuaciones se comprobó que algunas de ellas y cuando digo algunas me estoy refiriendo fundamentalmente a la productora del programa y a la operadora de telecomunicaciones no mantenían los datos que se iban pasando entre diversas empresas, con las debidas medidas de seguridad y en algunos casos además los datos que en principio se obtienen de los concursantes estaban enriquecidos a través de test que les habían hecho con datos sobre la salud, como son los referidos al padecimiento de enfermedades mentales. Este procedimiento sigue aún pendiente de resolución, aunque creo que está en el último trámite de alegaciones y posiblemente de finalizar el mes se pueda dictar la correspondiente resolución. Por lo que se refiere a los datos sanitarios, a los que también ha hecho referencia S.S., he

de señalar que la entrada en vigor de las medidas de seguridad se ha hecho de forma paulatina; primero entran en vigor las medidas de nivel básico, el 26 de marzo de 2000, que tienen que cumplir todos; después las de nivel medio, que se tienen que implementar el 26 de junio de 2000, y, por último, las de nivel alto, que son las referidas a los datos sensibles, a los datos de salud, que se empezarán a poder exigir el año 2001, concretamente el 26 de junio de 2001. Esto por lo que se refiere a los ficheros que ya estaban declarados, es decir, a los ficheros en vigor, porque los ficheros de nueva creación en cualquier caso tienen que venir con las medidas incorporadas, del grado que les corresponda, y para estos no existen plazos de adaptación.

Por otro lado, la ley prevé que se pueda dilatar hasta tres años, que en casos en que haya graves inconvenientes para la implantación de las medidas de seguridad se pueda conceder una habilitación que llega a tres años; ello no obstante, cuando han inspeccionado las instituciones sanitarias, especialmente a través de los planes sectoriales de oficio, como los realizados el pasado año al hospital militar Gómez Ulla, al hospital psiquiátrico penitenciario de Fontcalent y al Centro Nacional de Epidemiología de la Secretaría del Plan sobre el sida, realizamos una serie de recomendaciones que, a sugerencia de ustedes en mi última comparecencia, hice llegar a la presidencia para que estuvieran a su disposición y vieran cuál había sido la actuación de la Agencia en este aspecto.

Igualmente, en la inspección realizada al Insalud en febrero del presente año, se recabó un informe sobre seguridad y confidencialidad, relativo al sistema de información del consumo farmacéutico del citado centro para hacer un estudio comparativo de dicho documento y de las
 medidas de seguridad aplicables conforme al Real Decreto 994/1999, del reglamento de medidas de seguridad, haciéndose algunas observaciones por parte de la Agencia en aquellos supuestos en que creíamos que no se cumplía suficientemente con las medidas de seguridad. También para atender las dificultades que se presentan con una nueva ley y con el reglamento, la Agencia ha firmado un protocolo con la asociación profesional que, como saben ustedes, engloba a todos los consejos generales de colegios y entre ellos está, por supuesto, el Colegio de Médicos, para ayudarles precisamente en la mejor adecuación de los sistemas a la ley. Asimismo se pretende atender a las dificultades que puede implicar para un colegio profesional, con ficheros de titularidad pública y de titularidad privada, para poder distinguir entre ambos; como los de titularidad pública tienen que buscar una norma habilitante para su creación, queremos ayudarles a cumplir con esta norma.

La última observación que quisiera hacer respecto a los ficheros sanitarios es para referirme a la incidencia que sobre los mismos puede tener el secreto profesional. Una reciente sentencia de la Sala de lo Contencioso administrativo del Tribunal Superior de Justicia de Madrid, de 12 de julio de 2000, estima un recurso contra una resolución de la Agencia de Protección de Datos y viene a declarar que el contenido del ordenador personal de un profesional de la medicina queda fuera del ámbito de aplicación de la Lortad hoy, Ley de protección de datos y de la acción inspectora de la Agencia de Protección de Datos, a lo que añade que las relaciones del médico con su paciente están ligadas por un insuprimible deber de secreto profesion y, en consecuencia, los datos de los pacientes que el médico tiene registrados en su ordenador deben quedar garantizados y salvaguardados por la confidencialidad del secreto profesional. Yo, señorías, como siempre, acato las sentencias judiciales, pero, a mi modo de ver, esta incurre en un craso error, porque el secreto profesional está protegiendo al afectado y no al médico, y si el afectado denuncia, la Agencia tendrá, creo yo, facultad para investigar qué es lo que se ha hecho con los datos de ese ciudadano, porque el ciudadano, con la denuncia, está levantando el secreto profesional. De todas formas, habrá que ver en qué supuestos sí y en cuáles no podrá intervenir la Agencia. Con carácter general, creo que podríamos tener una actuación limitada y es un tema que tenemos en estudio, pendiente de una instrucción que clarifique qué es lo que puede ocurrir con este sector.

Por último, me voy a referir a la sentencia del Tribunal Constitucional y a las indudables incidencias que la misma ha de tener sobre la actuación de la Agencia.

En primer lugar, el director de la Agencia de Protección de Datos lo que tiene que decir es que acata la sentencia, y en este caso además la acata de buen grado porque, como ha dicho S.S., es trascendental, por cuanto que viene a establecer el derecho a la protección de datos con carácter individual, y lo hace por primera vez, porque hay otras dos sentencias anteriores en que se habla del **habeas data** y del derecho constitucional vinculado a la intimidad sobre todo y a la informática. Aquí el Tribunal Constitucional viene a decir: el ciudadano va a ser dueño y señor de sus datos, se utilicen de forma informática o no. Creo que esto es algo importante y además coincide con el artículo 8 de la Carta Europea de Derechos Humanos, aprobada en Niza días pasados, donde se contiene la protección de datos de carácter personal como un derecho auténticamente independiente, por lo cual no puedo estar más que de acuerdo con la sentencia del Tribunal Constitucional. Es de agradecer al Tribunal Constitucional que haya resuelto un recurso en tan poco tiempo y eso es especialmente significativo para alguien como el director de la Agencia de Protección de Datos, que debe velar por el cumplimiento de la ley, y si una ley está en principio tachada de inconstitucionalidad y pendiendo la espada de Damocles de que pueda resultar parcial o más ampliamente inconstitucional, esto dificulta indudablemente la tarea que se le encomienda al director, por lo cual me ha parecido de una gran utilidad que la sentencia se haya dictado con esta rapidez.

Por otra parte, la claridad y rotundidad de la sentencia va a facilitar y condicionar nuestra labor de futuro.

Entrando en el análisis de la misma debo afirmar que, concretamente en los preceptos 21.1, 24.1 y todo el apartado 2, que se declaran inconstitucionales, lo que hace el Tribunal Constitucional es trasladar su doctrina ya consolidada en otras múltiples sentencias sobre la incidencia de la limitación de los derechos fundamentales, la reserva de ley y luego que deben de ser tasadas las cuestiones en que pueden dejarse o restringirse los derechos de los ciudadanos. Además la sentencia tiene otra ventaja y es que no sólo se limita a declarar la inconstitucionalidad, sino que también declara la nulidad que va implícita en la inconstitucionalidad. De no existir esta declaración, estaríamos ante un supuesto claro de necesidad de reforma legislativa, según la propia doctrina del Tribunal Constitucional, sobre todo lo explicitado en su sentencia de 20 de febrero del año 1989. Aquí, afortunadamente, hay declaración de inconstituciona-

lidad y de nulidad, con lo cual no necesitaría ley, a mi juicio, reforma legislativa, con independencia de las actitudes que se tomen por los diversos grupos parlamentarios si quieren reformarla o no. Ahora, al desaparecer ese cheque en blanco que se daba a las administraciones, la ley queda en una situación más restrictiva que la establecida por la directiva comunitaria.

El artículo 13 de la directiva comunitaria habilita para que, estableciéndolo expresamente, se puedan restringir los derechos en determinados supuestos.

Hay otro tema en el que voy a disentir de S.S., a pesar de su mayor conocimiento sobre derecho constitucional, y es el de la retroactividad de la ley.

Respecto de posibles aplicaciones retroactivas hay que señalar que si bien la nulidad declarada tiene efectos **es tun**c, es decir, ineficacia de la norma declarada nula desde su nacimiento, toda vez que la sentencia tiene efectos negativos respecto de las cesiones y de los derechos que las administraciones públicas podían ejercer en base a los preceptos declarados inconstitucionales, hay que señalar que por aplicación del principio de irretroactividad **in peius** de las disposiciones sancionadoras, conforme al artículo 9.3 de la Constitución, no podrá, a mi juicio, aplicarse la norma con efectos retroactivos. En cambio, desde su publicación en el Boletín Oficial del Estado, y si la ley no se reforma, podrá ser aplicada directamente solamente con considerar los incisos que declara inconstitucionales y nulos, aplicando por tanto la ley en el resto de su articulado. Creo que con esto he contestado a todas sus preguntas.

Si en algún caso no hubiera sido así, con mucho gusto le responderé a continuación. Nada más. Muchas gracias.

La señora **PRESIDENTA:**

¨Grupos que desean intervenir?
(Pausa.)

Por el Grupo de Coalición Canaria, tiene la palabra el señor Mardones.

El señor **MARDONES SEVILLA:**

Señora presidenta, seré breve.

Voy a comenzar por agradecer la presencia aquí del señor director de la Agencia de Protección de Datos y la amplia, detallada e instructiva información que nos ha facilitado en este trámite (también creo que ha sido muy oportuna la iniciativa del Grupo Parlamentario Socialista, con la intervención del señor López Garrido), sobre todo en la parte en la que el señor director general ha expresado su opinión sobre la aplicación de la sentencia del Tribunal Constitucional. Mi grupo se congratuló de la rapidez con la que el Tribunal Constitucional abordó esta materia, que no podía estar sometida a una dilación del alto Tribunal.

Señor director, usted ha dicho que esta sentencia del Tribunal Constitucional va a condicionar la actuación de la Agencia en el inmediato futuro. Me gustaría que me concretara, señor director, en qué aspectos fundamentales tendrá que rectificar la Agencia algunas de sus actuaciones. También al hilo de esta misma cuestión quisiera preguntarle si esto va a implicar una modificación de los actuales reglamentos, oficialmente aprobados, con los que funciona la Agencia, y si de alguna manera se van a tener que modificar o no las disposiciones de la vigente Ley 15/1999 y cuál es la situación en este momento.

Para la Administración, para la Agencia y para el Gobierno la propia Ley 15/1999 en su artículo 48, del procedimiento sancionador, obliga a acudir a la vía reglamentaria para establecer el procedimiento a seguir en la determinación de las infracciones. Quisiéramos saber qué efecto podría tener la sen tencia del Tribunal Constitucional en estas figuras que entran en el capítulo de infracciones y la calificación de la mismas. También hay que conocer si va a afectar lo que impone una posición transitoria segunda de la ley, de la utilización del censo promocional, que reglamentariamente se desarrollará para esta cuestión, porque son muchas las empresas privadas que para sus promociones comerciales, de buzoneo, de venta a empresas, etcétera, están recurriendo a este censo promocional, cuestión que viene bien delimitada en la ley, ya que dice que del censo electoral se derivan solamente lo que son las cuestiones básicas de identificación de la persona censada, y nada más, que lo que se haya obtenido del padrón municipal y lo que se ha traspasado al censo electoral se utilice como censo promocional.

Creo que este censo promocional es una de las mayores demandas, supuestamente por vía legal. Pero como la ley impone que el reglamento establecerá los plazos para la puesta en marcha del censo promocional, se produce esa situación. Igualmente, habría que saber en qué medida puede afectar esta sentencia del Tribunal Constitucional a lo que se dice también en la disposición final segunda, en la que el Gobierno queda facultado para aprobar o modificar las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente ley, si va a ser precisa una modificación reglamentaria que tenga en cuenta la sentencia del Tribunal Constitucional, porque al decir usted que la Agencia de Protección de Datos va a condicionar su actuación en los tiempos futuros, quisiera saber qué parte de esa actuación tiene que hacerse por reglamento la Agencia tiene un reglamento para ejecutarlo y cumplirlo y qué parte se efectuará a través de normas de funcionamiento interno que no requieren el rigor de un reglamento publicitado y aprobado oficialmente por el Gobierno. Dicho esto, señora presidenta, señor director general, mi grupo entiende que la Agencia viene funcionando bien, recogiendo el íritu de la Ley 15/1999, tratándose, además, como estamos viendo por las propias directivas comunitarias, debates del Parlamento Europeo y una serie de cuestiones que están surgiendo al hilo de un proceso que avanza a medida que la tecnología de la informática lo hace, y España, en relación con el

derecho comparado de otros países, está en iguales o mejores condiciones que algunos, aunque se podrían hacer modificaciones legales.

Estoy de acuerdo con lo que usted ha dicho sobre el Tribunal Constitucional, que si declara inconstitucional un determinado artículo, párrafo o precepto, se declara la nulidad del propio precepto, y en derecho es totalmente inaplicable.

Convendría, tanto por parte de los grupos parlamentarios como por parte de la Agencia que, a medida que va avanzando la comisión de infracciones administrativas porque en España se ha discutido siempre si las leyes 5/1992 y 15/1999, que tienen un capítulo de infracciones y sanciones, solamente se refieren al campo administrativo, se vaya creando una protección penal.

Usted ha recordado lo que se ha aprobado en Niza sobre la Carta Europea de los Derechos Humanos.

En las sentencias del Tribunal Constitucional se ha considerado la libertad informática como un derecho inherente a la dignidad de la persona, y respecto a esto quería preguntar si aparte de tener una protección administrativa debe tener una protección penal.

Si se están conculcando derechos fundamentales habría que pensar no sólo en mantener los capítulos, como la vigente Ley de protección de datos, donde se refleja la protección de infracciones administrativas y sus correspondientes sanciones, faltas leves, graves y muy graves, sino en si algunos comportamientos de ciudadanos o de empresas que manejan la informática y los ficheros de datos se podrían tipificar y tener penal.

No estamos hablando de aparcar un coche en un sitio prohibido, permitido o no por una ordenanza municipal de tráfico, sino que se pueden estar conculcando derechos fundamentales. Esta figura se deriva de estudios y publicaciones. Por ejemplo, el artículo 99 señala la prestación de servicios de información sobre solvencia patrimonial y crédito.

Esto lo planteaba el señor López Garrido y yo lo hago desde otro punto de vista, es decir, los derechos del ciudadano a la protección de datos y los derechos de las entidades financieras de derecho público a la protección de sus patrimonios y de sus actividades dentro de una normativa legal. Igualmente, como lo ha recordado también el señor director general, hay que aprovechar para hacer modificaciones, porque a lo largo del año 1999, en el trámite de ponencia y Comisión, en la disposición sexta introdujimos la modificación de la Ley de ordenación y supervisión de seguros privados, ya que nos encontramos con que podía haber intenciones de los usuarios, no de la compañía, de cambio de compañías de seguros, de ocultación de datos. La jefatura de Tráfico tiene el fichero más completo de automóviles que existe en el país.

No se puede circular sin matrícula y sin permiso de circulación, pero las obligaciones del seguro obligatorio pueden ser incumplidas, como de hecho se ha informado en esta Cámara periódicamente. Se pueden mezclar los datos de los ficheros de la base informática que tiene la jefatura de Tráfico con los que tienen las compañías de seguros, que son las que saben si un señor tiene o no el seguro obligatorio de circulación, y esto plantea problemas sobre si lo que se deriva de la Ley de protección de datos puede tener una futura proyección la protección penal, vía Código Penal.

La señora **PRESIDENTA:**

Por el Grupo Parlamentario Vasco (EAJPNV) tiene la palabra el señor Erkoreka.

El señor **ERKOREKA GERVASIO:**

Señora presidenta, voy a intervenir muy brevemente. Con carácter previo quiero agradecer al director de la Agencia de Protección de Datos su comparecencia de hoy y su disposición, ya habitual, a someterse, a las preguntas e informar a cuantas cuestiones se plantean en esta Comisión. En primer lugar, es forzoso expresar la preocupación de nuestro grupo, pero esto puede ser general, por la perpetración de hecho como algunos de los que han motivado la presente comparecencia del director de la Agencia de Protección de Datos; me refiero singularmente a los que recoge la secuencia del cubo de basura con papeles que recogen información detallada y puntual sobre aspectos importantes y de la intimidad de las personas.

Quiero también expresar la preocupación del grupo al que me adscribo. ¨Por qué? Por el descontrol que a veces se da en la gestión, manejo y custodia de datos de los ciudadanos, datos en muchas ocasiones sensibles, por parte precisamente como se ha puesto de manifiesto por algún interviniente de quienes más poder tienen para poder irrumpir ilegítimamente en la vida e intimidad de los ciudadanos, sobre todo administraciones públicas y grandes compañías financieras. Entidades que además, curiosamente como ha puesto de manifiesto el director de la Agencia, se da la circunstancia que tienen instaladas todas las medidas de seguridad exigidas por la Ley orgánica de protección de datos.

La preocupación se atenúa, efectivamente, porque parece, en principio, que la actuación de la Agencia es diligente, ha sido correcta y ha hecho uso de todos los mecanismos a su alcance para intentar corregir este tipo de situaciones. Tengo alguna duda, en el caso de las entidades financieras, que sea suficiente el que se haya mantenido una conversación con los responsables de la asociación de la banca privada y ési hayan comprometido a que no vuelva a ocurrir. No sé si eso es suficiente, porque no se sabe con qué disposición han dado la respuesta y si volverá a ocurrir o no.

En segundo lugar, es inevitable también hacer una referencia a la sentencia del Tribunal Constitucional y algún comentario a propósito de lo que supone a efectos de la posible modificación de la ley vigente o, en su caso, a los

efectos de la actuación de la Agencia, bien sea en el contexto de la actual normativa o bien en el contexto que eventualmente pueda aprobarse, si se decide definitivamente abordar una modificación de la ley todavía joven. Efectivamente la sentencia, como se ha puesto de manifiesto aquí, es crucial porque, por primera vez, reconoce un derecho a la protección de datos, caracterizándolo, además, como un derecho subjetivo, individual, de carácter fundamental. De la sentencia resulta la inconstitucionalidad parcial de algunos preceptos; singularmente quisiera hacer referencia ahora a la inconstitucionalidad que declara el alto Tribunal en este pronunciamiento en relación con la habilitación en blanco que se hace a la posible remisión a la vía reglamentaria de la vigente Ley de protección de datos en relación con los datos que obran en poder de las admi nistraciones públicas. Y quisiera hacer referencia a esta cuestión porque es un tema en el que mi grupo parlamentario durante la tramitación de la Ley orgánica de protección de datos puso especial énfasis se pueden analizar los antecedentes parlamentarios y se comprobará que el portavoz del Grupo Vasco insistió en reiteradas ocasiones en que esa habilitación en blanco a las administraciones, ignorando de alguna manera la reserva de ley, era problemática y resultaba contraria a la Constitución.

Por tanto, en ese sentido hay que expresar la facción, porque ya anunciamos una posible inconstitucionalidad que al final ha obtenido la confirmación del Tribunal Constitucional. Al mismo tiempo que expresar la satisfacción, quisiera subrayar la paradoja de que la defensa constitucional la haya llevado a cabo precisamente el Grupo Vasco, frente a grupos que son los grandes defensores de la Constitución. Con respecto a los efectos de la sentencia, yo creo que es una buena ocasión para repensar la ley en vigor, que tiene algunos defectos técnicos como se ha puesto de manifiesto en esta misma Comisión.

La sentencia hace unas reflexiones que permiten reabordar toda la cuestión relativa a la protección de datos.

Insisto en que sería una buena ocasión para retomar la posibilidad de modificar el texto de la ley actualmente vigente introduciendo una exposición de motivos, de la que carece, aunque no sea más que añadiendo aspectos puntuales en la excelente exposición de motivos de la Ley de 1992, que la tenía (ha declarado el Tribunal Constitucional en numerosas ocasiones que la exposición de motivos es un excelente instrumento interpretativo a la hora de determinar el alcance y contenido de muchos preceptos de la ley), e introduciendo mejoras técnicas que enriquecerían el texto de la ley y nos permitirían dotarnos de un instrumento jurídico normativo más eficaz para la consecución de estos fines de la protección de datos en el contexto de la jurisprudencia o la doctrina sentada por esta nueva sentencia del Tribunal Constitucional, que efectivamente es innovadora y que abre nuevos caminos a la configuración, a la concepción de este derecho en el ámbito de nuestro ordenamiento jurídico.

La señora **PRESIDENTA:**

Tiene la palabra, por el Grupo Catalán, el señor Jané.

El señor **JANÉ I GUASCH:**

En primer lugar, en nombre del Grupo Parlamentario Catalán (Convergéncia i Unió), quiero agradecer al director de la Agencia su comparecencia y la exposición amplia que ha realizado hoy en esta Cámara a solicitud del Grupo Parlamentario Socialista . Coincido con gran parte del sentido de su exposición y con el celo que muestra la Agencia de Protección de Datos en lo que es el objetivo principal de la misma: proteger los datos de carácter personal, datos que afectan de forma muy directa a la vida íntima de las personas y sobre todo datos especialmente sensibles. Por tanto, quiero compartir con el director de la Agencia esa preocupación y en gran parte la exposición que ha hecho hoy, así como compartimos con otros grupos parlamentarios la preocupación, que no es responsabilidad de la Agencia que usted dirige, por hechos que ocurren y que pueden parecer anecdóticos, pero todos tenemos muchas veces una sensación de desprotección por el uso que se hace de nuestros datos personales por parte de entidades financieras y aseguradoras. El hecho que provocó la comparecencia y el propio hecho de encontrar datos tirados en una entidad que precisamente cumplía con requisitos adicionales de seguridad nos encienden una luz de alarma a todos.

Yo creo, señor director, que todos los grupos estamos preocupados por estos hechos porque las nuevas tecnologías de la sociedad de la información nos abren a todos grandes posibilidades de comunicarnos, la globalización un dato puede transportarse fácilmente de una parte a otra del mundo, pero también mayores riesgos, por lo que deberemos entre todos buscar puntos de equilibrio. En el próximo período de sesiones vamos a tramitar en esta Cámara una ley que será importantísima, la ley de comercio electrónico. Esa ley abre grandes posibilidades de transacciones, de comprar y vender, pero los datos de carácter personal, datos muy sensibles como los de las tarjetas de crédito o el domicilio de las personas van a estar en la red con una posibilidad de ser conocidos por terceras personas mayor que la que tenemos actualmente. Por ello debemos buscar mecanismos de protección, pero a la vez no podemos impedir el desarrollo de las nuevas tecnologías y las nuevas formas de comercio.

Por tanto, hay una preocupación que creo que compartimos todos los grupos de esta Cámara, y desde la misma quiero apelar al director a que siga con un especial celo estos aspectos. Hay aspectos de la nueva ley que pueden ser más o menos entendidos pero que pueden ser cauces adecuados para un buen uso de los datos en el ámbito comercial, como es el censo promocional.

El censo promocional, que está previsto en el artículo 31 de la nueva ley, debe permitir encauzar la actividad comercial lícita que existe en todos los países de la Unión Europea y que en España tiene contradicciones normativas entre lo que dispone la Ley de comercio y lo que dispone la Loreg, qué datos pueden ser o no difundidos.

Debe permitirse que quien no quiera estar en ese censo no esté, buscar claramente los mecanismos de oposición, uno de ellos, que prevé la propia ley, es el documento de empadronamiento que todos los ciudadanos tienen que rellenar y

en el que se debe tener la posibilidad de decir, que no se quiere estar en el censo promocional.

A partir de ahí tendremos un censo que será el que podrán utilizar las empresas que se dediquen a la prospección comercial porque quienes están han querido estar. En consecuencia, nos evitaremos la difusión y el buzoneo de millones de cartas que muchos ciudadanos no quieren recibir porque han dicho que no quieren estar en ese censo, y para quienes quieran estarlas empresas de prospección comercial legítimamente podrán realizar su actividad.

Ayer hice una pregunta al vicepresidente segundo del Gobierno, señor Rato, para instarle a que regule el censo promocional porque depende del Instituto Nacional de Estadística. Por tanto, con las debidas garantías y controles debemos intentar buscar ese punto de equilibrio para no entorpecer lo que es la dinámica de la nueva sociedad de las telecomunicaciones, de la sociedad de la información, con la necesaria y escrupulosa garantía de la protección de los datos de carácter personal. Yo le insto a que seamos celosos pero también a que busquemos cauces de solución a problemas de interpretación jurídica que en este momento se están dando. Después, seguro que la nueva sentencia del Tribunal Constitucional nos va a permitir a todos los grupos, de esta Cámara eso sí que ya no compete al director de la Agencia reinterpretar y modificar en aspectos concretos la Ley Orgánica de Protección de Datos de carácter personal, que tiene un año de vigencia.

Con el consenso de todos los grupos parlamentarios quizá podamos hacer una modificación que permita lo decía ahora el portavoz del Grupo Vasco dar a esa importantisima ley una exposición de motivos que con las prisas de un final de legislatura no se le pudo dar, retocar también algunos aspectos que entren en contradicción con la sentencia del Tribunal Constitucional, que es lo que deberemos analizar todos con el sosiego necesario, y buscar si algún aspecto de la nueva normativa puede ser mejorado. Sepa el director de la Agencia que tiene al Grupo Catalán (Convergéncia i Unió) plenamente dispuesto a encontrar, con el resto de grupos parlamentarios, una solución normativa para que sobre todo prime la seguridad, la garantía de los datos de carácter personal, así como buscar puntos adecuen a lo que es el tráfico de la Unión Europea sin crear mayores impedimentos en otros Estados, pero siendo pioneros en las garantías de protección.

La señora **PRESIDENTA:**

Por el Grupo Parlamentario Socialista tiene la palabra el señor López Garrido.

El señor **LÓPEZ GARRIDO:**

Solamente quiero hacer algunas observaciones a la intervención del director de la Agencia de Protección de Datos, que le agradecemos, y pedirle una mayor precisión en algunos de los temas que planteé que considero no suficientemente desarrollados en su intervención. En primer lugar, debemos congratularnos por la coincidencia que ha habido entre los grupos parlamentarios, al menos así lo han señalado explícitamente el Grupo Vasco y el Grupo de Convergéncia i Unió, sobre la trascendencia de esta sentencia del Tribunal Constitucional, su carácter expansivo y la conveniencia de modificar la Ley de protección de datos.

Es una conclusión que al menos nuestro grupo obtiene de la sesión de esta mañana.

Por las manifestaciones de diversos grupos parlamentarios, hasta el momento ninguno se ha opuesto a esa idea. Es sensato reflexionar sobre las importantes consecuencias que tiene esta sentencia del Tribunal Constitucional porque su doctrina va mucho más allá de los dos artículos que considera inconstitucionales para extenderse al conjunto de una norma.

La sentencia del Tribunal Constitucional sitúa la protección de los datos por encima de lo que la sitúa la Ley de protección de datos, y eso requiere una adecuación. Como arranque de esta última intervención por nuestra parte, disentimos cordialmente del director de la Agencia de Protección de Datos sobre la no retroactividad de la sentencia.

Es un tema importante que afectaría a la acción de la Agencia de Protección de Datos. Es una sentencia retroactiva, como todas las del Tribunal Constitucional que no dicen lo contrario.

¨En qué sentido? Cuando una ley se declara no sólo inconstitucional, sino nula, significa que tiene efectos desde entonces, **ex tun**c, no desde ahora, **ex nun**c. Por tanto, esa ley era nula, estaba dañaba en su interior desde que nació, en 1999, con la Ley de protección de datos y por tanto es claramente retroactiva. Cuando el Tribunal Constitucional ha querido que no lo sea lo ha dicho. Por ejemplo, en aquella famosa sentencia relativa a las consecuencias de un recurso de amparo que hizo modificar la Ley del impuesto sobre la renta para que no hubiera discriminaciones entre los que estaban casados y los no casados.

El Tribunal Constitucional dijo: que quede claro que es a partir de ahora, no hacia atrás. O en otras ocasiones (porque todos los tribunales lo han hecho así), cuando el Tribunal Europeo de Justicia, en la famosa sentencia del caso **Defrenne,** que igualó a hombres y mujeres en el salario a igualdad de trabajo como consecuencia del recurso que presentó una azafata de las líneas aéreas Sabena y dijo: A partir de ahora.

Porque ¨qué hubiera ocurrido si todas las empresas hubieran visto recursos de mujeres discriminadas en el salario años atrás? En este caso el Tribunal no ha dicho eso sino que es nula. Es cierto que las disposiciones sancionadoras no son retroactivas, pero la sentencia del Tribunal Constitucional no es una disposición sancionadora, es una sentencia y no sanciona a nadie, simplemente dice que esas normas son inconstitucionales. Por tanto es retroactiva.

La Agencia de Protección de Datos tendría que examinar qué es lo que ha pasado en este año de vigencia de la Ley de protección de datos con las administraciones públicas que han tenido, como ha dicho usted, un cheque en blanco.

Cuántas reclamaciones se han denegado este año, cuántas cesiones se han hecho sin haberse hecho.

Todo eso ¨qué efectos tiene? ¨No habría que comunicarse con los afectados durante este año para decirles que pueden hacer aquello que quisieron hacer y que no le dejaron erróneamente esta ley ha resultado ser inconstitucional? Esto tiene que afrontarlo la Agencia de Protección de Datos y nos gus taría saber qué va a hacer a este respecto, qué instrucciones va a dar a las administraciones públicas. Ha sido una auténtica revolución lo que ha producido esta sentencia del Tribunal Constitucional en prácticas de las administraciones públicas.

En cuanto a los temas que ha señalado, voy a destacar dos sobre los que quisiera una mayor precisión. No se ha referido a algo a lo que nosotros sí hemos hecho alusión: a esas cartas de las entidades financieras o compañías de telecomunicación diciendo: Si en 30 días no me contesta voy a manejar sus datos como quiera. ¨Qué pasa con eso? Después de la sentencia del Tribunal Constitucional eso es definitivamente imposible.

El Tribunal Constitucional dice que una persona tiene que saber en todo momento dónde están sus datos. En este sentido, hay artículos de la ley vigente que son imposibles de aceptar, como cuando se dice que en al cesión de datos sólo se comunicará la primera cesión. Y luego, ¨qué pasa? Una persona tiene que saber en todo momento dónde están sus datos y tiene que decir si le parece bien o no.

Por ejemplo, en cuanto al censo promocional, al que se ha referido el señor Jané, yo coincido con que una persona tiene que querer estar en ese censo promocional y no simplemente que se suponga que quiere estar sin que lo haya dicho y sin haberse asegurado de que ha recibido una carta a ese respecto. Lo mismo que pasa con las compañías de seguros, cuya regulación en la Ley de protección de datos, a nuestro juicio, es inconstitucional. No basta con que la ley lo diga. Una de las cosas que dice la sentencia del Tribunal Constitucional es que no basta con que la ley lo diga, sino que sea un cheque en blanco, porque entonces esa ley será inconstitucional, como dice claramente el Tribunal Constitucional en el fundamento jurídico 11. Dice: De ser ese el caso, la ley habrá vulnerado el derecho fundamental en cuestión; sería la ley la que vulneraría el derecho fundamental en cuestión.

No basta con que sea una ley la que lo permita; el contenido de la ley es lo que importa.

Por último, voy a referirme al tema de los centros de salud. Este es un asunto muy importante, no solamente por la sentencia del Tribunal Constitucional, también por disposiciones de enorme rango, por encima de la ley, como es el reciente convenio de Oviedo, ratificado por España el 4 de abril de 1997. Este convenio se refiere a la protección de los derechos humanos y de la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina. En el artículo 10 se dice que toda persona tiene derecho a que se respete su vida privada cuando se trate de informaciones relativas a su salud. En muchas instituciones sanitarias repito, yo diría que en casi todas, hay un riesgo enorme de conocimiento y de acceso a datos sobre la salud de las personas, y más que de la salud. Técnicamente es posible que alguien entre en el fichero de un hospital y que cambie la prescripción farmacéutica a un enfermo. Cabría hacerlo técnicamente, tal como está ahora mismo.

En los hospitales hay conexión a Internet sin medidas de seguridad. Nosotros tenemos dos ejemplos, por citarle algunos, de médicos que se han dirigido a nosotros. Un médico del centro de salud de Beraún, del País Vasco, dice claramente que cualquiera puede tener acceso a través de Internet a las historias clínicas de los ordenadores. Concretamente este médico dice: ¨Cómo se evita que se puedan introducir extraños? Y contesta: Así de claro. No se evita.

Hay un problema serio, que en muchas ocasiones afecta a médicos, que tampoco cumplen las condiciones mínimas de protección de datos. Cosas básicas como identificar al solicitante del dato, información consultada, nada de eso está regulado. Es un tema muy importante en el que quisiera que la Agencia de Protección de Datos hiciese hincapié, se ocupase de ely pudiese informarnos sobre cómo está esa situación, quizá no ahora, quizás en una próxima comparecencia, porque nos parece que es una situación de enorme riesgo para la protección de los datos de la salud. Otro médico del centro de salud de Albacete dice que ese centro lleva informatizado desde septiembre de 1999 y tiene acceso a Internet desde hace cuatro meses. No hay clave de acceso o, si la hay, no hay encriptación y, por tanto, existe riesgo de que se pueda acceder a Internet.

Por ejemplo, este médico decía que tenía acceso desde su consulta a Internet y a las historias clínicas, y como él otros. Este es un problema muy serio que tiene que ver con la forma de funcionamiento de las administraciones públicas. Sobre estos temas quisiera que hubiera una mayor precisión por parte del director de la Agencia de Protección de Datos.

La señora **PRESIDENTA:**

Por el Grupo Parlamentario Popular tiene la palabra el señor De Juan.

El señor **DE JUAN I CASADEVALL:**

En nombre del Grupo Popular, quiero dar la más cordial bienvenida al señor director de la Agencia de Protección de Datos. Después de su primera convocatoria durante esta legislatura ya viene con una cierta veteranía a esta Comisión. Mi grupo, muy sucintamente, señorías, quiere efectuar básicamente dos consideraciones. En primer lugar, participar de la preocupación que anima a otros intervinientes, a otros ponentes que me han precedido en el uso de la palabra y

singularmente al peticionario de esta comparecencia, por todo lo relativo a la tutela de este derecho de libertad informática, este derecho que tutela el artículo 18.4 de la Constitución y que en la actualidad, y después de la sentencia del Tribunal Constitucional, parece que se afirma cada vez con mayor grado de autonomía dentro de los derechos que protege el artículo 18 de la Constitución. Queremos dejar patente esta preocupación aquí, en la Comisión Constitucional, aprovechando la compare cencia del director de la Agencia de Protección de Datos y aprovechando que todavía está fresca la reciente sentencia del Tribunal Constitucional.

En ese sentido, mi grupo quiere expresar una vez más el acatamiento al pronunciamiento del Tribunal Constitucional, su más escrupuloso respeto a esa función depuradora del ordenamiento jurídico que le corresponde como supremo intérprete de la Constitución. Quisiera subrayar que, en cualquier caso, se trata de dos vicios de inconstitucionalidad muy concretos, muy puntuales, que probablemente estarían también, de haber mediado un fallo en ese sentido, en la Lortad del año 1992. En cualquier caso, frente a ese pronunciamiento del Tribunal Constitucional, insisto, mi grupo quiere expresar su más escrupuloso respeto y acatamiento. En segundo lugar, y muy sucintamente, en cuanto al de la convocatoria, nosotros estimamos razonablemente satisfactorias las explicaciones que ha vertido el señor compareciente en orden a los extremos que han sido sometidos a su consideración. En primer lugar, en cuanto a las entidades financieras, insisto, participamos de esa preocupación que se ha expresado por algunos ponentes que me han precedido en el uso de la palabra.

Entendemos que la Agencia de Protección de Datos está actuando con prontitud y con celo en la aplicación de sus competencias lo ha explicado el señor compareciente iniciando procedimientos de inspección y, en su caso, iniciando procedimientos sancionadores respecto a los cuales nos corresponde expresar ese respeto a un procedimiento administrativo abierto para determinar responsabilidades cuando concurran. Apreciamos especialmente la manifestación que ha efectuado sobre ciertos listados aparecidos en ocasiones en contenedores y la labor de investigación que está desarrollando en ese sentido la Agencia para determinar si se deben a una falta de aplicación de la ley o si obedecen a simples descuidos por parte de los interesados. Creemos, en cuanto a los listados de insolvencias, que es acertada la filosofía que preside esa instrucción que ha citado el señor compareciente, una instrucción del año 1995 sobre registros de insolvencia en lo relativo a la inclusión en los mismos. En definitiva, no es algo novedoso, pero es algo asumido por el derecho en cuanto al mismo concepto de insolvencia, el concepto de morosidad que tiene establecido nuestro Código Civil en sus artículos 1.100 y siguientes, si no recuerdo mal, de liquidez, de vencimiento y de requerimiento previo para que podamos hablar de moroso o podamos hablar de insolvente y, por tanto, nos parece sumamente acertado exigir por vía de instrucción el cumplimiento de esos requisitos para incluirse en esos registros. El compareciente ha efectuado una consideración no queremos entrar nosotros en el comentario de la sentencia del Constitucional, en relación con el registro central de entidades aseguradoras, que nosotros compartimos plenamente.

Estamos hablando de una disposición adicional que forma parte del cuerpo normativo de la Ley de protección de datos de 1999 y estamos hablando, por consiguiente, de un supuesto que disfruta de rango legal. Y de una lectura, no muy pormenorizada pero sí rápida, que he tenido ocasión de efectuar de esa sentencia del Constitucional se desprende que esa puntual y concreta declaración de inconstitucionalidad de un par de incisos normativos de los artículos 21 y 24 obedece básicamente a la falta de cobertura legal, a la existencia de un rango infralegal en el establecimiento de excepciones a esa cesión de datos. Es decir, que, básicamente, el vicio de inconstitucionalidad que declara el alto tribunal obedece al insuficiente rango en la determinación de esas excepciones en ambos preceptos legales. Por tanto, participamos plenamente de las consideraciones que ha efectuado al respecto el señor compareciente.

En cuanto a las administraciones públicas, quisiera destacar aquí que estamos analizando supuestos singulares y concretos, pero, en términos generales, la aplicación de la Ley de protección de datos ha avanzado positivamente en el radio de acción de las administraciones públicas, como tuvimos ocasión de comentar a raíz de su reciente comparecencia en esta Comisión Constitucional. Tengo que decir que apreciamos el que se hayan realizado gestiones informaba al respecto el señor compareciente a raíz de las recientes reestructuraciones ministeriales, actuaciones de carácter claramente preventivo, como ponerse en contacto con los subsecretarios, como jefes organizativos de los distintos ministeriales, recordándoles la aplicación de la ley y avanzando en ese proceso de sensibilización de la protección de ese derecho de autodeterminación informática o **habeas dat**a, que configura con autonomía la reciente sentencia del Tribunal Constitucional. Entendemos que, obviamente, deben ejercitarse las potestades sancionadoras, pero también debe incidirse en esa función preventiva en orden a la aplicación de la ley. Compartimos también con el señor compareciente algunas de las manifestaciones que ha efectuado en orden a la sentencia del Tribunal Constitucional. Ha citado la sentencia del alto tribunal de 20 de febrero de 1989, sentencia que, si no recuerdo mal, se refiere a la declaración de inconstitucionalidad de diversos preceptos de la Ley del IRPF, la Ley 44/1978 el señor López Garrido lo ha comentado también y yo reconozco su superior criterio en derecho constitucional, que es una ley que, efectivamente, obedecía a un recurso de amparo que se presentó por un sujeto particular y dio lugar a la sentencia de noviembre de 1988 en la que se autoplanteaba la propia cuestión de inconstitucionalidad de la sala al pleno del Tribunal Constitucional y que dio lugar a esta sentencia.

Esta sentencia motivó modificaciones de la Ley del IRPF, de 1989, que desembocaron en la Ley de 1991. No es ésta la situación que se produce en la actualidad a raíz de la sentencia del Constitucional, que es una sentencia que declara inconstitucionales, por insuficiente cobertura legal, determinados preceptos y que opera sobre esos dos supuestos explícitos y concretos. Es decir, aquí el Tribunal Constitucional ha actuado ejercitando esa función kelseniana de legislador negativo en esos dos puntos concretos. Con ello no quiero en modo alguno decir que mi grupo sea partidario o no de modificar la ley; sencillamente son que se hacen al hilo de una sentencia del Tribunal Constitucional y que exigirán en días sucesivos que mi grupo continúe reflexionando sobre dicho pronunciamiento. Por lo demás, ofrecemos al señor compareciente la predisposición, la colaboración del Grupo Popular y le rogamos encarecidamente que continúe con el mismo celo en la protección de este derecho fundamental que es el derecho a la autodeterminación informática o **habeas dat**a. Igualmente, quiero decirle que valoramos el que en la Administración exista un nivel razonable de cumpli-

miento de la ley y que no debemos dejarnos llevar en ningún caso por generalizaciones de supuestos concretos y determinados.

En cualquier caso, mostramos aquí una vez más nuestra confianza en que la Agencia de Protección de Datos ejercitará las facultades que le corresponden al respecto y le reiteramos la colaboración de nuestro grupo.

La señora **PRESIDENT**

A: Señor director de la Agencia de Protección de Datos.

El señor **DIRECTOR DE LA AGENCIA DE**

PROTECCIÓN DE DATOS

(Fernández López): Ante todo quiero agradecer a SS.SS. las palabras amables y de aliento que me han dirigido, y a continuación voy a tratar de contestar por orden las preguntas que me han hecho. Respondiendo al señor Mardones, cuando me he referido a que la sentencia va a condicionar mi actuación futura he querido decir, en definitiva, que de inmediato habrá que aplicar los preceptos en la forma en que el Tribunal Constitucional lo ha establecido; de inmediato, en el momento en que la ley aparezca en el Boletín Oficial del Estado. Por lo tanto, en mi opinión, como la desaparición consecuencia de nulidad de los incisos que el Tribunal Constitucional declara nulos de los artículos 21 y 24 posibilita la aplicación de la ley, haya reforma o no, mientras tanto en cualquier caso aplicaremos con el rigor que ello requiere lo establecido por el Tribunal Constitucional.

Por lo que respecta a los reglamentos de la Agencia, indudablemente hay que establecer un reglamento a la ley, eso sería lo conveniente. Tal vez hasta ahora, hasta que no se ha pronunciado el Tribunal Constitucional, las cosas no corrían prisa, y no corrían prisa porque estaba vigente, porque así lo dejó la ley, el anterior reglamento y podíamos bandearnos hasta ahora. Tampoco parecía conveniente que estando pendiente la declaración o no de la inconstitucionalidad se hiciera un nuevo reglamento, pero posiblemente ahora ha llegado el momento en que el nuevo reglamento pueda ver la luz. En cuanto al censo promocional, cuestión que S.S. también me ha planteado, debo decir que yo he sido y sigo siendo un defensor del censo promocional, y les cuento además por qué, pues yo sé que en algunos casos no se me interpreta bien. En la situación actual, la Ley General Electoral impedía que los datos del censo electoral pudieran utilizarse por las compañía de marketing y las de publicidad para una actuación que en la generalidad de los casos es lícita e incluso conveniente para los ciudadanos, porque no todos nuestros ciudadanos viven en grandes ciudades donde tienen grandes centros comerciales y ofertas importantes de productos.

A muchos ciudadanos las ofertas que les llegan a través de la publicidad y el marketing les son verdaderamente útiles.

Son en muchos casos ofertas culturales; fundamentalmente me estoy refiriendo a libros y discos, por lo que el ejercicio de una lícita profesión de comercio a mi modo de ver debe posibilitarse. Lo que ocurre es que esto no puede tener lugar con infracción de derechos fundamentales de los ciudadanos. La Ley de comercio minorista habilitaba, encontrándose así con la Ley General Electoral, para que pudieran tomarse del censo los nombres, apellidos y direcciones de los ciudadanos para esta materia. El problema de reserva de ley de la Ley General Electoral como ley orgánica imposibilitaba las previsiones contenidas en la Ley de comercio minorista, con lo cual estas empresas están en la actualidad en una situación de franca inferioridad respecto a sus competidores de la Unión Europea.

No olvidemos que hoy el territorio único hace que se reciban ofertas de otros países, por tanto, nuestras empresas son las que están en peor situación, algunas de ellas incluso amenazan con la posibilidad de trasladarse a estos países donde es mucho más fácil realizar esta actividad, con lo cual aquí perderíamos la empresa, los puestos de trabajo y en definitiva la riqueza que una empresa en principio incorpora a la economía nacional, lo que en ningún caso es algo a desear. De ahí que el desarrollo del censo promocional sea algo útil.

¨Cómo habría que desarrollar el censo promocional? Ahí está el quid de la cuestión a mi modo de ver, corresponde hacerlo a través del Instituto Nacional de Estadística porque es el que tiene el censo. Desde que se publicó la ley me puse al habla inmediatamente con la presidenta del INE para ofrecer la colaboración de la Agencia en todo lo que fuera necesario a fin de desarrollar esta cuestión. Por otro lado, al cambiar la presidencia ya he hecho llegar a la nueva presidenta mi disposición a la colaboración para este desarrollo, que por supuesto creo que es importante. También los grupos empresariales que habitualmente visitan la Agencia para interesarse por diversos temas como el del marketing directo nos han hecho llegar su preocupación porque esto se desarrolle. Yo personalmente estoy de acuerdo en que se desarrolle, pero posibilitando que el ciudadano que quiera estar en el censo lo esté y el que no quiera estar no lo esté, y que se establezca un sistema ágil para que, como dice la ley, uno se pueda dar de baja o entrar en el censo promocional del año siguiente (está previsto que tenga vigencia anual) y así los ciudadanos, según les vaya, podrán dejar de estar o introducirse en el censo. Indudablemente puede ser algo útil.

Además, no debemos olvidarnos de que, en el resto de países de la Unión Europea donde tienen también legislación de protección de datos, estas promociones comerciales están funcionando y posiblemente lo están haciendo con bastante mayor libertad de la deseada desde el punto de vista de la protección de la intimidad. Por supuesto que deseo que en nuestro país se establezca, pero dentro del marco normativo que permita la protección de la intimidad. Por lo que respecta a la protección penal, a la que usted también ha hecho referencia, yo no soy penalista pero indudablemente hay tipificados una serie de delitos de este tipo en el Código son suficiente eficacia. Tampoco soy capaz de decirle si merecerían algún tipo de reforma.

En cualquier caso, estas conductas sí están recogidas como tipos penales en el Código de 1995. Quisiera hacer una reflexión sobre la circulación de los datos, con lo que estamos siendo rigurosos. Les puedo decir que tenemos la legislación más rigurosa, más garantista de la Unión Europea. En estos momentos somos país de referencia para otros del Centro y Este de Europa que se van a incorporar a la Unión Europea.

Concretamente, la República Checa nos pidió que nos presentáramos a un concurso de la Comisión Europea para que fuéramos el país que les ayudara a llevar a cabo la reforma legislativa y la puesta en marcha de su autoridad de control en materia de protección de datos, ya se nos ha adjudicado el concurso. Es otra tarea más que no sé cómo vamos a poder llevar a cabo teniendo en cuenta las competencias cada vez mayores que tenemos, pero haremos el esfuerzo de la forma que corresponda. Del mismo modo Polonia también está interesada en nuestra legislación, y eso es porque es la más rigurosa y porque ven además que nosotros aplicamos la ley de forma contundente y clara, que no se trata de unos simples principios que hay en una ley estática sino que nuestra ley es dinámica y cuando se infringe se inspecciona y cuando se tiene conciencia de la infracción se sanciona, y eso desgraciadamente no ocurre en el resto de los países de la Unión Europea.

Actualmente, señorías, países de la importancia de Alemania y Francia no tienen traspuesta la directiva del año 1995 a su derecho interno, con lo cual fíjense la diferencia que existe. Y si en materia de telecomunicaciones hablamos de la directiva de 1997, los países que la han traspuesto españa, Portugal y Bélgica, y el resto no lo ha hecho.

Ya me referiré luego a ello cuando conteste al señor López Garrido en relación con los encartes que envían las compañías telefónicas, cómo están dentro de la ley y cómo están mandándolos de forma absolutamente ilegal. Con estoy doy por contestadas las preguntas del señor Mardones. En cualquier caso, posteriormente le podré aclarar cualquier cosa si quiere. El señor Erkoreka ha hablado de las medidas de seguridad y de la sensibilidad de los datos que éstas deben proteger. La realidad es que el reglamento de medidas de seguridad ha tenido un efecto muy positivo para la protección de datos en nuestro país, ya que a través del conocimiento del mismo muchos se han dado cuenta de la existencia de la ley.

¨Por qué? Porque el reglamento ha ido estableciendo unas fechas de cumplimiento escalonadas y cuando han ido a cumplirlo algunos se han dado cuenta de que la ley estaba por medio, no sabiendo ni que existía. De ahí que este año me estoy refiriendo al 2000 en relación con 1999, en que ya crecimos un 50 por ciento con respecto a 1998, estemos creciendo casi un 300 por ciento, lo cual les dará idea de la incidencia que este reglamento de medidas de seguridad ha tenido. Por supuesto, somos conscientes de que las entidades financieras lo deben vigilar. Por eso el legislador estableció que las medidas que deben cumplir estas entidades son de grado medio y desde el punto de vista técnico al menos son bastante fuertes.

Lo que siempre nos falla aquí es la cuestión organizativa. Muchas medidas son organizativas. Irnos a tomar un café y dejar conectado el ordenador o tirar los papeles a la basura y que no se destruyan son medidas organizativas a las que no se les da la debida importancia; sin embargo, a mi modo de ver éstas importantes para que este tipo de cosas no ocurran. Las entidades financieras, como he manifestado antes, tienen medidas de seguridad y yo creo que cumplen suficientemente. Por otro lado, como también he dicho, las conversaciones se han quedado en unas instrucciones que ha pasado la AEB a los bancos recordándoles la necesidad de cumplir con las medidas de seguridad, pero no sólo con la implantación de unas medidas técnicas sino cuidando de que los datos estén guardados y no salgan por ahí listados de ordenador, con las graves consecuencias que ello puede tener no sólo desde el punto de vista de la protección de datos. Además, como decía, he mantenido reuniones con miembros de la asociación, con su secretario general y con los asesores, para ver cómo se están cumpliendo todas estas cuestiones a las que me he referido, como los ficheros de morosos, y sobre todo que no se lleven a cabo estas prácticas del **scorin**g, del **data mailing** o del **data warehouse** sin el consentimiento expreso de los ciudadanos, ya que, repito una vez más, esto supone un paso más adelante al sacar perfiles en la intimidad de los ciudadanos. La sentencia del Tribunal Constitucional se refiere a transmisión de datos entre administraciones públicas. Podrá tener proyección toda la doctrina de la volumi nosa e importante sentencia del tribunal en el resto de la ley, pero la sentencia sólo incide directamente sobre la cesión de datos entre administraciones públicas, y como ya he dicho antes no es necesaria para aplicar la reforma de la ley. Si deciden SS.SS. reformar la ley y es para bien, bienvenida sea.

Me plantean que falta la exposición de motivos, también la echo yo en falta que tengo que aplicarla todos los días, pero la ley por los motivos que fueran no pudo tener exposición de motivos y la aplicación diaria de la misma nos ha dado cierta facilidad en su manejo a estas alturas.

Creo que ha quedado todo contestado y paso a responder al señor Jané. En cuanto a los riesgos de transferencias, les diré que, efectivamente, hay riesgos de transferencias. Fíjense si hay riesgos de transferencias de datos que se ha planteado en la Unión Europea una cuestión que yo he considerado de suma importancia y es la habilitación que se ha dado por la Comisión de las Comunidades a través de una decisión a los Estados Unidos de Norteamérica para considerarlo territorio equiparable al común de la Unión Europea y puedan circular libremente los datos, simplemente con que las empresas que lo deseen se adhieran a los llamados principios de puerto seguro. Son unos principios de buenas intenciones en donde se comprometen a preservar la intimidad, a no ceder los datos, a no utilizarlos para finalidades distintas, pero no hay autoridad alguna que controle esto, ni una legislación que verdaderamente obligue a su cumplimiento, sino que queda en unos buenos principios. Esto ha durado dos años y por supuesto las autoridades de control de datos de la Unión Europea, en donde por supuesto participa España, nos hemos opuesto desde el principio a que esto fuera así y eso que hay distintas tendencias siendo los grupos anglosajones más abiertos a la facilidad de transmisión de datos a los Estados Unidos.

El núcleo más duro lo formamos países latinos como Italia, Portugal, España y también Grecia. A pesar de que nuestro

último dictamen fue contrario a esta decisión de la comisión y a pesar de que el Parlamento Europeo intervino a instancia nuestra también dictaminó en contra, la realidad es que la Comisión Europea ha dictado una decisión que ya está publicada en el DOCE y que ya ha entrado en vigor la libre circulación de datos a Estados Unidos. Menos mal que hemos dejado muy claro que antes de salir los datos del territorio de alguno de los Estados miembros se aplicará la normativa interna, y de acuerdo con esa normativa interna, indudablemente las cosas no les van a resultar tan fáciles. A estos efectos la Agencia de Protección de Datos ha dictado una completa instrucción sobre transferencias internacionales que hace aproximadamente quince días se ha enviado al Boletín Oficial del Estado para su publicación y uno de estos días verá la luz.

Por supuesto que es importante el comercio electrónico al que se ha referido el señor Jané, y además tiene dos riesgos importantes: uno el material económico de que si facilito a través del comercio electrónico los datos de mi cuenta corriente o de mi tarjeta de crédito y los mismos no van cifrados, cualquiera en la red pueda obtenerlos, puede tener un problema económico; por supuesto también el problema de protección de la intimidad porque nuestros datos a través de varios medios podrán ser sustraídos por otro navegante en la red. De ahí que también en alguna otra ocasión me he referido a ello, la Agencia de Protección de Datos ya en el año 1997 publicó un documento con una serie de instrucciones para los navegantes de Internet y para la gente que a través de este medio quisiera llegar a transacciones comerciales, buscando la fórmula de hacerlo a través de un programa seguro y un navegador seguro y no de cualquier forma que pudiera ver su intimidad cogida por cualquiera. Ya me he referido al censo promocional y estoy absolutamente de acuerdo en su desarrollo. Por lo que respecta a la referencia que ha hecho el señor Jané en cuanto a la reforma de ley, como muy bien ha dicho corresponde a la Cámarrá ésta la que pueda decidir sobre ella.

Paso a contestar al señor López Garrido. También se ha referido a la posible modificación de la ley. En mi opinión sería posible que pudiera seguirse con el mismo texto, por supuesto suprimiendo aquellos preceptos declarados inscontitucionales por nuestro más alto tribunal, pero también se puede modificar y si se modifica para poder hacer alguna mejora será siempre bien acogida por la Agencia. Tengo que recordarle, y perdonen que insista, que tenemos una legislación muy rigurosa y que los demás europeos están por debajo. Con esto que digo no estoy invitando a renunciar a la protección que debemos a nuestros ciudadanos, sino a que no imposibilitemos tanto las cosas que favorezcamos las actuaciones desde otros países de la Unión Europea y que nuestras empresas se queden en situación de peor competencia con el resto. Usted opina que la ley es retroactiva.

Yo entiendo sinceramente que toda vez que va a suponer una irretroactividad **in peius,** en definitiva resultarían sancionables administraciones que estaban haciendo algo en base a una ley; y por aplicación del artículo 9.3 de la Constitución no cabe esta aplicación retroactiva de la ley. Por otro lado hemos de tener en cuenta la situación real. Hasta el momento no he tenido conocimiento de que se haya producido ninguna cesión de datos entre administraciones públicas por la norma de creación del fichero, con lo cual a lo mejor estamos hablando de algo que hasta ahora afortunadamente no se ha producido y por tanto no tenemos que hacer nada al respecto. Por otro lado sí le puedo decir respecto a los procedimientos tramitados que no se ha archivado ninguno por este motivo, con lo cual el problema a mi modo de ver en este caso no existe, al menos en la actualidad. Efectivamente como usted ha recordado, se contestar las famosas cartas o encartes de las compañías telefónicas que dirigían a los ciudadanos solicitando su consentimiento.

A este respecto tenemos que señalar lo siguiente. En un primer momento Telefónica dirigió unas cartas a sus abonados pidiéndoles consentimiento para la cesión de datos de forma indefinida. Además, empezaron a tratar estos datos, tanto de los que habían dicho que sí, como de los que habían dicho que no, o de los que no habían contestado. Esto supuso una actuación contundente de la Agencia, que llegó a la paralización del fichero y estamos hablando de un fichero donde se están tratado 17 millones de datos, pero inmediatamente Telefónica rectificó su actitud y mandó un nuevo encarte en el que solicitaba el consentimiento tácito.

Pero el consentimiento tácito ¨para qué? No para ceder los datos a otras empresas sino para tratar ella misma los datos que tenía de facturación de los ciudadanos para ofrecer nuevos productos, pero nuevos productos comercializados por ella misma. Efectivamente, el consentimiento era tácito, pero lo era porque así lo permite el artículo 65 del Real decreto que desarrolla la Ley de Telecomunicaciones, por el que se traspone la Directiva del año 1997 en materia de telecomunicaciones. Recuerdo otra vez a SS.SS. que somos uno de los tres únicos países que han traspuesto esta directiva, lo cual supone que en los demás cada compañía estará haciendo lo que le apetezca, porque no tienen ninguna traba legal para ello. Lo que han podido hacer las compañías, no sólo Telefónica sino también las otras que están en el mercado, es una comunicación a los ciudadanos en la que les señalan que van a tratar sus datos de facturación para promover nuevos productos vuelvo a repetir por la propia compañía y no por otras del grupo ni nada semejante, solicitando su consentimiento tácito en un plazo determinado. A este respecto, debo decir varias cosas. En primer lugar, que el artículo 65 del reglamento lo permite expresamente, pero es que además nuestra Ley de protección de datos también habilita el consentimiento tácito. Prueba de ello es que en el artículo 7.

§, donde se regulan los datos especialmente protegidos o datos sensibles en la terminología comunitaria, se hace referencia a que cuando sean los de ideología, religión o creencias, aparte de informar de la no obligación de declarar sobre los mismos, cuando se dé el consentimiento éste tiene que ser expreso y escrito. Sin embargo, cuando se refiere a los datos de salud, origen racial y vida sexual exige el consentimiento expreso, pero no escrito, lo cual quiere decir que hay otro tipo de consentimiento; además en nuestro Tribunal Supremo hay multitud de sentencias donde se admite el consentimiento tácito. Lo que ocurre es que esto afectará a la forma de consentir pero no al fondo, y el problema que tendrán estas empresas será probar que han obtenido el consentimiento, porque la carga de la prueba recaerá sobre ellas. Y si no prueban que tienen el consentimiento del ciudadano escrito, tácito, como quieran indudablemente serán sancionadas. Esto es así de claro, a mi modo de ver, en el contexto de la ley, por lo cual estas cartas posteriores sí cumplían con la normativa.

El problema se presentará cuando haya una denuncia, si no son capaces de probar que tienen el consentimiento. Por supuesto, en ninguno de estos casos se posibilita cesión alguna de datos, a empresas del grupo, a empresas participadas, ni a otras empresas que se dediquen a actividades colaterales o complementarias, solo pueden utilizar para promocionar ellas sus propios productos. Finalmente, pasando a contestar al señor De Juan, estoy absolutamente de acuerdo con la importancia y la trascendencia que tiene la sentencia del Tribunal Constitucional que viene a declarar los mismos defectos que tenía la Lortad, porque los artículo 21 y 24 no son más que la traslación de los artículo 19 y 22 de la Lortad, a los que también había tachado de inconstitucionalidad el Defensor del Pueblo; lo que ocurre es que la otra sentencia que dicta el Tribunal Constitucional deja a este recurso sin objeto. También comparto su opinión en cuanto a la legislación de seguros.

No sólo hay norma de rango legal, es que la norma de rango legal habilita para cosas determinadas, no es una norma en blanco aunque tenga rango de ley, es una norma que habilita para cuestiones concretas. Personalmente, no me gustó que se introdujera esta reforma de la Ley de seguros en la Ley de protección de datos, creo que debió llevarse la reforma donde correspondía, pero la habilitación que se da a las compañías para crear ficheros comunes es limitada y, por otro lado, también tiene un importante control. Según he llegado a conocer, hay un importante número de ciudadanos que circulan sin seguro obligatorio. Esto lleva, por un lado, a riesgos para la circulación y, por otro, a un costo que los demás ciudadanos debemos soportar a través del consorcio de compensación de seguros, que es el que ha de indemnizar estos siniestros en el caso de que se produzcan. Si estas cesiones se hacen para los casos concretos que habilita la Ley de seguros, estará bien. En todo este contexto, hablábamos de si hay que reformar o no la ley.

Creo que, con la actual Ley de protección de datos, se ha avanzado en una cosa muy importante respecto de la Lortad. Fíjense que principios de información, finalidad y cesión, lo que yo llamo siempre la columna vertebral de la protección de datos, están reforzados en la Ley de protección de datos de una forma muy cualificada con respecto a la anterior ley. Si esto lo trasladamos ahora, por ejemplo, al supuesto de las administraciones públicas, que no tienen ya ese cheque en blanco para transmitir los datos cumpliendo con estos principios, creo que los derechos de los ciudadanos estarán suficientemente protegidos y no se precisará de mayor reforma legislativa. Por mi parte, no creo que haya quedado ninguna cosa que contestar, señor de Juan. Si así fuera, con mucho gusto volvería a intervenir.

La señora **PRESIDENT**

A: ¨Algún grupo desea intervenir?

(Pausa.)

Agradeciendo la presencia y la exhaustividad de las explicaciones ofrecidas por el director de la Agencia de Protección de Datos, antes de levantar la sesión, por indicación y acuerdo de los miembros de la Mesa, desearía expresar, en nombre de la Mesa de la Comisión Constitucional, nuestro más rotundo rechazo al atentado terrorista ocurrido esta mañana en Terrassa, que ha causado gravísimas heridas al concejal del Partido Popular en el Ayuntamiento de Vila-decavalls Francisco Cano i Consuegra. ¨Sus señorías acuerdan unirse a este rechazo y a la solidaridad con esta víctima, afortunadamente creemos que no mortal, de un nuevo atentado terrorista?

(Asentimiento.) El compareciente me comunica que también se une a este rechazo. Muchas gracias, señorías, señor director de la Agencia de Protección de Datos. Se levanta la sesión.

Era la una y treinta y cinco minutos de la tarde.

MEMORIA DE 2000 - ANEXO V - SESIÓN NÚM. 4 CELEBRADA EL MIÉRCOLES, 20 DE SEPTIEMBRE DE 2000

COMISIONES

Año 2000 VII Legislatura Núm. 53

CONSTITUCIONAL PRESIDENCIA DE LA EXCMA. SRA. D.a MARGARITAMARISCALDE GANTE MIRÓN

Sesión núm. 4 celebrada el miércoles, 20 de septiembre de 2000

ORDEN DEL DÍA:

Comparecencia del señor director de la Agencia de Protección de Datos (Fernández López) para informar sobre:

La memoria de la Agencia de Protección de Datos correspondiente al año 1999. A petición propia.

(Número de expediente 212/000069.) . 1134

Contenido de la memoria correspondiente al año 1999. A solicitud del Grupo Parlamentario Socialista. (Número de expediente 212/000046.) .. 1134

Protección de la intimidad personal y familiar en relación con Internet. A solicitud del Grupo Parlamentario Socia - lista. (Número de expediente 212/000080.) . 1155

Se abre la sesión a las diez y cinco minutos de la

mañana.

COMPARECENCIA DEL SEÑOR DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

(FERNÁNDEZ LÓPEZ) PARA INFORMAR SOBRE:

LA MEMORIA DE LA AGENCIA DE PROTECCIÓN DE DATOS CORRESPONDIENTE AL AÑO 1999. A PETICIÓN PROPIA. (Número de expediente 212/000069)

CONTENIDO DE LA MEMORIA CORRESPONDIENTE

AL AÑO 1999. A SOLICITUD DEL GRUPO PARLAMENTARIO SOCIALISTA.

(Número de expediente 212/000046)

La señora **PRESIDENT**

A: Buenos días.

Como SS.SS. conocen, el orden del día está conformado por las tres comparecencias del director de la Agencia de Protección de Datos, dos de ellas, una a petición propia y otra del Grupo Socialista, tienen el mismo contenido, que es el informe sobre la memoria de la Agencia. El desarrollo de la comparecencia en el día de hoy será, en primer lugar, y para que exponga el resumen de la memoria, la exposición del director de la Agencia de Protección de Datos, don Juan Manuel Fernández López, a quien saludamos y agradecemos su presencia ante esta Comisión. Ysin más, y si SS.SS. no tienen nada que objetar, tiene la palabra el señor compareciente.

El señor **DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS**

(Fernández López): Muchas gracias, señora presidenta. Como es habitual, el director de la Agencia de Protección de Datos comparece ante esta Comisión del Congreso de los Diputados para informar de la memoria que preceptivamente tiene que redactar anualmente la Agencia dando cuenta de la labor desarrollada en el año anterior, en este caso la correspondiente a 1999. La comparecencia se realiza a petición propia y de uno de los grupos parlamentarios. Quiero agradecer a la Mesa de la Comisión la celeridad con la que se ha producido mi convocatoria, prácticamente al principio de la legislatura, y aprovechar este momento para saludar a SS.SS. como miembros de esta Comisión.

Espero continuar con SS.SS. la misma fluidez y cordialidad en la relación que tuve con los anteriores miembros de la Comisión. Como ya destaqué en anteriores comparecencias, el control parlamentario es una importante garantía de la independencia y sometimiento a la legalidad que ha de guiar todas las actuaciones de la Agencia de Protección de Datos, sirviendo además para que el director de la misma reciba de SS.SS. las sugerencias que, como representantes de los ciudadanos, contribuirán, sin duda, a fortalecer la garantía y protección en lo que concierne al tratamiento de datos personales y las libertades públicas y derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar, empleando la terminología del artículo 1 de la vigente Ley orgánica de protección

de datos. La memoria les fue remitida el pasado mes de junio, dando cumplimiento a la exigencia que establece el Estatuto de la Agencia. Siguiendo su estructura, que viene condicionada por aquel estatuto, comentaré los puntos más relevantes, quedando a disposición de SS.SS. para las precisiones o aclaraciones que estimen pertinentes lugar, he de referirme al Registro General de Protección de Datos. Ante el mismo, por imperativo legal, se han de declarar todos los ficheros informatizados de los que sean titulares tanto las administraciones públicas como las entidades privadas.

Su principal finalidad es posibilitar a los ciudadanos el conocer al titular del fichero y su domicilio a efectos de ejercitar sus derechos de acceso, rectificación o cancelación. Como saben SS.SS., a partir del año 2007 también estarán bajo la competencia de la Agencia aquellos ficheros que no se traten informatizadamente, toda vez que el legislador español ha hecho uso de la prerrogativa que en este aspecto otorga la directiva y ha diferido a tal fecha el establecer competencias de la Agencia sobre este tipo de ficheros. A lo largo de 1999, las solicitudes recibidas en el registro general se han visto incrementadas en más del 50 por 100 respecto de las del año anterior.

No obstante, la gestión de todo tipo de movimientos referentes a la inscripción de ficheros ha seguido siendo significativamente fluida, ya que el tiempo medio de respuesta desde que la notificación tiene entrada hasta que se emite la correspondiente resolución de inscripción no ha superado los siete días. Sin embargo, la evolución de solicitudes de inscripción lleva una tendencia fuertemente creciente durante el presente año, ya que en los siete primeros meses del año 2000 se han recibido más del cuádruple de solicitudes que en el mismo período del año anterior. Dentro de las actividades propias del registro, durante el año 1999 se ha tramitado, a instancias de los responsables de ficheros, la inscripción de 5.201 nuevos ficheros, se han modificado 2.753 inscripciones y se han suprimido 1.479, lo que supone un total de 9.433 operaciones.

Una de las causas a las que puede imputarse el crecimiento de inscripción ha sido la aprobación por el Real Decreto 994/1999, de 14 de junio, del reglamento de medidas de seguridad. Somos, señorías, el primer país de la Unión Europea que ha dictado un reglamento de medidas de seguridad en materia de protección de datos. Este reglamento prevé una exigencia escalonada de los tres niveles de medidas de seguridad que el mismo establece, dispo niendo que las medidas de nivel básico, es decir, aquellas exigibles a todo fichero que contiene datos, entraran en exigencia el 26 de diciembre de 1999, luego prorrogada al 26 de marzo de 2000. Ello ha supuesto un auténtico colapso en la Agencia de Protección de Datos en el último mes del año, debiendo recurrir a medidas extraordinarias y contratando por ello servicios externos, aunque prestados en la propia sede de la Agencia, para dar respuesta al imprevisible aumento de la declaración de ficheros. A pesar de que el reglamento de medidas de seguridad no exige ninguna declaración inmediata complementaria de la que ya se hubiese realizado, de lo que informó la Agencia entre otros medios a través de su página web en Internet, la exigencia de implantación de medidas de seguridad ha tenido el efecto beneficioso de que se conociera la obligación derivada de la ley de declaración de los ficheros ante la Agencia, con el efecto inducido de acumulación de solicitudes que antes mencioné. Por otra parte, la entrada en vigor de la Ley Orgánica 15/1999, de protección de datos de carácter personal, ha exigido la adecuación del registro a las nuevas previsiones legales.

A lo largo de este año 1999, se ha realizado el estudio y desarrollo de los sistemas de información necesarios para implantar aquéllas. Esta situación ha dado lugar a la aprobación de la resolución de la Agencia de Protecció Datos, de 30 de mayo de 2000, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos. Asimismo, se ha desarrollado el proyecto que está permitiendo en la actualidad instrumentalizar la notificación de ficheros para su inscripción en el registro a través de Internet.

Otro aspecto importante que afecta al registro es la publicación del catálogo de ficheros. La Ley 15/1999 dispone en su artículo 14, como ya lo hiciera la vieja Lortad, el derecho de consulta al Registro General de Protección de Datos. Entre las funciones de la Agencia se encuentra la de velar por la publicidad de la existencia de los ficheros automatizados, a cuyo efecto se publica periódicamente una relación de dichos ficheros. El objetivo de este catálogo es dar publicidad a la existencia de los ficheros, siendo fundamental conocer la dirección ante la que el ciudadano pueda ejercitar los derechos de acceso, rectificación y cancelación de sus datos personales que la ley le reconoce. Para cumplir el precepto de dar publicidad a la existencia de ficheros se ha mantenido con una actualización mensual el catálogo de ficheros en la web de la Agencia, lo que permite completar las publicaciones que se vienen realizando, tanto en formato papel como en CDROM, de forma que los ciudadanos puedan, por este medio, conocer la situación de los ficheros con una actualización mensual. La publicación en Internet se incluye como una opción más dentro de la web institucional de la Agencia, donde se puede encontrar, en primer lugar, información de carácter general. También se facilitan las instrucciones necesarias para inscribir nuevos ficheros en el registro, pudiendo obtenerse el modelo normal de inscripción, tanto de ficheros de titularidad pública como de titularidad privada, y el catálogo de ficheros propiamente dicho. Descargando los formularios o un programa de la página web de la Agencia de Protección de Datos, se facilita el cumplimiento de estas notificaciones por un medio rápido y eficaz.

También debo hacer mención a los ficheros con transferencias internacionales. Salvo los países que proporcionan un nivel de protección equiparable al que presta la ley española para transferir datos a terceros países es necesario solicitar la preceptiva autorización de transferencia internacional al director de la Agencia de Protección de Datos, según detallaré posteriormente. Dada la relevancia que han adquirido los movimientos internacionales de datos por diversos motivos, como puede ser la centralización de recursos de las empresas para su tratamiento de forma globalizada, los nuevos sistemas de información de la comunicación, las nuevas formas de mercado, los nuevos sistemas de gestión integrada de las compañías y otros factores similares, se ha producido un aumento de los ficheros privados que declaran transferencias internacionales de datos. El total de ficheros inscritos en el registro a fecha 31 de diciembre de 1999 que contienen en su declaración transferencias internacionales es de 1.081, de los cuales 53 corresponden a inscripciones de titularidad pública y 1.028 a titularidad privada. Entre los supuestos legales en los que se amparan las

declaraciones de los ficheros inscritos con transferencias internacionales de datos destacan las transferencias amparadas en la norma general del movimiento internacional de datos cuando se efectúan con destino a países con nivel de protección equiparable al español. El número de ficheros privados declarados en el registro amparados en este o legal es de 923. A continuación, con 53 inscripciones, se encuentran los ficheros que declaran transferencias dinerarias conforme a la legislación específica, casi todos ellos pertenecientes a entidades financieras que realizan transferencias amparadas en la legislación en materia dineraria, normalmente adheridos al sistema internacional de intercambio de datos bancarios.
Los ficheros que realizan la transferencia de datos a otros países, con objeto de intercambiar datos de carácter médico, cuando así lo exija el tratamiento del afectado o una investigación epidemiológica, ascienden a 24. En cuanto a los ficheros de titularidad pública, en la mayoría de los casos se trata de transferencias internacionales con destino a países de igual nivel de protección. Los amparados en tratados o convenios se declaran en los ficheros de las administraciones tributarias y Seguridad Social, en vir tud de lo dispuesto en los convenios internacionales de asistencia mutua en estas materias y en ficheros de los Cuerpos y Fuerzas de Seguridad con fines de investigación concreta, amparado en convenios internacionales como los de Interpol, Schengen o Europol. Conforme a la ley española, a la hora de efectuar una transferencia internacional de datos, hay que solicitar autorización del director de la Agencia de Protección de Datos. Durante el año 1999 se ha producido un aumento en el número de solicitudes de autorización de transferencias internacionales, lo que ha supuesto un incremento del 25,8 por 100 respecto del año anterior. Así, en 1999 se han tramitado 39 expedientes, encontrándose resueltos todos, autorizándose de ellos 37 y archivándose dos por desistimiento. Todas las autorizaciones tienen como destino Estados Unidos de Norteamérica, excepto dos, cuyo destino ha sido Filipinas y Marruecos. Las autorizaciones internacionales están amparadas en el consentimiento informado de los afectados, a excepción de cuatro expedientes que están amparados en una solución contractual y a los que se exigen determinadas garantías.

Otra función importante de la Agencia de Protección de Datos es la inscripción de códigos tipo o deontológicos. El artículo 32 de la Ley Orgánica 15/1999, de protección de datos de carácter personal, prevé, como ya lo hacía la Lortad, la posibilidad de formar códigos tipo a los responsables de los ficheros, a través de acuerdos sectoriales o mediante decisiones de empresas o convenios administrativos. Estos códigos tienen el carácter de códigos deontológicos o de buena práctica profesional y deben ser depositados en el registro general de protección de datos, donde se procederá a su inscripción, siempre que se ajusten a las disposiciones legales y reglamentarias sobre la materia o se denegará en caso contrario. En este último supuesto, previamente, los solicitantes son requeridos para que efectúen las correcciones necesarias. Durante el año 1999 se ha inscrito el código ético de publicidad en Internet por la asociación de autocontrol de la publicidad.

Este código tiene por objeto cubrir el vacío que sobre conductas publicitarias en general existe en el entorno de Internet, estableciendo unas normas mínimas sobre la publicidad en Internet, partiendo del principio de control en origen, que son adoptadas de forma voluntaria por los sectores integrados en la asociación de autocontrol de la publicidad. Al establecer el principio de control en origen se siguen las recomendaciones que las instituciones comunitarias europeas propugnan en el libro verde sobre la comunicación comercial y se asegura la efectividad a la hora de establecer mecanismos que aseguren el cumplimiento del código. En el ámbito deontológico, este código tiene vocación de complementariedad con el establecido por la Federación española de comercio electrónico y marketing directo, del que trataré posteriormente. Otro módulo de la Agencia de Protección de Datos lo constituye la Secretaría General. Las principales actividades realizadas por la misma durante 1999 han ido dirigidas a posibilitar el funcionamiento de la Agencia en sus aspectos materiales, técnicos y de recursos humanos, así como el área de atención al ciudadano. El incremento de actividades de la Agencia exige un aumento continuado de recursos humanos y en el año 1999 se ha concretado, al finalizar el mismo, con una plantilla total de 62 funcionarios. El mismo problema se plantea respecto a la sede de la Agencia, a la que se ha tratado de dar una solución mediante la firma de un contrato de arrendamiento con opción de compra de un edificio de casi 3.000 metros cuadrados en la calle de Sagasta, toda vez que en diciembre de este año nos vence el contrato de arrendamiento de las plantas que tenemos alquiladas en Castellana 41, los costes del arrendamiento son muy altos y, además, tampoco nos posibilitaban el volumen de metros de crecimiento que nos eran necesarios.

En el ejercicio de sus competencias, con el fin de lograr un mejor conocimiento de la ley y para tratar en profundidad temas de la mayor actualidad e interés, la Agencia de Protección de Datos ha organizado unas jornadas sobre privacidad, contratación electrónica e Internet, en colaboración con el centro regional de Extremadura de la Universidad Nacional de Educación a Distancia, que tuvieron lugar en Mérida los días 1 y 2 de julio de 1999.

En el año 2000 se han celebrado, en colaboración con la universidad pública de Navarra, otras jornadas sobre protección de la privacidad, en este caso en el aspecto de las telecomunicaciones y también de Internet. De igual forma, con la finalidad de extender el conocimiento de la Ley de protección de datos y las funciones de la Agencia, se han multiplicado los foros en los que la Agencia de Protección de Datos ha participado, y estos han sido en multitud de cursos y seminarios, tanto sobre aspectos generales como específicos y novedosos, tales como los relativos a Internet, firma electrónica, comercio electrónico. Personalmente he intervenido en el pasado año en más de 30 jornadas, cursos y seminarios sobre estas materias. Se ha convocado, en 1999, la tercera edición del premio protección de datos personales, con una dotación de un millón de pesetas y un accésit dotado con 250.000 pesetas, con la finalidad de profundizar en el estudio del desarrollo del artículo 18.4 de nuestra Constitución. El jurado establecido en las bases de la convocatoria otorgó el premio a la obra **Protección de los datos de carácter personal relativos a la salu**d, presentada por la doctora en medicina doña Carmen Sánchez Carazo y el licenciado en derecho don Juan María Sánchez Carazo. De la referida obra, la Agencia ha realizado una edición de 1.000 ejemplares para su entrega y difusión institucional. Se concedió el accésit a la obra titulada **El derecho a la autodeterminación informativa, marco constitucional y europeo,** de la que es autora doña Juana Marí Cardona, profesora de la universidad de Barcelona.

En el año 2000 se ha convocado la cuarta edición de este premio y, además, un premio de periodismo en materia de protección de datos. El área de atención del ciudadano desarrolla, dentro de la Agencia, la función personalizada a todos aquellos ciudadanos que, o bien acudiendo directamente a las dependencias de la Agencia o a través de teléfono o de correo ordinario o electrónico, solicitan información sobre la protección de sus datos personales. A lo largo de 1999 se han contestado alrededor de 15.000 consultas. De ellas, 11.500 han sido telefónicas, 1.150 presenciales y 1.739 por escrito. Con respecto a 1998, se observa que se han incrementado en un 20 por 100 las consultas escritas. Por lo que se refiere al año 2000, se constata un creciente aumento de las consultas, tanto las efectuadas por escrito como presenciales o telefónicas, que pueden suponer a final del año un incremento aproximado del 54 por 100.

Con el fin de lograr una mayor difusión de la existencia y funciones de la Agencia, así como de la legislación en materia de protección de datos, en general, y de los derechos de los ciudadanos, en particular, se ha editado una página web de la Agencia de Protección de Datos. El número de ciudadanos que han accedido a dicha página durante 1999, en cómputo global, fue el de un total de 506.362 accesos, lo que supone un incremento del 43 por 100 respecto al número de accesos del año anterior. De conformidad con lo establecido en el artículo 36, h), de la Lortad y en el artículo 5 del Estatuto, corresponde a la Agencia informar con carácter preceptivo los proyectos de disposiciones generales que desarrollen la ley orgánica. A lo largo de 1999, se ha sometido al parecer de la Agencia de Protección de Datos un total de 35 disposiciones, lo que supone un incremento del 59 por 100 respecto a 1998. Entre las disposiciones informadas por la Agencia, deben destacarse las siguientes: la propuesta de reforma con rango de ley para la actualización de la regulación de la Central de Información de Riesgo del banco de España Cirbe, el anteproyecto de la ley de creación de la Agencia Catalana de Protección de Datos y el anteproyecto de ley sobre firma electrónica, aprobado posteriormente por el Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

Trataré a continuación los problemas planteados con las consultas efectuadas por los responsables de ficheros. La Agencia ha venido resolviendo desde su creación un importante número de cuestiones de mayor complejidad jurídica planteadas por las personas o entidades públicas o privadas que ostentan la condición de responsables de ficheros o por sus representantes legales o empresas que prestan a aquéllas asesoramiento en materias relacionadas con la informática y el derecho. Esta actividad ha experimentado un incremento a lo largo de 1999, año en el que se ha pasado de la elaboración de 221 informes a 370, con un aumento de casi el 68 por 100. El volumen de consultas provenientes de los sectores públicos y privados es sustancialmente similar 55 por 100 de privados, frente al 45 por 100 de públicos, siendo destacables por su importancia numérica las planteadas por los ayuntamientos 27 por 100, dentro del sector público, y por los empresarios mercantiles 39 por 100, dentro del sector privado. Es de reseñar el volumen de cuestiones planteadas por el sector financiero, aparte de las relacionadas con servicios de solvencia patrimonial y crédito, y el incremento de las cuestiones planteadas por las empresas del sector de las telecomunicaciones, respecto de las cuales se ha acentuado la actividad de la Agencia de Protección de Datos durante 1999, tal y como se expone en la memoria. Atendiendo, por otra parte, al origen geográfico de las consultas planteadas, debe indicarse que la práctica totalidad de las mismas 363 fueron planteadas por entidades u organismos nacionales o en territorio nacional, mientras que sólo siete de ellas lo fueron por no residentes en España o extranjeras.

En cuanto a las materias objeto de consulta, debe destacarse la cesión de datos de carácter personal en especial, los relacionados con la cesión de datos del Padrón Municipal y cesión de datos sensibles o especialmente protegidos, en terminología de la Lortad y las consultas planteadas como consecuencia de la entrada en vigor del Reglamento de medidas de seguridad: las relacionadas con los ficheros de la Hacienda pública y el tratamiento de datos por cuenta de terceros con la aparición cada día más habitual de la figura del encargado del tratamiento. Me corresponde también exponer a continuación, señorías, las actividades realizadas en el año 1999 en el ámbito de la inspección de datos. A estas alturas de mi exposición, y con el fin de no cansarles excesivamente, trataré de sintetizar las tareas realizadas por la Agencia en dos de sus más importantes funciones para el efectivo cumplimiento de la ley: la función inspectora o investigadora y la función instructora de los expedientes sancionadores y procedimientos de tutela de derechos. En el ámbito de la función inspectora, se iniciaron 292 inspecciones durante 1999, a las que hay que añadir 23 actuaciones de información previa con el fin de determinar con carácter preliminar si concurrían circunstancias que justificaran la iniciación de procedimientos y actuaciones inspectoras. Además, se han realizado diversos planes sectoriales de inspección, a los que luego me referiré más concretamente, a fin de comprobar el grado de adecuación de los ficheros de administraciones públicas y de titularidad privada a las prescripciones de la legalidad sobre protección de datos de caracter personal. Con este objeto se han iniciado y terminado durante 1999 las inspecciones de oficio realizadas a la Agencia Estatal de Administración Tributaria, a la Dirección General de Tráfico, al sector de Atención Primaria, al Hospital Psiquiátrico de Fonca lent, al Hospital Militar Central Gómez Ulla y al Centro Nacional de Epidemiología, ésta última iniciada en 1998.

El director de la Agencia ha dictado las correspondiente recomendaciones dirigidas al sector de prestación de servicios de información, sobre solvencia patrimonial y crédito, y al sector de las compañías aseguradoras, cuyas inspecciones de oficio tuvieron lugar a lo largo de los ejercicios de 1998 y 1999 y de las que informé en mi anterior comparecencia. Uno de los últimos planes sectoriales ha sido el relativo al campo de las telecomunicaciones. Durante el pasado ejercicio se ha inspeccionado a los principales operadores de telefonía fija Telefónica de España, Retevisión, Lince Telecomunicaciones Uni2 y Euskaltel de cara a conocer no sólo el grado de adecuación a la Ley orgánica de protección de datos, sino también al Real Decreto 1736/1998, que desarrolla la Ley general de telecomunicaciones y que ha traspuesto a nuestro derecho interno la Directiva 97/66 CE. En cuanto a la función instructora, voy a resaltar que, de las tres clases de procedimiento que incoa la Agencia, 131 corresponden a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad privada, 24 a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad pública, y 167 a procedimientos iniciados por tutela de derechos.

La novedad introducida por la Ley 4/1999, de 13 de enero, del restablecimiento del recurso de reposición ha supuesto que durante el año 1999 se hayan presentado y resuelto por primera vez 65 recursos de esta clase, de los que 61 han

sido desestimado y cuatro estimados. Como consecuencia de los expedientes sancionadores incoados frente a los responsables de ficheros de titularidad privada se han impuesto sanciones por importe de 1.571 millones de pesetas. Lo digo sólo a efectos informativos y estadísticos, dado que no es un dato del que me sienta especialmente orgulloso; como he repetido en diversos foros, el funcionamiento de la Agencia de Protección de Datos habrá alcanzado su cenit precisamente el día en que la cuantía de las sanciones sea insignificante, ya que ello supondrá no sólo que la Agencia ha cumplido con la función encomendada por la ley velar por su cumplimiento sino también que los ciudadanos, empresas y entidades de derecho público han tomado conciencia de la importancia de respetar el derecho a la intimidad de las personas físicas consagrado como derecho fundamental por nuestra Ley de leyes. Entrando más pormenorizadamente en el análisis de la actividad de la Agencia por sectores, paso a detallar los aspectos más relevantes que se han puesto de manifiesto en el curso de las inspecciones realizadas en los distintos sectores de actividad pública y privada. En el campo de los ficheros de titularidad pública cabe destacar la inspección de oficio realizada a la Agencia Estatal de Administración Tributaria, a la que ya se había inspeccionado en otras ocasiones como consecuencia de denuncias planteadas por los ciudadanos, y a la Dirección General de Tráfico, administraciones ambas que disponen de ficheros automatizados de tal volumen y riqueza de contenido que incluyen datos de carácter personal, de ámbito nacional, con información concerniente a millones de españoles.

No obstante, teniendo en cuenta que las actuaciones inspectoras a los citados organismos finalizaron en diciembre de 1999 la nueva Ley Orgánica 15/1999, de protección de datos, ya había sido publicada y prevista su entrada en vigor para el 14 de enero de 2000, como director de la Agencia decidí aplazar el dictado de las recomendaciones a fin de que las mismas fueran acordes con la nueva ley, permitiendo así a dichos organismos una mejor adecuación de los tratamientos automatizados que realizan a los nuevos principios establecidos por la normativa vigente en materia de protección de datos.

Por otra parte, entre las resoluciones dictadas, como director de la Agencia, en virtud de denuncias de los ciudadanos referentes a ficheros de titularidad pública, merecen especial mención las siguientes: la relativa a una cesión de datos realizada, vía fax, por la Dirección General de Instituciones Penitenciarias a una entidad privada dedicada a la creación de ficheros de altos cargos, resultando sancionado el organismo público por infracción del artículo 11 de la Lortad, por cesión de datos; la que efectuó la Agencia Estatal de Administración Tributaria por haber facilitado a terceras personas un certificado sobre la declaración del IRPF de un contribuyente sin el consentimiento del afectado y sin la acreditación de su personalidad ante el responsable del fichero, lo que supuso una infracción del artículo 10 de la ley, por vulneración del deber de secreto. En el campo de los Cuerpos y Fuerzas de Seguridad del Estado, se dictó una resolución de archivo en la inspección realizada a la Jefatura Superior de Policía de Sevilla por mantener unas fichas de filiación en las que se recogían datos de raza, color de piel y otras características físicas de los sospechosos. En este caso, las actuaciones fueron archivadas, atendiendo a que el tratamiento realizado en las fichas era manual y estaban, por tanto, fuera ámbito de la Lortad y que, en todo caso, la información se recababa en el ámbito de una investigación concreta y, por tanto, amparada en el artículo 20 de la ley. También se iniciaron actuaciones inspectoras para verificar si los ayuntamientos de Arganda del Rey y Alcobendas habían procedido a cumplimentar unas fichas de filiación de personas que incluían datos antropomórficos, datos relativos a la vida sexual, origen racial y salud, todos ellos especialmente protegidos de acuerdo con el artículo 7 de la Lortad.

En el caso del Ayuntamiento de Arganda del Rey las actuaciones se archivaron, ya que las fichas de filiación estaban sin rellenar y además no se encontraban indi cios de su posible automatización, resultando por ello no ser aplicable la Ley de protección de datos. En el seno del Ayuntamiento de Alcobendas se inició procedimiento de infracción de administraciones públicas al comprobarse que la policía local mantenía un fichero automatizado de personas de interés policial en el que se recogían datos especialmente protegidos sin contar con el consentimiento de los afectados y sin cumplir lo señalado en el artículo 20 de la ley orgánica, es decir, lo relativo a los ficheros policiales y al tratamiento de datos sensibles sólo en el supuesto de investigaciones concretas.

Hay que resaltar que en este caso se había adoptado inicialmente una medida cautelar, consistente en que ese Ayuntamiento cesara de manera inmediata en la utilización ilícita de los datos personales de carácter antropomórfico, de raza, vida sexual y salud, que se recogían en el fichero en cuestión. Tras comprobarse en una inspección posterior que, aun habiéndose ordenado la adopción de esta medida cautelar los datos en cuestión seguían permaneciendo en el fichero director de la Agencia acordé la inmovilización del mismo. En la resolución final del procedimiento se acordó elevar a definitiva la medida cautelar adoptada, así como ordenar la destrucción de los datos especialmente protegidos que se incluían en aquel fichero. Otro tema a considerar es el que afecta a los ficheros de las comunidades autónomas.

Dentro de los procedimientos no informados en anteriores comparecencias mías, merecen destacarse los siguientes. El Departamento de Economía y Hacienda del Gobierno navarro facilitó a determinadas entidades, con las que previamente había suscrito un convenio de colaboración, un CDROM conteniendo datos identificativos y económicos de los contribuyentes navarros para facilitar la confección de la declaración del IRPF. El sistema permitía el acceso a los datos tributarios de los clientes de las entidades financieras sin el consentimiento previo de los afectados. De ello se dedujo que el departamento de Economía y Hacienda había infringido lo dispuesto en el artículo 11 de la Lortad, lo que supone una infracción tipificada como muy grave por la ley. Bueno es decir que inmediatamente estas deficiencias fueron corregidas voluntariamente por el responsable del fichero.

El Servicio Canario de la Salud, a pesar de los requerimientos de la Agencia de Protección de Datos, no procedió a notificar los ficheros automatizados que contuvieran datos de carácter personal y cuya titularidad les corresponde. Por ello, el director de la Agencia resuelve declarar la infracción del artículo 18 de la Lortad, tipificada como leve en esta ley. El número de procedimientos de infracciones de administraciones públicas por vulneración de la ley orgánica incoados a integrantes de la Administración local durante 1999 fue nueve, de ellos seis se debieron a infraccion del artículo 18 de la ley orgánica por no atender la obligación de inscripción, en otras dos ocasiones por cesión de datos a terceros y sólo

en un caso, en el caso del Ayuntamiento de Motril, se archivó el procedimiento al no quedar acreditado los hechos denunciados. En el campo de la sanidad pública ya avancé al comienzo de mi exposición que, como continuación del plan de oficio de inspección a hospitales en 1999, se han inspeccionado los hospitales militar Gómez Ulla y psiquiátrico penitenciario de Foncalent, de Alicante. Asimismo, durante este año han realizado dos inspecciones de oficio, iniciadas en 1998, al Registro Nacional del SIDA y al denominado proyecto TAIR, terminal autónomo de identificación de recetas, implantado en centros de salud de atención primaria del Insalud, del que ya informé en mi anterior comparecencia.

Igualmente, de acuerdo con el compromiso de someter al criterio de la Agencia de Protección de Datos los sucesivos desarrollos del proyecto TAIR, a lo largo del presente año el Insalud presentó para su análisis nuevas aplicaciones del proyecto que, tras su examen por la Agencia, merecieron diversas observaciones que fueron recogidas por aquel organismo. De las actuaciones de investigación y comprobación realizadas por la inspección de datos de esta Agencia en el ámbito sanitario se obtuvieron una serie de conclusiones que dieron lugar a que a principios del año 2000 se dictaran por la Agencia las oportunas recomendaciones de las que se dará información en la memoria correspondiente a dicho ejercicio. No obstante, sí quiero resaltar a SS.SS. que la Agencia de Protección de Datos tiene una especial sensibilidad en el tratamiento de datos especialmente protegidos, como son los relativos a la salud, y de ahí la preocupación y seguimiento constante que se hace de los mismos por la Agencia.

Entrando ahora en el área de los ficheros de titularidad privada, las inspecciones realizadas y consecuentes expedientes incoados han sido muy diversos y afectan a varios sectores de actividad. Destacaré tan sólo los más significativos. En el caso de los colegios profesionales, durante 1999 se han recibido en la Agencia nueve escritos donde se pone de manifiesto la posible utilización irregular de los datos de profesionales colegiados y la comunicación o cesión de datos a colegios, consejos de colegios profesionales y otras entidades. Agrupando las reclamaciones por sectores, se observa que la mayor parte se han referido al sector médico. Dos denuncias se refieren a los colegios de abogados de Madrid y de Vigo, y otra reclamación concierne a los consejos de colegios profesionales de médicos y de arquitectos. Respecto a la tipología de las reclamaciones formuladas, cabe destacar que la mayor parte de ellas denuncian la cesión de datos de los colegios profesionales a sus respectivos consejos. Sin embargo, la interdependencia existente entre ambos tipos de instituciones, según los diversos estatutos, justifican la relación jurídica existente entre ellos y, por tanto, la comunicación de datos. Por el contrario, cuando se han efectuado cesiones a entidades privadas sin el consentimiento del afectado, se han dictado las correspondientes resoluciones sancionadoras. Quiero adelantarles que, dada la doble personalidad, jurídicopública y jurídicoprivada, que ostentan los colegios profesionales, se les permite ser titulares de ficheros tanto públicos como privados, con la consiguiente dificultad en muchos casos de su diferenciación.

Por ello, en el año 2000, la Agencia de Protección de Datos ha suscrito un protocolo con la Unión Profesional, de la que dependen todos los consejos superiores profesionales, al objeto de facilitar a los colegios, por sus cauces institucionales, el conocimiento y cumplimiento de la Ley de protección de datos. Otro sector importante es el de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito. En este campo, las principales infracciones sancionadas fueron consecuencia de: falta de notificación a los afectados respecto de los que se han registrado datos personales en este tipo de ficheros en los términos establecidos en el artículo 28.1 de la Lortad; la conculcación del principio de calidad de datos establecido en el artículo 4 de dicha ley; la vulneración del principio del consentimiento del afectado en el tratamiento automatizado de sus datos personales, regulado por el artículo 6 de la misma; la cesión no legítima de datos entre entidades, conculcando los principios establecidos en el artículo 11 de la ley. Alo largo de 1998, la Agencia de Protección de Datos llevó a cabo un plan de inspección, de oficio sobre este tipo de ficheros. El alcance, criterios de la inspección, objetivos y resultados de la ejecución del plan de inspección fueron descritos en la memoria correspondiente a dicho año y en 1999, como colofón de las actuaciones derivadas del plan de inspección, se dictaron una serie de recomendaciones dirigidas a las empresas del sector responsables de ficheros de prestación de servicios sobre solvencia patrimonial y crédito, como ya adelanté a esta Comisión en mi anterior comparecencia. Al igual que en años anteriores, el sector de la publicidad y del marketing también ha recibido denuncias por parte de los ciudadanos. El envío postal de publicidad y el marketing son sectores que tradicionalmente se denuncian ante la Agencia.

Las principales resoluciones sancionadoras han sido por cesión de datos sin consentimiento y por tratamiento de datos personales sin contar con el consentimiento del afectado.

Es de destacar, en lo que se refiere a este sector, que la nueva Ley orgánica de protección de datos de carácter personal mejora la protección de los ciudadanos al exigir que en cada comunicación que se dirija al interesado se le informe del origen de los datos y de la entidad responsable del tratamiento, así como de los derechos que le asisten.

Estas exigencias no estaban en la Lortad, lo que hacía que, muchas veces, el ciudadano tuviera que recurrir de una empresa a otra, que le remitía a otra anterior, que a su vez había recibido los datos de otra.

Ahora, en cada comunicación habrá que comunicar el origen de los datos; en definitiva, dónde se obtuvieron esos datos por primera vez.

De esta forma, el ciudadano podrá ejercitar con mucha más facilidad, si así lo desea, el derecho de cancelación o rectificación de los mismos.

En el año 1999, la Agencia de Protección de Datos inició un plan de oficio, con el objeto de analizar los ficheros automatizados y la información manejada por las entidades del sector de la investigación privada, por los detectives privados, cuya actividad está regulada en la Ley 23/1992, de 30 de julio, de Seguridad Privada, y en el Real Decreto

2364/1994, por el que se aprobó el Reglamento de Seguridad Privada.

De las investigaciones y comprobaciones realizadas sobre los ficheros inspeccionados no se han detectado irregularidades significativas. La mayor parte de su actividad afecta a personas jurídicas, por lo que quedan fuera del ámbito de aplicación de la Lortad, y en cuanto a los datos de personas físicas, en las inspecciones realizadas no se han constatado cesiones de datos inconsentidas, siendo el propio cliente que encarga la investigación el dústinatario de sus resultados, cumpliendo los detectives privados con la obligación de guardar el secreto que les impone la legislación vigente. Por tanto, a tenor de los resultados de la inspección, que finalizó a finales de año, y al margen de las obligaciones que a los detectives privados impone su normativa específica, el Director de la Agencia, a principios del año 2000, emitió unas recomendaciones que deberán ser observadas por estas entidades del sector de la investigación privada al objeto de adecuar sus tratamientos automatizados a los principios normativos de la Ley de protección de datos. Para terminar con este apartado relativo a los planes sectoriales, voy a concretar los aspectos más relevantes de las inspecciones realizadas en el sector de las telecomunicaciones. La normativa sobre protección de datos se complementa en este sector por la Directiva 97/66CE, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que ha sido incorporada a nuestro ordenamiento jurídico por la Ley 11/1998, General de Telecomunicaciones y el título V del Real Decreto 1736/1998, de 21 de julio. Las actuaciones de la Agencia durante 1999 en el sector de las telecomunicaciones se han desarrollado en un doble plano de actividad: planes sectoriales de inspección de oficio y atención a las denuncias de los ciudadanos que se han presentado sobre esta materia. Las más significativas actuaciones de la Agencia en uno y otro orden de actividad han sido las siguientes.

En el ámbito de los planes sectoriales de inspecciones de oficio realizadas en el sector, se han inspeccionado los principales operadores de telefonía fija, como ya cité al comienzo de esta comparecencia.

Dentro de estas inspecciones merecen destacarse tres actuaciones diferentes: la primera, se refiere a la forma de prestación de consentimiento de los abonados para que los datos personales puedan ser tratados por los operadores; la segunda actuación se concreta en el análisis sectorial del Real Decreto 1736/1998 y el grado con que los operadores se adecuan a sus prescripciones, y la tercera actuación afecta a los denominados procedimientos de **scorin**g. Voy a referirme a ellos brevemente. En la inspección realizada a uno de los principales operadores se ha podido constatar un tratamiento masivo de datos que afectaba a dos colectivos de abonados: el primero, formado por los abonados que no habían dado su consentimiento para que sus datos personales fueran tratados por operadores de telefonía o a los que ni siquiera se les había dado la posibilidad de prestar su consentimiento para dicho tratamiento y el segundo, integrado por los abonados a los que les fue solicitado por el operador el consentimiento para tratar sus datos, pero mediante una fórmula no considerada válida por la Agencia de Protección de Datos al no cumplir las exigencias de la Lortad y de la legislación especial. Respecto del primer colectivo, y como resultado de la mencionada inspección, se constató que el operador disponía de un fichero automatizado de **data warehouse** cuyo objetivo era el tratamiento automatizado de los datos de tráfico y facturación telefónica con fines comerciales propios. El sistema recogía, grababa y almacenaba también los datos de detalle de todos los abonados, manteniendo al día el detalle de varios millones de llamadas diarias durante varias semanas, así como prácticamente la facturación del último año, y todo ello referido a la totalidad de sus abonados que ascienden a varios millones.

Igualmente, el **data warehouse** permitía obtener información sobre el nombre, apellidos y domicilio, tanto de los titulares que realizaban la llamada como de los titulares del teléfono que recibe la llamada.

Como saben SS.SS., para realizar la facturación las compañías telefónicas tienen que mantener durante un tiempo los datos de aquellos teléfonos a los que llamamos, pero en ningún caso es necesario para esta función conocer los números de teléfonos de aquellas personas que nos llaman, pero estos también se incluían en el tratamiento. La misma situación se producía respecto de los datos personales de tráfico y facturación telefónica de los abonados que habían adquirido tal condición con posterioridad al mes de enero de 1999, fecha en la que el operador remitió un encarte solicitando el consentimiento de los afectados, por no haberse requerido su consentimiento para haberlo llevado a cabo. Todo ello ha supuesto la incoación al citado operador de un procedimiento sancionador por infracción del artículo 6 de la Ley Orgánica 5/1992, por tratamiento automatizado de datos de carácter personal sin consentimiento de los afectados y por incumplimiento de los preceptos de protección de datos que imponen las disposiciones reglamentarias de desarrollo. Dentro de este procedimiento sancionador y mediante acuerdo del director de la Agencia de Protección de Datos, se adoptó la medida cautelar consistente en que por parte del operador se cesase de manera inmediata en el tratamiento automatizado de estos datos. Dicha medida cautelar fue cumplida por el operador, que procedió a borrar todos los datos de carácter personal de **data warehouse,** borrado que afectó a la totalidad de sus abonados y que impidió que el sistema se volviera a cargar con nuevos datos.

Este procedimiento terminó con una resolución de la Agencia, confirmatoria de los hechos imputados, que sancionó al operador en los términos arriba estos con una multa de 50 millones de pesetas. Respecto del segundo colectivo mencionado y dentro de la citada inspección, se investigó el procedimiento utilizado por el operador para recabar el consentimiento para tratar datos de tráfico telefónico de sus abonados. Considerando que la carta remitida a los abonados para recabar el consentimiento no reunía las exigencias normativas, se hizo necesario que la operadora de telefonía remitiera una nueva carta. Respecto a este punto debo señalar que la Directiva 97/66 no distingue, en su artículo 6, sobre la forma de prestar el consentimiento para tratar datos de facturación del abonado. El legislador español ha admitido expresamente en el artículo 65 del Reglamento el consentimiento tácito del afectado para que los operadores puedan tratar sus datos de tráfico y facturación para la promoción comercial de sus propios servicios de telecomunicaciones.

Aquí no están habilitadas cesiones a terceros ni a ninguna empresa del grupo. Por ello, la segunda carta recibida por los abonados debe considerarse que es conforme con las exigencias del artículo 65.3, antes señalado, porque efecti-

vamente opta por el sistema de la obtención del consentimiento tácito. En efecto, en ella se requiere el consentimiento para tratar automatizadamente los datos personales, se informa de que el consentimiento solicitado, facultativo y no obligatorio, es para ofrecer servicios de telecomunicaciones de la empresa Telefónica, no de terceras compañías, así como de la norma que habilita para obtener el consentimiento tácito, y se incluye la referencia expresa a la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y el lugar del responsable del fichero ante el que pueden ejercitarse esos derechos. De otro lado, el destinatario de la carta puede conocer los datos de tráfico y facturación objeto de tratamiento, en la medida en que consta en la factura que se le envía periódicamente por la compañía.

De ahí que aconsejáramos que esta petición de consentimiento se acompañara a la factura para que el ciudadano, a la vista de la misma, supiera de verdad qué datos suyos estaba consintiendo que se trataran. En lo que se refiere al procedimiento a través del cual el operador solicita el consentimiento, la norma no contiene previsiones específicas que obliguen a garan tizar la efectividad de la recepción por los destinatarios. Se tratará, en su caso, de un problema de prueba cuya carga deberá ser soportada por el operador que afirma contar con el consentimiento del abonado. En consecuencia, en tanto no se produzca una modificación normativa del artículo 65.3 del Real Decreto 1736, de 1998, deberá considerarse que la carta remitida se adecua a las exigencias disponiendo el abonado de la opción de manifestar su consentimiento contrario de los datos, así como de revocarlo posteriormente. Otro de los aspectos analizados durante las inspecciones sectoriales de oficio y que aún se encontraba en fase de tramitación a finales del ejercicio ha sido dirigido específicamente a comprobar el grado de adecuación de estos operadores a las prescripciones del Real Decreto citado 1736, de 1998, relativas a la prestación de servicios avanzados de telecomunicaciones, encontrándose determinadas deficiencias relativas a la seguridad, datos que deben constar en las guías telefónicas para identificar a un abonado concreto, llamadas telefónicas con fines de venta directa y servicio de prestación y limitación de identificador de línea llamante y línea conectada, entre otros más importantes. Para corregir estas deficiencias, en el año 2000 se den las oportunas recomendaciones de las que se dará cuenta en la memoria de dicho ejercicio. Cabe destacar también las inspecciones sectoriales practicadas en relación con los denominados procedimientos de **scoring.**

Estos procedimientos consisten, en esencia, en que un operador facilita a otra entidad especializada una información sobre solvencia patrimonial y crédito en relación de sus propios o potenciales clientes, la cual es posteriormente devuelta por ésta pero ampliada con una clasificación con información sobre la aptitud crediticia de cada uno de esos clientes, lo cual sirve al operador para rechazar o no la solicitud del servicio realizada por el potencial cliente.

Esta operación de **scoring** puede suponer una cesión inconsentida de datos personales a efectos de la Ley española de protección de datos, razón por la que se han abierto dos procedimientos sancionadores a otros tantos operadores y que han concluido en el año 2000 con una resolución sancionadora por cesión de datos sin consentimiento. Pensemos, señorías, que todas estas nuevas técnicas de marketing son un paso más en la invasión a nuestra intimidad. Si nosotros damos el consentimiento para recibir una determinada publicidad o para que nos oferten unos determinados servicios, ello no supone que mediante unos tratamientos sofisticados puedan conocer nuestros hábitos de consumo, incluso nuestras capacidades de decisión en diversos ámbitos. A mi modo de ver, son sistemas peligrosos ante los que tendremos que estar vigilantes porque son un paso más dentro de nuestra intimidad. Por último, dentro del sector de las telecomunicaciones me referiré al alto porcentaje de denuncias relacionadas con el uso de datos personales de abonados a los servicios de telecomunicaciones. Las más significativas afectan a las siguientes.

Se han recibido denuncias que hacen referencia a la difusión de datos personales de un importante operador de telefonía realizada a través del enlace Internet con el nombre de ®páginas blancas **on line¯,** que permitía a cualquier usuario conocer el nombre completo, número de teléfono y domicilio y al que se adjuntaba un plano a través del cual se puede ubicar el emplazamiento exacto de la calle donde está el domicilio del abonado. Este servicio que ofrece el operador, según consideran los denunciantes, vulnera la legislación de protección de datos al incluir en el tratamiento datos que no son adecuados ni pertinentes y sí excesivos para la celeridad legítima de dicho tratamiento, que no es otra que la de facilitar el número telefónico de un abonado para realizar una comunicación telefónica, siempre que figure en la guía su nombre y dirección. Lógicamente, esta información no podrá proporcionarse respecto de aquellos ciudadanos que ejerciten el derecho de exclusión de su domicilio en la guía telefónica. Las actuaciones previas relacionadas con este tipo de denuncia han concluido con resolución de archivo, por entender la Agencia de Protección de Datos que la mera posibilidad de poder consultar la localización geográfica del domicilio de los abonados no supone una ampliación de los datos de acceso público de dichos abonados, dado que en la consulta simplemente aparece el plano de situación con el nombre de la calle y la ubicación del número del inmueble al que corresponde. Los planos de una localidad no suponen en sí mismos una invasión de la intimidad de las personas físicas que en ella residen, máxime cuando los ciudadanos tienen derecho a excluir su domicilio en las guías telefónicas y en cuyo no se facilita ni aquel domicilio ni el plano donde se ubica.

En todo caso, a la hora de dictar esta resolución se tuvieron en consideración por la Agencia las recomendaciones del grupo internacional de protección de datos en materia de telecomunicaciones, en las que se considera como una violación de la intimidad el acceso a la imagen digitalizada de los edificios, pero no a un simple plano callejero de guía urbana que no da mayor tipo de información.

También se han denunciado ante la Agencia aspectos relacionados con la búsqueda inversa en directorios, esto es, obtener identificación y/o dirección de una persona a través de su número telefónico, de su fax o de su correo electrónico. La existencia de este tipo de servicios representa una amenaza para la privacidad. La finalidad de un repertorio con búsqueda inversa es diferente de la de un repertorio tradicional de abonado, y si bien el recurso de los directores inversos puede servir a intereses legítimos en los casos especiales de emergencia o de seguridad pública, el proporcionar los datos de un usuario a partir de su número telefónico sin disponer del consentimiento del usuario constituye, a nuestro juicio, un tratamiento desleal de la información. En virtud de las denuncias recibidas y por estar los operadores que proporcionan esta información en el extranjero, concretamente en Bélgica, la Agencia se ha dirigido a la autoridad

de control de este país al amparo de lo establecido en el artículo 28.6 de la Directiva para que informe sobre si el tratamiento de datos denunciados se adecua a las previsiones de la ley belga y, en su caso, actúe. Este sistema, que en principio puede parecer inofensivo, tiene en definitiva graves consecuencias. Como ustedes saben, señorías, en nuestro Estado de derecho sólo pueden interceptarse las comunicaciones por en judicial.

Si el juez da la orden para interceptar una comunicación, se intercepta ese número pero no los números que llaman a él. A través de esa interceptación se conocerán los números que llaman y se podrá proceder al margen del control judicial a realizar prácticas que pudieran ser ilegales con esos números llamantes. De ahí que este tipo de búsquedas inversas que pueden ser útiles con los debidos controles no pueden nunca ser de acceso público, a criterio de la Agencia de Protección de Datos. Este tema, por otra parte, ya lo he puesto en conocimiento de las autoridades de control de la Unión Europea dentro del grupo del artículo 29 de la directiva que nos obliga a todas las autoridades de control a reunirnos periódicamente para tratar temas de armonización, a fin de que se tome una postura común en un tema tan delicado. En el ámbito internacional y con esta última faceta de la Agencia termino la exposición de la memoria, destacan las siguientes actuaciones de la Agencia. En primer lugar, los trabajos llevados a cabo por el grupo del artículo 29, que ha sido creado como un grupo de trabajo sobre protección de datos de las personas en lo que respecta al tratamiento de datos personales. Este grupo es un foro común de debate de las autoridades de control nacionales que permite la armonización de la actuación e iniciativas desarrolladas en cada Estado miembro. Además, el grupo del artículo 29 tiene la obligación de facilitar a la Comisión, al Parlamento Europeo y al Consejo un informe anual sobre el estado de protección de las personas físicas con respecto al tratamiento de sus datos personales en la comunidad y en terceros países.

La Agencia española forma parte de este grupo y participa activamente en los diversos debates y trabajadpres aleatorios de los distintos documentos elaborados por el mismo. Como fruto de este trabajo en el ejercicio de las competencias atribuidas por la directiva, el grupo de trabajo ha elaborado durante 1999 más de trece documentos. Los grandes asuntos que han ocupado la atención del grupo del artículo 29 han sido el análisis de proceso de trasposición de la Directiva 95/46 a la legislación nacional de los Estados miembros, la adecuación o no del nivel de protección de datos en terceros países, las negociaciones entre la Comisión Europea y el Gobierno de los Estados Unidos de Norteamérica en relación con los llamados principios de puerto seguro, el estudio de diversos códigos tipo sectoriales, las propuestas de cláusulas contractuales tipo confeccionadas por diversas organizaciones al objeto de garantizar los principios de protección de datos en las transferencias internacionales a países que no gozan de igual nivel de protección y la aplicación de los principios de protección de datos en Internet, aspecto este que abordaré luego al intervenir en una petición de comparecencia expresa sobre el tema. Por lo que respecta a la trasposición de la directiva, en cada una de las reuniones de trabajo se ha efectuado un seguimiento, estando previsto dirigir en los primeros meses del año 2000 una recomendación instando a los Estados que aún no han traspuesto la directiva a cumplir con su obligación. Como resumen de la situación en este campo, a finales de 1999, los trabajos de trasposición no habían concluido en Dinamarca, Alemania, Francia, Irlanda, Luxemburgo y Países Bajos, lo que ha motivado la apertura de un procedimiento de infracción a estos Estados por parte de la Comisión en el año 2000.

En lo que respecta al análisis de adecuación de terceros países, a lo o de 1999 se han aprobado sendos dictámenes favorables a la consideración de Suiza y Hungría como Estados que conceden un nivel de protección adecuado.

Asimismo, durante 1999 se ha iniciado el análisis del régimen existente en otros terceros Estados como Eslovaquia, Eslovenia y Polonia y los territorios extracomunitarios británicos de las islas de Man, Guernsey y Jersey. No obstante lo señalado anteriormente, la mayor parte de los esfuerzos realizados por el grupo durante 1999 se han centrado en el análisis de un nivel adecuado de protección de datos en los Estados Unidos de Norteamérica. Frente al estudio de otros Estados en los que el punto de partida para el análisis de las cuestiones ha sido el estudio de una legislación de protección de datos aplicables en todo el territorio del Estado, la protección de la intimidad y de los datos en Estados Unidos se enmarca en un complejo entramado de regulación sectorial, tanto a nivel federal como estatal, que se combina con la autorregulación industrial. En este sentido, el grupo de trabajo ha considerado que este conjunto de leyes sectoriales, muy segmentadas y de autorregulación voluntaria, no son suficiente para proporcionar protección adecuada en todos los casos a los que los datos personales se transfieren desde la Unión Europea. A fin de superar los problemas derivados de esta dispersión normativa, el departamento de Comercio de los Estados Unidos presentó como documento para la discusión entre las autoridades norteamericanas y la Unión Europea un borrador de principios de puerto seguro, complementado posteriormente con una lista de preguntas más frecuentes, FAQ, a fin de garantizar a los operadores que se adhirieran a los mismos una protección de adecuación al nivel similar con el que dota la directiva comunitaria, permitiéndose así la libre circulación internacional de datos a dichos operadores. Para ello los operadores deberían manifestar ante la Oficina federal de Comercio u otra entidad por ella designada su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas.

Reiteradamente, a lo largo de los dictámenes emitidos por el grupo de trabajo del artículo 29 se ha puesto de manifiesto la dificultad en la comprensión de los principios como consecuencia de la aparición de las FAQ, que en muchos casos excepcionan el régimen general contenido en aquellos principios; también la ausencia de un mecanismo ágil y adecuado para satisfacer los posibles perjuicios causados a los ciudadanos europeos por el incumplimiento de los principios; la inexistencia de mecanismos que aseguren en la práctica el cumplimiento de los principios, garantizando la imposición de sanciones a las entidades adheridas que los incumplan; la falta de mecanismos previstos para evitar que una vez producida la transferencia a Estados Unidos los datos sigan protegidos adecuadamente, siendo posible que los mismos sean cedidos a otras terceras entidades en cualquier otro lugar del mundo; la imposibilidad de conocimiento por parte de los nacionales de los Estados miembros de la Unión Europea y de las propias autoridades de control de las empresas adheridas al puerto seguro y de las medidas adoptadas en caso de incumplimiento; la falta de adecuación de algunos de los principios con los criterios derivados de las directrices de la OCDE y, aún en mayor medida, de las normas europeas de protección de datos y la falta de mecanismos de verificación por parte de las auto-

ridades federales de los Estados Unidos, a fin de comprobar el cumplimiento de los principios por parte de las empresas adheridas.

Todos estos mecanismos se reemplazan por un sistema de autoverificación. Ante estos hechos, y tras conocer la noticia publicada en diversos medios de comunicación el 15 de marzo de 2000 en que había aparecido en los medios de comunicación la existencia de un principio de acuerdo entre la Comisión y el Gobierno de los Estados Unidos sobre los principios de puerto seguro sin que se hubiera producido la posibilidad de que el grupo del artículo 29 realizara un análisis final de los mismos, en la reunión del 16 de marzo de 2000 se adoptó por unanimidad un documento de la Agencia española instando al comité representativo de los gobiernos de los Estados miembros que habían de dar su conformidad definitiva al texto a que, con carácter previo a dicha decisión, se sometiera el documento final de puerto seguro en su integridad para nueva deliberación por el grupo de trabajo del artículo 29, dado que el mismo tendría una importancia vinculante sobre las autoridades de control europeas. Además, el documento recordaba que el Parlamento Europeo en su reunión de 23 de febrero de 2000 había solicitado conocer la opinión del grupo de trabajo con carácter previo a la discusión y aprobación de su dictamen. Como consecuencia de lo que se ha venido exponiendo, en el último dictamen aprobado en el año 1999 el grupo de trabajo del artículo 29 consideró que los acuerdos de puerto seguro propuestos, tal como quedaban en la versión existente y en diciembre de 1999, continuaban siendo insatisfactorios y se invitaba a la Comisión a que instase a la parte estadounidense a realizar una mejora de los mismos. En particular, los principios de puerto seguro no pasan de ser unos códigos de buena conducta enunciados mediante un conjunto de normas genéricas a las que se añade un grado aún mayor de indefinición con las FAC o preguntas más frecuentes, que además son inconcretas y generales.

Si ha ello unimos que toda la aplicación del código está basada en mecanismos de autorregulación del sector privado, que las autoridades gubernamentales norteamericanas, a través de una gran dispersión de organismos y competencias, sólo puedan entrar a juzgar sobre la existencia de infracciones cuando el tipo infractor se puede encuadrar en lo que según la legislación estadounidense genéricamente se conocen como prácticas comerciales engañosas o desleales, y para finalizar no existen cauces claros y adecuados para que los ciudadanos europeos puedan ejercer sus derechos de acceso, rectificación, oposición y cancelación con las garantías adecuados; si se tienen en cuenta todas estas cuestiones, de ahí la crítica y la oposición que mantenemos a los principios de este acuerdo.

Las negociaciones relativas a los principios de puerto seguro continuaron a lo largo del año 2000, y a partir del dictamen final del grupo de trabajo en el que se hace notar que seguía preocupado por diversos aspectos, y a pesar también de que el dictamen emitido por el Parlamento Europeo era contrario a estos principios, la realidad, señorías, es que por una decisión de la Comisión, publicada el 25 de agosto en el DOCE, se han aprobado los principios de puerto seguro. A pesar de esta desfavorable situación para la protección de los datos con destino a Norteamérica, la Agencia de Protección de Datos, dentro de las competencias que la ley le atribuye, seguirá controlando que con carácter previo a cualquier transferencia los datos sean tratados en origen con las garantías que establece la ley española y, por tanto, con respeto de los principios de cesión, de finalidad, etcétera. Otro foro importante donde participa también la Agencia es en el Consejo de Europa. En el año se firmó, como saben SS.SS., el Convenio 108 para la protección de los individuos en relación con el tratamiento automatizado de datos; convenio ratificado por nuestro país en 1984. Durante estos años, el Comité Jurídico de Protección de Datos, el CJPD, no sólo ha creado una serie de recomendaciones sino que también ha publicado estudios sobre temas específicos en el ámbito de protección de datos.

La Agencia española participa en este comité colaborando activamente en los diversos debates y trabajos. Durante 1999 el comité concluyó los trabajos relacionados con las recomendaciones sobre vida privada en Internet, adoptando defi nitivamente una recomendación, la R/99/5, para protección del individuo en lo que respecta a la recogida y tratamiento de datos de carácter personal en las autopistas de la información, que fue aprobada por el Comité de Ministros en su reunión de 23 de febrero de 1999, de las que les daré luego cuenta más detallada. Otro foro en el que estamos presentes es indudablemente Schengen, donde la Agencia española ha continuado participando como autoridad de control.

En este aspecto podemos decirles, resumiendo mucho, que se ha inspeccionado la unidad de apoyo técnico, el SIS, donde están todos los datos policiales que transmiten los distintos policías de los países miembros de Schengen, y que esta inspección se ha llevado a cabo fundamentalmente en base a un programa realizado por ingenieros de la Agencia de Protección de Datos española. También estamos presentes en Europol, tanto en la autoridad de control común como en el comité de recursos, en donde se establece la posibilidad de que los ciudadanos europeos, en el caso de que existan infracciones por parte de la autoridad común, recurran a un comité de recursos se han constituido y han empezado a funcionar este año. También es fruto de nuestra atención y de nuestra actividad el grupo de telecomunicaciones conocido por grupo Berlín, donde se han producido diversos documentos de importancia sobre este sector. Debo también hacer mención al grupo de trabajo sobre ficheros policiales de los comisionados europeos para la protección de datos, en el que se integrarán los del convenio SIA y los convenios Eurodac, relativo al almacenamiento de huellas dactilares sobre los solicitantes de asilo en los Estados miembros de la Unión Europea.

Y, finalmente, debo referirles nuestra participación en la conferencia de primavera de autoridades europeas de protección de datos, celebrada en Helsinki del 14 al 16 de abril, donde la Agencia de Protección de Datos presentó tres ponencias, además de participar en los debates de las restantes. Por lo que respecta a la conferencia internacional, en la que se reúnen no sólo las autoridades de control europeo sino de otros países ajenos a la Unión que tienen autoridad de control, este año se celebró en 1999 en Hong Kong. Tengo que decirles que si bien asistió una delegación de la Agencia española, personalmente no fui porque pocos meses antes se había producido la anulación por parte del Partido Comunista chino de las sentencias dictadas por el Tribunal Supremo de Hong Kong, con lo que a mi modo de ver se quebraba el principio de un país dos sistemas y se sustituía desgraciadamente por el de un país un sistema, y no parecía adecuado participar en aquel foro con un sistema donde se estaban violando los derechos humanos, porque

sin garantía judicial no pueden existir derechos humanos. Esta actitud mía fue seguida también por algunos comisionados europeos como el de Luxemburgo y el de Alemania. He tratado, de sintetizar las actividades de la Agencia, pero como ven son bastante amplias, sobre todo si tenemos en cuenta que se refieren a un año y a aspectos tanto nacionales como internacionales. No obstante, quedo a su disposición para cualquier aclaración o cuestión que quieran formularme.

La señora **PRESIDENT**

A: ¨Grupos que desean intervenir, aparte del Grupo Parlamentario Socialista, que evidentemente al ser el solicitante de la comparecencia será el primero?

(Pausa.)

Por el Grupo Parlamentario Socialista tiene la palabra la señora Del Campo.

La señora **DEL CAMPO CASASÚ**

S: Ante todo quiero, en nombre de mi grupo, agradecer al señor Fernández López su primera comparecencia de esta legislatura en esta Comisión para presentar la memoria de la Agencia de Protección de Datos y agradecerle, asimismo, el carácter exhaustivo de su exposición.

Ciertamente, esta es una memoria de transición en el sentido de que corresponde a un año, 1999, sobre el que ya planea la nueva Ley Orgánica 15/1999, que entró en vigor en enero de 2000. Pero a pesar de este carácter de transición, sí hay aspectos importantes sobre los que a mi grupo le gustaría hacer algunas observaciones y, aunque pueda parecer mentira a los miembros de esta Comisión, todavía nos queda alguna aclaración que solicitar a lo expuesto por el señor Fernández López. Trataré de seguir en lo posible el orden que el director de la Agencia de Protección de Datos ha seguido en su exposición, aunque no me será tan fácil. Por ello, empezando por el principio, aunque no sea lo más importante, he de decir que nos ha preocupado hasta cierto punto el aumento del tiempo medio de respuesta desde que una notificación tiene entrada en la Agencia hasta que se emite la resolución de inscripción; en 1998, si no recuerdo mal, eran tres días y en 1999 son siete.

Es cierto que todavía no es en absoluto preocupante esta cantidad de tiempo y también lo es que ha habido un gran aumento de solicitudes de inscripción, de un 50 por 100 más en 1999 y he creído entender que se han cuadruplicado en el año 2000. Sin embargo, querríamos instar a la Agencia a extremar la vigilancia para que este aumento de cantidades no redunde en una disminución de una eficiencia que hasta ahora es loable pero que poco a poco se va deteriorando. También nos gustaría plantear alguna cuestión y solicitar alguna aclaración relativa a la inscripción de ficheros públicos. Figura en la memoria de 1999 la existencia de reuniones por parte de la Agencia con una serie de representantes de distintas administraciones públicas para determinar sobre todo qué sistemas informáticos, con datos personales, todavía no han sido inscritos. Nos gustaría conocer el resultado de estas reuniones en el paso siguiente, es decir, en la consiguiente inscripción de los ficheros por parte de las administra ciones públicas, porque resulta hasta cierto punto preocupante la ausencia de inscripción sobre todo por parte de la administración local.

Hemos observado que todavía hay bastantes ayuntamientos, creo que 92 de más de 4.000 habitantes, que no han formalizado inscripción alguna de sus ficheros en el registro. Quisiéramos saber si a lo largo del 2000 esta inscripción ha ido aumentando y si han dado resultado aquellas actividades que se realizaron en 1999. También tendría curiosidad este grupo por alguna mayor aclaración en cuanto a las transferencias internacionales de datos de carácter contractual.

En 1998, según figura en la memoria del año pasado, hubo una sola transferencia de este carácter, precisamente la transferencia de Reader's Digest. Expuso su señoría las condiciones en que se efectuó esta transferencia, condiciones que ciertamente fueron muy rigurosas y absolutamente garantistas. Nos gustaría saber si en las tres transferencias correspondientes al año 1999 se ha mantenido igual rigor de condiciones e igual nivel de garantías. Otro aspecto que preocupa a mi grupo y que quisiera comentar de algún modo es el mal funcionamiento o las disfunciones en la aplicación de la protección de datos por parte de las administraciones públicas.

En la memoria figuran casos de sanciones a administraciones públicas. Concretamente ha mencionado su señoría las sanciones al departamento de Economía y Hacienda del Gobierno navarro por cesión de datos personales, la sanción al Servicio canario de Salud y, aunque no ha sido mencionada hoy pero sí ha sido abundantemente comentada a lo largo del año 1999, la cesión por parte de la Consejería de Bienestar Social de la Generalitat valenciana de datos de pensionistas destinados a la convocatoria de la famosa fiesta de la tercera edad. Aún sin llegar a producirse sanciones, la verdad es que hay ámbitos de la administración pública en que parece que la memoria refleja una cierta deficiente seguridad en los datos o al menos un constante caminar por la línea de la peligrosidad en la protección de los datos. No sólo la Agencia Tributaria o la Dirección General de Tráfico, también instituciones del ámbito sanitario, las inspecciones a que ha hecho referencia S.S. al Hospital Gómez Ulla, al Psiquiátrico Penitenciario de Alicante y al Centro Nacional de Epidemiología o los avatares del famoso proyecto de terminal autónomo de identificación de recetas, tanto desde el ámbito del Insalud como desde el farmacéutico, revelan una cierta situación fluctuante de la seguridad que la propia memoria de la Agencia de Protección de Datos refleja al establecer la necesidad de recomendaciones a todos estos organismos para una mejor protección de los datos personales. Dado que estas recomendaciones en la memoria se difieren al año 2000, quisiéramos tener alguna información sobre si se han llevado ya a cabo, y otra nueva información. Sabemos que el peligro en que pueda encontrarse la seguridad de los datos no es sólo un problema de formación y capa cidad de los funcionarios. Pero la capacidad y la formación de los funcionarios es un elemento importante para la protección de los datos personales.

Por ello, dado que el señor Fernández López, el año pasado, anunció su intención de organizar jornadas de formación de funcionarios de las distintas administraciones en la Ley de protección de datos, quisiéramos saber si estas jornadas de formación se han podido llevar a cabo y cuál ha sido su resultado, todo ello teniendo en cuenta que con la plantilla de 62 personas, que me parece recordar que usted ha dicho que tiene, es una tarea difícil de acometer y larga de culminar en el tiempo. Posiblemente, una necesidad de la Agencia de Protección de Datos que mi grupo desea resaltar en este momento es la de la ampliación de esa plantilla y mejorar su situación personal para llevar a cabo su labor con más eficiencia. Por otra parte, señorías, no voy a hacer aquí mención de los problemas de los ficheros privados. Sabemos que hay problemas serios en los ficheros que se refieren a la capacidad de crédito, problemas en los ficheros que promueven el marketing y problemas con Internet, pero como después hay una comparecencia que se centrará en el sector privado y fundamentalmente en Internet tampoco quiero alargar demasiado en este trámite la lista de preguntas del Grupo Socialista. Sí me gustaría hacer alguna referencia a la atención al ciudadano en sus reclamaciones o en sus solicitudes de información con relación a los ficheros de la Administración pública.

Sabemos que van aumentando las denuncias de los ciudadanos, además con una frecuencia casi vertiginosa, con relación al sector privado y también al sector público. Ahora bien, con algunas denuncias de vulneración de la intimidad por parte de las administraciones públicas, desde mi grupo creemos, señor Fernández López, que es posible que muchas de ellas se desvíen o no entren directamente en la Agencia de Protección de Datos sino en una institución más conocida y, por decirlo así, entre comillas, más popular, como es la del Defensor del Pueblo. Quisiéramos saber si existen criterios de comunicación sistemática y de coordinación con la institución del Defensor del Pueblo para hacer frente a estas denuncias y ubicarlas con mayor rapidez en su lugar natural, que es la Agencia de Protección de Datos. Por último, señorías, yo decía al principio que esta es una memoria de transición. La Ley Orgánica 15/1999 entró en vigor el pasado 14 de enero, lleva ocho meses funcionando y parece que esta solicitud de información y de aclaraciones no sería completa y no estaríamos al día si no pidiéramos algún avance sobre su funcionamiento.

En su última comparecencia ante esta Comisión decía que la aplicación de la ley no iba a estar exenta de dificultades y argumentaba una serie de motivos: la carencia de la exposición de motivos, el haber introducido las mayores novedades en un trámite no público y la falta de jurisprudencia interpretativa consolidable. Nosotros quisiéramos saber si en la práctica, a día de hoy, se están produciendo o no esas dificultades y en qué aspectos. Quisiéramos sobre todo una respuesta a dos cuestiones que nos preocupaban el año pasado, que nos siguen preocupando éste y que en este momento ya pueden ser respondidas. Una es hasta qué punto está respetando el derecho a la intimidad la discutida adicional sexta, la que preveía la posibilidad de compartidos por las entidades aseguradoras, sobre cuya adecuación el señor Fernández López también manifestaba algunas dudas en su comparecencia del año pasado. También quisiéramos saber si ese reglamento de medidas de seguridad (que fuimos el primer país en la Unión Europea en aprobar, yo no sé si con carácter diligente o con carácter prematuro, puesto que adelantamos en seis meses a una ley pendiente de aprobarse ese reglamento), en la práctica se está adelantando a esta ley posterior a él y está funcionando adecuadamente.

La señora **PRESIDENT**

A: Por el Grupo Parlamentario Vasco tiene la palabra el señor Erkoreka Gervasio.

El señor **ERKOREKA GERVASI**

O: En primer lugar, yo también quería darle la bienvenida, en nombre del Grupo Vasco, a esta Comisión Constitucional; bienvenida que no obedece exclusivamente a razones de cortesía parlamentaria elementales, por otra parte, sino que guarda relación, de alguna manera, con la importancia que desde el Grupo Vasco le damos al organismo que usted dirige, la Agencia de Protección de Datos; un organismo expresamente situado por la Lofage entre los organismos a los que la ley reconoce una independencia funcional o una especial autonomía con respecto a la Administración general del Estado; un organismo cuya ley creadora declara expresamente que actuará con plena independencia de las administraciones públicas en el ejercicio de sus funciones; un organismo, por otro lado, que entronca directamente con un derecho fundamental recogido en el párrafo cuarto del artículo 18 de la Carta Magna y que tiene encomendado el control de determinado tipo de actos de vulneración de derechos fundamentales, básicamente el derecho al honor, el derecho a la intimidad personal o familiar y, además, este nuevo y autónomo derecho a la autodeterminación informativa. Creemos que el cometido de la Agencia es importante de cara al futuro en una sociedad como la contemporánea o, más precisamente, como la occidental contemporánea, tan fuertemente mediatizada por la realidad informática y telemática, en la que quizás el paradigma orwelliano del Estado omniscente, o quizás habría que precisar más y decir de las grandes corporaciones omniscentes, ha superado ya completamente el terreno de la quimera para situarse en el ámbito de los riesgos reales y efectivos.

He leído con atención la memoria, he escuchado también su intervención (hay una sustancial identidad entre la primera y la segunda) y tenía una serie de preguntas, una serie de sugerencias, algunas de las cuales me las ha pisado la portavoz del Grupo Socialista, a pesar de lo cual me voy esmerar en reformularlas de manera que no se aprecie excesiva identidad entre las que ella ha formulado y las que yo voy a plantear. Aunque la Agencia actúa en principio con independencia en relación con la Administración general del Estado, es cometido de esta Comisión, quizá más precisamente de esta Cámara, controlar a la Agencia porque se sitúa en la órbita de la Administración general del Estado, pero controlar al mismo tiempo lo que dice a propósito de los archivos, de las bases de datos, de la información automatizada que contenga la Administración general del Estado. Por eso, en mi lectura de la memoria he puesto especial énfasis en aquello que la Agencia afirma a propósito de los archivos inspeccionados de la Administración general del Estado. He observado que en el ámbito competencial de la Subdirección General de Inspección de Datos, la memoria da cuenta de actuaciones de oficio desarrolladas en relación fundamentalmente con dos organismos: la Agencia Esta-

tal de Administración Tributaria y la Dirección General de Tráfico. Con respecto a la primera, se aprecian algunas irregularidades como la conservación de datos que debían ser cancelados, la inexistencia en los formularios del IRPF de referencia alguna al deber de información previsto en el artículo 5 de la Lortad y la inexistencia de unas normas documentadas que contemplen los procedimientos y criterios de tramitación.

En relación con la Agencia Estatal de Administración Tributaria, la memoria se limita a señalar que a principios del año 2000 dictará las recomendaciones oportunas para que la Agencia adopte las medidas pertinentes a fin de adecuar las deficiencias observadas en los tratamientos automatizados a los principios de la normativa vigente en materia de protección de datos.

Como se ha superado ya este límite temporal que preveía la memoria (desafortunadamente el tiempo como decían los clásicos, **tempus fugi**t transcurre a una velocidad endiablada) y nos estamos acercando mucho más a las postrimerías del año 2000 que a sus principios, que era el límite temporal marcado por la memoria, yo querría saber si han dictado ya alguna recomendación en relación con esta materia y, en caso afirmativo, qué se establece en ella. Otro tanto querría en relación con lo que se dice en la memoria a propósito de la inspección cursada por la Subdirección General de Inspección de Datos en la Dirección General de Tráfico. Aquí parece que las irregularidades revestían una enjundia mayor, eran más y algo más graves. Tampoco se han dictado recomendaciones y la memoria lo justifica con la próxima entrada en vigor de la ley actualmente vigente, la Ley Orgánica de protección de datos de carácter personal, que aconsejaba no dictar recomendaciones que después no estuvieran de acuerdo con las previsiones contenidas en la ley próxima a entrar en vigor. En relación con esto y ya que la nueva ley lleva varios meses en vigor, quería preguntarle si se ha dictado alguna recomendación adaptada a las nuevas previsiones y, en caso afirmativo, qué se establece en ella. Tengo un par de observaciones de carácter jurídico.

Aunque la memoria hace referencia a un período temporal en que la norma en vigor era la vieja Lortad y no la Ley Orgánica de protección de datos de carácter personal, quisiera plantear algunas cuestiones relacionadas con esta última. La Ley de protección de datos de carácter permisido objeto ya de algunas críticas en el plano doctrinal por parte de la doctrina científica. La memoria augura, como bien ha puesto de manifiesto la portavoz del Grupo Parlamentario Socialista, que su aplicación no estará exenta de dificultades por una serie de razones como la falta de exposición de motivos y demás. No es este el lugar adecuado para abundar en estas críticas, que son fundamentalmente de carácter técnico pero que tienen una incidencia importante en la salvaguarda real de los derechos fundamentales que se protegen a través de la ley.

Con todo, quisiera formularle una serie de preguntas en relación con este tema:

¨Han apreciado algún problema de aplicación? ¨Han apreciado algún espacio necesitado de protección de derechos fundamentales que, como consecuencia de los contenidos concretos de la ley, quede exento o al margen de la protección efectiva que requiere? ¨Se ha revelado ya alguna laguna o deficiencia técnica en la aprobación de la ley? Por otra parte, hablando en términos jurídicos, es inevitable hacer referencia al problema que planteaba el reglamento de seguridad.

La memoria alude explícitamente al problema que ha constituido para la Agencia de Protección de Datos el hecho de que durante varios años no se dictase el reglamento de seguridad que la Lortad requería inexorablemente para hacer efectivas las sanciones previstas en relación con las infracciones que supusieran incumplimiento de las medidas de seguridad. Paradójicamente, después de varios años de inactividad reglamentaria del Gobierno, se aprueba el reglamento cuando la nueva ley ya está siendo objeto de tramitación en las Cortes Generales. Un resultado entre otros es que, a efectos de sancionar el incumplimiento de las medidas de seguridad, el reglamento que ha entrado en vigor hace poco más de un año nos remite a los artículos 43, 44 y 45 de la Lortad ya derogada y, por tanto, extraída del ordenamiento jurídico.

¨No cree que una falta de adaptación, siquiera formal, del reglamento podría acarrear algún problema a la hora de hacer efectivas las sanciones, habida cuenta de la rigidez y el carácter restrictivo que presiden y que deben presidir el derecho administrativo sancionador? Una tercera sugerencia en cuanto a la información a los interesados.

Soy jurista, como usted, y sé que en nuestro ordenamiento jurídico la ignorancia de la ley no excusa de su cumplimiento, una máxima que aprendemos los estudiantes de derecho en el primer curso; pero me preocupa una declaración reciente del Consejo Superior de Cámaras de Comercio en la que se denuncian los perjuicios económicos que el desconocimiento de la Ley de protección de datos de carácter personal puede causar a las pequeñas y medianas empresas, cuya labor en un mercado tan condicionado por el marketing requiere inevitablemente disponer de información automatizada sobre posibles clientes o personas a las que pueden ampliar sus ofertas empresariales. Al expresar esta preocupación no intento anteponer el interés económico de las empresas privadas ni hacer prevalecer el derecho a la libertad de empresa, proclamado en el artículo 38 de la Constitución, sobre los bienes jurídicos que protege el artículo 18.4. No es, por tanto, mi propósito hacer prevalecer los intereses vinculados al tráfico mercantil sobre derechos fundamentales tan relevantes en el contexto constitucional como el derecho al honor, el derecho a la intimidad personal o familiar o el derecho a la autodeterminación informativa. Me limito a dejar patente una inquietud ante el riesgo de que un esfuerzo insuficiente de la Agencia por difundir los contenidos de la le
re los afectados pudiera generar graves daños en el tejido empresarial. Me consta que la Agencia ha llevado a cabo numerosas actividades orientadas a la difusión de la ley vigente, pero me permito sugerirle que intensifique en lo posible el esfuerzo desarrollado a fin de que nadie pueda alegar ignorancia y de que las infracciones que eventualmente puedan producirse sean todas ellas dolosas.

La señora **PRESIDENT**

A: Por el Grupo Parlamentario Catalán (Convergéncia i Unió), tiene la palabra el señor Jané.

El señor **JANÉ I GUASCH:**

En primer lugar, quiero agradecer al director de la Agencia de Protección de Datos su comparecencia y el contenido y la extensión de su intervención, que permite a todos los grupos parlamentarios profundizar en aspectos relevantes de la memoria presentada. Para no alargar la sesión de hoy no incidiré en aspectos ya planteados por otros portavoces que me han precedido en el uso de la palabra. Quiero manifestar al director de la Agencia que compartimos la importancia, a la que aludía expresamente, de respetar el derecho a la intimidad de las personas físicas. Es un derecho fundamental que, como tal, tiene esa vis expansiva que debe prevalecer siempre como principio ordenador del ordenamiento jurídico.

Hablaba también el director de la Agencia de las amenazas que las nuevas tecnologías pueden acarrear ante la invasión de la privacidad de los datos de los ciudadanos. El portavoz que les habla, profesor de derecho constitucional y miembro de la Comisión de Economía y de la nueva de Ciencia y Tecnología, quisiera reflexionar en voz alta sobre algún dato de la memoria. Considero que deberíamos intentar entre todos acotar el ámbito de aplicación de algunas sanciones. En la memoria se dice expresamente que el régimen administrativo sancionador en materia de protección de datos personales establecido en la ley española por tanto responsabilidad de los que estamos hoy aquí, los que tenemos la responsabilidad de hacer las leyes, y no del director es el más alto de la Unión Europea atendiendo al importe de las sanciones.

Por tanto, se reconoce expresamente que tenemos un régimen sancionador alto, con multas elevadas; un régimen que hemos querido los parlamentarios que sea así. Las sanciones de este régimen sancionador alto alcanzan la cifra de 1. 571 millones de pesetas, según reconoce la memoria. Cuales nociones son elevadas fracasa el derecho; cuando existe una sanción lo decía hace un momento el portavoz del Grupo Vasco, o la ley no está bien difundida o no la hemos regulado de la forma más adecuada. Pues bien, el hecho es que las sanciones son elevadas y se sanciona mucho, lo cual debe sugerirnos la reflexión sobre si se sanciona siempre de forma adecuada. En la memoria presentada se analizan 29 sentencias de las cuales 10 han sido revocadas por los tribunales; de las 29 sentencias recurridas en 10 han dado la razón al recurrente.

Quiero hacer la siguiente reflexión: tenemos el régimen sancionador más alto, se aplican las sanciones, se recurren y en una proporción de uno a tres se da la razón a la persona que ha sufrido la sanción. Yo quisiera que se aplicaran escrupulosamente las sanciones, siendo consciente a la vez de la necesidad de salvaguardar siempre los derechos fundamentales con esa vis expansiva y de no caer en una situación que colocara al tejido empresarial español en una posición comparativamente distinta de la del resto de Estados de la Unión Europea con los que tiene que competir. Hay un tema que el director de la Agencia conoce muy bien, que es la desigualdad jurídica en cuanto a la utilización de datos del censo electoral. Hay una desigualdad jurídica en España en relación con otros Estados de la Unión Europea, que se intentó superar con la Ley del Comercio Minorista, a través de una enmienda presentada por el Grupo Popular y que tuvo la aceptación de la Cámara; se quería aclarar una situación para superar determinadas resoluciones de la Junta Electoral Central.

La Agencia de Protección de Datos aludía en este caso a una disparidad normativa; estaba la Ley Orgánica del Régimen Electoral General, estaba la Ley del Comercio Minorista, y a ese artículo concreto también se declaró el carácter de orgánico. El propio director de la Agencia de Protección de Datos, usted mismo, reconoció en esta Cámara que era un tema preocupante porque podía dejar a las empresas del sector del marketing y de la publicidad en nuestro país en una situación peor que la de sus homólogos en los países de la Unión Europea. El 27 de mayo de 1998 usted apuntaba también a las consecuencias que esto puede tener de extraterritorialización de algunas empresas. Si aquí somos mucho más rígidos, la empresa se va a otro país de la Unión Europea cuya normativa, por lo menos en ese aspecto, tiene una mayor claridad de resolución; sin embargo, en el caso del Estado español podía darse esa disconformidad. Nuestro grupo se manifestó claramente en esta Comisión a favor de la interpretación que daba la Ley del Comercio Minorista, incluso por el criterio de que ley posterior deroga o aclara ley anterior cuando se regula el mismo supuesto. Para nosotros con la Ley de Comercio Minorista, en este caso y en ese artículo, que tenía la consideración de ley orgánica, porque así se aprobó en esta Cámara, quedaba clarificado el tema; sin embargo, como ha habido interpretaciones diversas, creemos que el nuevo marco normativo lo da la ley que se aprobó en la pasada legislatura, la Ley 15/1999. Esta ley, cuando enumera cuáles son las fuentes accesibles al público, cita al censo promocional. El censo promocional debe regularlo el Instituto Nacional de Estadística, pero bien es cierto que cuando ya se especifique en una ley orgánica que una fuente accesible al público es el censo promocional; deberíamos en estos supuestos concretos no penalizar a las empresas españolas cuando el marco normativo expresa una voluntad esos datos puedan ser accesibles al público.

Debemos pedirle al INE que lo regule, pero en ese período transitorio en el cual el INE aún no lo ha regulado, nosotros consideramos que la Agencia de Protección de Datos debería ser especialmente sensible a esa realidad, precisamente por lo que usted mismo expresaba hace dos años ante esta Comisión, por el peligro de extraterritorialización de muchas empresas, con la consiguiente pérdida de puestos de trabajo.

Todo ello se lo digo desde la óptica de la Comisión Constitucional, porque lo que debemos hacer es cumplir la ley, hacer cumplir todas las garantías que la ley orgánica da para la protección de la privacidad, con esa vis expansiva que debe tener siempre un derecho fundamental, como es este derecho que regula la ley orgánica, pero ante un reconocimiento expreso de que la ley española establece las sanciones más altas; no nos encontremos al final con que los ciudadanos tengan que revocar, vía jurisdiccional, unas decisiones que se han podido extralimitar. Le pido que tenga

como máxima responsabilidad cumplir la ley, difundirla, como decía el portavoz del Grupo Vasco, asentar ante los ciudadanos la necesidad de ser conscientes de lo que supone la privacidad de los datos personales, porque esto es importantísimo y lo va a ser en el ámbito de las nuevas tecnologías. Aquí se abrirá un nuevo debate. Este mismo año vamos a regular en esta Cámara la nueva ley de comercio electrónico, que en el ámbito de la protección de datos va a dar lugar a muchísimas cautelas. Intentemos encontrar ese punto de equilibrio que creo que entre todos podremos lograr.

La señora **PRESIDENTE**

A: Por el Grupo Parlamentario Popular, tiene la palabra el señor de Juan.

El señor **DE JUAN I CASADEVAL**

L: Señor director de la Agencia de Protección de Datos, en nombre del Grupo Popular le damos la más sincera bienvenida a la Comisión Constitucional de esta Cámara en esta su primera comparecencia durante esta legislatura; una comparecencia que se dirime en el seno de la Comisión Constitucional del Congreso sin duda por la trascendencia que tiene en términos de protección de derechos fundamentales y en términos de protección del derecho a la intimidad, sancionado y garantizado en el artículo 18 de la Constitución el tratamiento automatizado de datos de carácter personal.

La vocación del precepto constitucional del artículo 18 de nuestra norma fundamental es muy clara, se trata de garantizar un ámbito, una esfera de privacidad inmune a intromisiones ilegítimas, intromisiones que en el seno de la llamada sociedad de la información pueden proceder, y de una forma muy cualificada, de la manipulación de esos datos de carácter personal que pueden producirse en distintas esferas de la realidad social; de ahí la necesidad de esa regulación de lo que se ha dado en llamar el derecho a la autodeterminación informativa, lo que también se ha dado en llamar el **habeas data** o derecho a la libertad informática, en definitiva, a disponer de los datos de carácter personal que figuran en programas informáticos. Esa y no otra es, entendemos, la razón de ser de la legislación tuitiva del tratamiento automatizado de datos de carácter personal en relación a la privacidad, y esa y no otra es la razón de ser de la Agencia de Protección de Datos. Señor director, el Grupo Popular quiere manifestar en ese sentido su satisfacción, tanto por el nivel de madurez social que lentamente se va abriendo en nuestra sociedad en materia tan sensible como ésta en relación a la tutela del derecho a la intimidad personal, como también por el grado de cumplimiento de la ley y por la encomiable e insustituible labor que está desempeñando la Agencia de Protección de Datos en ese sentido. Probablemente la memoria de 1999 que hoy analizamos, y que brillantemente ha expuesto el señor director de la Agencia, es una buena muestra de ello. Las palabras del director general y la propia memoria reflejan un panorama satisfactorio, en términos generales, en el cumplimiento de la ley y en el índice de sensibilización social.

La memoria constata, y lo ha dicho el director de la Agencia, un incremento notable en inscripción de ficheros de titularidad privada en el Registro General de la propia Agencia, concretamente, si no me equivoco, estamos hablando de un incremento del 43 por 100; han aumentado también todas las operaciones registrales relativas a ficheros de titularidad privada, y han causado diversos asientos en el registro. Todo ello lo ha expuesto el señor Fernández a lo largo de esta densa comparecencia y no voy a reproducir aquí sus palabras. En cualquier caso, sí que quiero subrayar que ese incremento de actividad del Registro General de la Agencia de Protección de Datos es sintomático de esa sensibilización social que es tan necesaria en orden a la garantía del derecho a la intimidad y a la aplicación de la ley. Y una reflexión similar probablemente podríamos hacer en relación al ejercicio de la función fiscalizadora por parte de la Agencia de Protección de Datos, que se ha traducido en la incoación de expedientes de investigación y, en su caso, cuando ha sido necesario, en el ejercicio de la potestad sancionadora, incluso **ex officio** a través de los llamados planes sectoriales de oficio, que dan lugar a la emanación de esas recomendaciones que pretenden una mayor adecuac
ión de los distintos segmentos de la realidad social al cumplimiento de la ley.

En el plano de la sensibilización social, la Agencia ha realizado una nada desdeñable labor de formación y de información. El señor Fernández ha hecho referencia a ello a lo largo de su exposición; me estoy refiriendo a las jornadas organizadas, a las campañas publicitarias o, sin ir más lejos, a la labor desempeñada por la llamada área de atención al ciudadano, con la resolución de consultas telefónicas, escritas o incluso con la propia visita de la página web de la Agencia de Protección de Datos. Es decir, una actuación preventiva, informativa; en definitiva, de difusión de la ley, que tiene su amparo en el artículo 36 de la Ley Orgánica 5/1992, que contribuye decisivamente en esa labor de información y en el cumplimiento de ese mandato legal de suministrar información al ciudadano en orden a sus derechos en materia del tratamiento automatizado de datos de carácter personal. Ésta es una vía, señor Fernández, en la cual se tiene que profundizar en el futuro, con la perspectiva de la aplicación de la nueva Ley 15/1999 y, sin perjuicio del ejercicio de la potestad sancionadora cuando proceda, creemos positivo, necesario y razonable incrementar la función informativa de la nueva ley en relación a los distintos sectores económicos y sociales, función informativa que corresponde a la Agencia de Protección de Datos en aras a facilitar en el mayor grado el cumplimiento voluntario de la ley.

Por tanto, señorías, señor Fernández, la conclusión del Grupo Popular es que la sociedad española es cada vez más permeable a la aplicación de esa ley y que hay un nivel positivo de sensibilización social en ese sentido. El balance de la gestión de la Agencia de Protección de Datos en este ejercicio de 1999 en términos de aplicación de la ley y difusión de sus prescripciones normativas, a nuestro juicio, arroja un saldo positivo, como ha expuesto a lo largo de su comparecencia el señor Fernández; un saldo positivo, tanto en lo que es la actuación respecto a ficheros de titularidad privada como de titularidad pública. Yo subrayaría de modo particular las actuaciones en relación a la Agencia Estatal de Administración Tributaria, que, por su propia naturaleza, por su objeto, por las funciones que tiene legalmente encomendadas maneja un gran número de información sensible y, por lo que se desprende de la memoria, parece que no hay incumplimientos en ese sentido, sino, en términos generales, una situación bastante razonable en cuanto a la

protección de derechos fundamentales. No hay que olvidar que a la mejora de la situación probablemente hayan contribuido también las mejoras normativas introducidas en la Ley General Tributaria a raíz de la Ley 15/1999, de Protección de Datos. En definitiva, y con ello concluyo, mi grupo valora positivamente esta memoria del año 1999 y, una vez más, quiere ofrecer al director y a la Agencia de Protección de Datos su colaboración en el plano político y legislativo, en la mejora de esa tutela al derecho a la intimidad personal y familiar, de ese llamado derecho de autodeterminación informativa.

La señora **PRESIDENT**

A: Para contestar a las diversas cuestiones planteadas, tiene la palabra el director de la Agencia de Protección de Datos.

El señor **DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS**

(Fernández López): Voy a tratar de responder, con mucho gusto, a las cuestiones planteadas, pero si me dejo algo en el tintero, les ruego que insistan, dado el importante número de preguntas, cosa que me satisface, ya que demuestra el interés de SS.SS. por las funciones que desarrolla la Agencia.

En primer lugar, me referiré a las cuestiones planteadas por la señora Del Campo. Evidentemente, yo soy el primero en desear que los tiempos se acorten, pero, sinceramente, ¨cree usted que habiéndose aumentado un 50 por 100 esto referido al año 1999, hablamos de un 400 por 100 en el año 2000 pasar de 3 a 7 días es mucho? Porque no se puede olvidar, como también he puesto de manifiesto, que no son inscripciones de ficheros sencillos, sino que son ficheros que hay que analizar, como ocurre en los casos en que señalan transferencias internacionales, y ello, indudablemente, conlleva una mayor dedicación antes de aprobar la inscripción de ese fichero, aunque ésta sea meramente declarativa; de entrada, la Agencia debe velar, debe actuar de oficio para que no se escape nada, sobre todo en las transferencias internacionales; debe velar por si pudiera resultar peligroso para los intereses de los ciudadanos simplemente el que algún fichero exista. Yo, por supuesto, tomo nota y trataremos de ser lo más rápidos posible en nuestras respuestas, pero creo que estamos en una situación óptima, sobre todo si se compara con cualquier otro organismo. También se ha referido la señora Del Campo a los ficheros de titularidad pública, sobre todo a los ficheros relativos a los ayuntamientos, y manifiesta que aún hay pocos inscritos. Nosotros, dentro de los medios que tenemos, estamos haciendo un constante recordatorio a los titulares de los ficheros, pero, además, en el pasado ejercicio, a través del consejo consultivo al director le asisten el consejo consultivo donde están representados los distintos estamentos sociales, entre ellos la Federación Española de Municipios y Provincias le hice notar al representante de dicha Federación de Municipios y Provincias esta carencia y quedó en posibilitar por este cauce un mejor conocimiento y cumplimiento de la ley.

La realidad es que aún no he recibido ninguna ayuda al respecto. No obstante, como también he expuesto, la Agencia trata de estar presente en todos los foros, no sólo en los que organiza ella, sino en los que organizan otros, tanto universidades como asociaciones de consumidores, como administraciones públicas, etcétera. Personalmente, he estado en 30 en un año, además de todo el trabajo, y le puedo asegurar que es bastante difícil ir a más. Por otro lado, aunque en la Agencia hay funcionarios con conocimientos muy superiores a los míos, cuando la gente llama quiere al director y el buscar sustituciones siempre resulta difícil, ya que, si se delega en alguien, se creen peor tratados. No obstante, ya he dicho que éste es uno de los medios que utilizamos para difundir la ley y para ayudar a su cumplimiento y, además, en todo el territorio nacional, porque yo soy consciente de que mi presencia debe ser constante no sólo en Madrid y Barcelona, que tal vez son las ciudades que más actos organizan a este respecto, sino en el resto del territorio nacional y, por supuesto, que debo visitar todas las comunidades autónomas.

Entre estas jornadas, ha habido algunas referidas a administraciones públicas, pero ocurre que no hemos podido hacer una serie que se puedan ir repitiendo por todas las comunidades.

Dentro del volumen de la Agencia, tanto presupuestario como de personal, trabajamos al límite, hacemos todo lo que podemos, pero, como todo, resulta mejorable. En cuanto a los ficheros autonómicos, a los planes sectoriales, referido a que echaba de menos las recomendaciones. Las recomendaciones están aquí y están a su disposición, como se dice en la memoria. Todas están publicadas y enviadas a los responsables. Si le parece bien a S.S., haré llegar a la presidenta de la Mesa una copia de todas y cada una de las recomendaciones, pero si tiene interés por alguna en especial, con mucho gusto se la podré aclarar en este mismo acto. En cuanto a las transferencias internacionales, efectivamente hemos sido el primer país de la Unión Europea que ha hecho uso de la posibilidad que da la directiva de la solución contractual, pero con auténticas garantías para posibilitar la transmisión de datos a terceros países que no tienen igual nivel de protección que los europeos.

El **Reader's Digest** fue el primero que se inscribió y se comunicó a la Unión Europea y el que está sirviendo de modelo para el subgrupo de trabajo que se está ocupando de establecer unas cláusulas contractuales que sean acordes para todo. Ya le adelanto que el nivel de protección que nosotros estamos otorgando se va a rebajar a nivel comunitario porque, no nos podemos engañar, no sólo en el régimen sancionador sino, de modo general, el carácter tuitivo de nuestra ley es muy superior al de la mayoría de los países de la Unión Europea. No obstante, seguimos insistiendo en la necesidad y validez de esas cláusulas. Por supuesto, en las transferencias que hemos realizado este año se han aplicado exactamente las mismas cláusulas y con el mismo rigor.

Por otro lado, y bueno es decirlo, no hemos encontrado inconveniente alguno por parte de los responsables de los ficheros a la hora de rechazarlas, porque, si SS.SS. las analizan, todas son absolutamente lógicas dentro de un ámbito de protección de la intimidad verdaderamente se quiere proteger; ahora bien, si no se quiere proteger es evidente que todas o la mayoría sobran. También ha hecho referencia S.S. a los comentarios que he realizado sobre las infracciones

en las administraciones públicas, y echaba en falta el expediente de la Consellería de Seguridad Social de la Generalitat Valenciana. Como ya he hecho constar en mi informe, sólo me he referido a aquellos expedientes que no he tratado en anteriores comparecencias, y precisamente en mi anterior comparecencia ese tema se debatió por SS.SS., y además se debatió en aspectos ajenos absolutamente a la protección de datos. No obstante, no tengo inconveniente en volver a referirme al mismo. La denuncia fue muy tardía y cuando la Agencia atendió la denuncia y realizó la inspección no había posibilidad alguna de obtener ninguna prueba de infracción; exclusivamente se obtuvo ésta por la propia declaración del viceconsejero, que reconoció que habían sido tomados datos ajenos a los que figuraban en la propia Consellería, y de ahí que se pudiera llegar a sancionar. En cuanto a la situación fluctuante que S.S. observa en los planes sectoriales, creo que responde a un objetivo por mí trazado desde el momento en que tomé posesión del cargo de director de la Agencia con independencia de atender puntualmente las denuncias de los ciudadanos y realizar como consecuencia de ello las inspecciones pertinentes, el de realizar planes sectoriales en aquellos sectores donde más volumen de datos existiera o a los que más afectara el número de denuncias o a los que pudiéramos considerar como sectores emergentes, como es el caso de las telecomunicaciones, que necesitaban de un reglaje y adecuación.

Ése es el criterio que hemos seguido en estos planes sectoriales que, como le decía, en cualquier caso han dado con las adecuadas sugerencias para que puedan adaptarse mejor a la ley.

Por supuesto en los casos en que hemos detectado alguna infracción grave, como ha sucedido en materia de telecomunicaciones y antes me referí a ello, con independencia de que se produzca este tipo de recomendaciones para el buen hacer futuro, se ha abierto el correspondiente procedimiento sancionador, y no sólo eso sino que se han adoptado medidas cautelares para que un tratamiento masivo, que afecta a millones de datos de millones de ciudadanos, cesara de forma inmediata. Evidentemente, comparto su sensibilidad respecto a que hemos aumentado la plantilla. Cuando yo me hice cargo de la Agencia había 49 funcionarios y ahora somos 62, pero la nueva ley y las nuevas exigencias de la ley están ya demostrando la necesidad de este aumento, y así lo tenemos previsto para el próximo ejercicio; hemos pedido el aumento correspondiente en la partida presupuestaria para atender este incremento de plantilla, que yo juzgo en estos momentos necesario, y que en los diversos niveles debe circunscribirse al menos a 30 nuevos funcionarios. Porque, señorías, no sólo tenemos que pensar en el hoy inmediato, que ya vemos el crecimiento que se está produciendo, sino en el hoy próximo, porque se nos viene encima el control de todos los ficheros no sólo informatizados sino también los no informatizados.

Hay obligación de inscribirlos a partir de 2007, pero ya los pueden inscribir los responsables de los mismos, y en algunos casos ya lo están haciendo, con independencia de que, como saben, la nueva ley habilita a los ciudadanos, aunque estos ficheros no estén bajo la tutela total de la ley, a ejercer sus derechos de acceso, rectificación y cancelación también respecto de los ficheros no informatizados. Esta es una realidad que ha de traducirse en un mayor volumen no sólo de inscripciones en el registro también de denuncias y de planes sectoriales que tengamos que establecer. En esta línea vamos, y antes les referí cómo ante la problemática que se deriva de los colegios profesionales que, por un lado, actúan con competencias de administración pública y en otros aspectos tienen ficheros de titularidad privada, y hay dificultad en saber cuándo son unos, cuándo otros y hasta donde está la obligación suscribimos este protocolo con la unión profesional, para que, a través de sus cauces, de los consejos generales de colegios y después de los distintos colegios, puedan llevar al conocimiento y mejor comprensión de la ley. Pero es que ya en el año 2000 hemos hecho lo propio con el Consejo General de Colegios Notariales, porque, por supuesto, los notarios también están obligados al conocimiento y cumplimiento de la ley, y lo hemos hecho también con el Consejo Superior de Cámaras de Comercio. A través de estas organizaciones empresariales habrá posibilidad de hacer llegar mejor a los empresarios el conocimiento y las necesidades de cumplimiento de la ley. También se ha referido S.S. a la atención al ciudadano. La atención al ciudadano, por supuesto que es un tema prioritario para la Agencia. Fijénse, señorías, tal vez todos tenemos la opinión de que a lo mejor la ley es bastante desconocida.

El año 1999 en una encuesta del CIS se incluyó alguna pregunta sobre el conocimiento de la legislación de protección de datos y de la Agencia, y aunque la cifra aún es pequeña para mí resultó satisfactorio que el 28 por 100 de los ciudadanos conocieran su existencia y estuvieran además contentos con su actuación. Indudablemente el aumento de las consultas que nos formulan más de 15.000 y los accesos a nuestra página web en internet que superan los 500.000 como antes referí están demostrando un mayor conocimiento de esta legislación. También me decía que la Agencia se conoce poco y que muchas de las denuncias pueden ir al Defensor del Pueblo cuando no es el órgano indicado para tramitar estas cuestiones. La realidad es que la relación que la Agencia, y personalmente su director, mantiene con el Defensor del Pueblo es cordial y fluida, tanto con el anterior como con el que estuvo en funciones, y con el actual. A todos ellos he visitado, con todos ellos he cambiado diversas opiniones y aspectos para mejor coordinarlo, y como SS. SS. saben en el supuesto de que haya infracción de administraciones públicas por imperativo legal debo de dar cuenta al Defensor del Pueblo de que éstas se han producido. Nuestra relación es afortunadamente muy fluida y, por supuesto, desde ambas instituciones tratamos de dar el mejor servicio posible al ciudadano. Le puedo garantizar que ninguna denuncia porque vaya el Defensor del Pueblo, si es que hay equivocación por parte del ciudadano, se va a quedar sin conocer por parte de la Agencia si es que resulta ser competente para ello. En cuanto a la nueva ley orgánica y sus dificultades, como todo lo nuevo tiene dificultades e indudablemente, como también ya me referí en la anterior comparecencia, una parte que no se tramita en fase pública hace que desconozcamos cómo se han ido gestando algunos artículos que resultan de especial dificultad, pero hay uno que a mí más me preocupa, y es concretamente la disposición adicional primera.

Me preocupa porque, señorías no sé en qué momento, porque el texto no era así se introduce un ®o no¯ que nos complica la vida.

Fijénse que la disposición adicional primera respecto a los ficheros preexistentes dice: Los ficheros y tratamientos

automatizados inscritos en el registro de protección de datos deberán adecuarse a la presente ley orgánica dentro del plazo de tres años a contar desde su entrada en vigor. Si esto se lee así, parece que el legislador está dando una **vacatio legis** de tres años cuando a mi modo de ver nunca estuvo en la intención del legislador producir esto, porque si leemos lo mismo y quitamos la expresión ®o no¯ dice: Los ficheros y tratamientos automatizados inscritos en el registro de protección de datos deberán adecuarse a la presente ley en el plazo de tres años a contar desde la entrada en vigor; es decir deberán adecuarse en aquello que haya diferencias entre la ley antigua y la ley nueva, pero no habrá una vacación de tres años. Este tema, verdaderamente me preocupa y me tiene con las manos atadas porque puede resultar que haya verdaderamente una vacación de tres años y a lo mejor estemos actuando para nada. Eso ha determinado que me dirija al Consejo de Estado como órgano consultivo supremo de la nación solicitando su dictamen sobre esta materia, porque aunque la Agencia tiene su interpretación clara y evidentemente no puede ser la que en principio literalmente pudiera derivarse, no sé al final quién será encar gado en última instancia de interpretar la ley y si podrá decir algo, con lo cual esto ha determinado, señora del Campo, que tampoco hayamos dictado instrucciones que tenemos en algunos casos preparadas para facilitar el cumplimiento y el conocimiento de la ley. Por otro lado, una actividad que me ha tenido seriamente ocupado y preocupado (no sé si no la he explicado bien y por eso a lo mejor no le han dado ustedes la misma importancia que le doy yo) ha sido toda la gestación del tema de puerto seguro para la transferencia libre de datos a los Estados Unidos de América. Éste es un tema a mi modo de ver, verdaderamente grave.

Ha habido unas presiones absolutas por parte del Gobierno americano para que los datos circularan libremente a los Estados Unidos (donde no hay protección de ningún tipo porque sólo hay leyes sectoriales y confusas) como si se tratara de la Unión Europea donde hay una ley de protección de datos y donde hay una autoridad de control y sólo en base a unos buenos principios que ni el Gobierno se decide a controlar.

Nosotros junto con Italia y Portugal (a principios también estaba Francia y luego se descolgó) éramos el núcleo duro en el grupo del artículo 29 contra esta situación, y en el mes de marzo me visitó el viceministro de Comercio de los Estados Unidos para conocer mi opinión al respecto y sobre todo para querer hacerme ver que si íbamos por este camino imposibilitaríamos que el comercio electrónico fuera una realidad en la Unión Europea. Ante esta actitud yo le dije que no estábamos hablando de comercio electrónico, que el comercio electrónico en primer lugar se da normalmente entre empresas en aproximadamente el 90 por 100, con lo cual ahí no había ninguna intimidad que proteger y en el caso del 10 por 100 restante de los ciudadanos cada uno tendría la opción de ceder o no ceder sus datos. Él me venía a hablar de cosa distinta del comercio de datos, porque los datos, señorías, sobre todo cuando se tienen en un volumen y depurados son importantes para que las empresas extranjeras puedan ofertar directamente productos a ciudadanos españoles. De aquí que a mí la libre circulación en estas circunstancias no me pareciera acorde, toda vez que al sistema contractual, que se podría incluso suavizar pero en los términos en que lo había propuesto la Agencia de Protección de Datos, por las grandes empresas no se había puesto ningún inconveniente.

No sé ese interés. El puerto seguro si quieren verlo ya publicado en el DOCE demuestra la negación absoluta del derecho del ciudadano español porque entre los principios que son etéreos, que no dicen nada, que no se comprometen a nada, y luego las FAQ, que lo único que hacen es complicarlo, tenemos un volumen de más de 100 páginas. Con eso se pretende proteger los derechos de los ciudadanos.

¨Qué se pretende además? Que el ciudadano no pueda ejercitar sus derechos desde el territorio español, sino que tenga además que acceder a Estados Unidos para poder ejercitar sus derechos con el coste económico que ello supone. Como comprenderán, señorías, es una situación verdaderamente preocupante y donde yo me he centrado precisamente para sacar una instrucción antes de que entre en vigor el puerto seguro para que en uso de la legalidad y toda vez que las autoridades tenemos el control sobre los datos, antes de salir del territorio español exijamos el cumplimiento de todos y cada uno de los principios de protección de datos. Será la única forma que en estos momentos tengamos para impedir que los datos, una vez fuera de nuestras fronteras, circulen con absoluta impunidad.

Esto me parecería muy poco serio porque, señorías, si no se remedia tendríamos que pedir la derogación de la directiva comunitaria y de la ley española, porque me parece absurdo que vayamos a tratar con más rigor a las empresas españolas o comunitarias y que en cambio Estados Unidos se convierta en el mercado de los datos personales. Estoy últimamente tratando de centrar la redacción de una instrucción que sin olvidar otras, pero por los motivos que le he explicado, no se han producido las que en principio debieran haberse llevado a cabo. Indudablemente el reglamento ha determinado que las empresas tengan que hacer un esfuerzo más, pero no un esfuerzo tanto económico, porque cuando estamos hablando de medidas de seguridad aquí parece que todo es técnico y que todo lo técnico en informática es caro y fundamentalmente en muchos casos son medidas organizativas; es decir que al ordenador no tenga acceso nada más que quien puede tener acceso, que se controle que los ordenadores quedan apagados, que al ordenador se accede por unos determinados empleados para unas cosas y por otros para otras, etcétera. Indudablemente los datos sensibles o especialmente protegidos como los de salud tendrán además que ir encriptados para evitar que pueda existir fuga de los mismos sobre datos que van más íntimamente dentro del propio derecho del ciudadano. Creo que en general he contestado a sus cuestiones; en cualquier caso quedo a su disposición. Paso seguidamente a responder al señor Erkoreka en cuanto a las instrucciones que hemos dictado.

Creo que podemos dar por reproducido lo que he dicho a la señora Del Campo porque estamos pendientes un poco de que se dilucide el tema de la aplicación de la entrada en vigor sin ningún tipo de **vacatio legis** de la ley para poder estructurar todo esto. En los planes sectoriales, como ya he dicho, se han dictado las correspondientes recomendaciones que por supuesto pondré a disposición de la Mesa para que se las hagan llegar a usted. En todos y cada uno se han dictado las recomendaciones y en cuanto a los problemas de aplicaciones en la ley, indudablemente los hemos encontrado principalmente con la adicional primera a que antes he hecho mención. Por lo que se refiere al reglamento de medidas de seguridad tengo que insistir en que se adecua perfectamente a las exigencias de la nueva ley, y tampoco ha habido problemas para su implantación toda vez que ha ido de forma gradual. Evidentemente nos ha

incrementado el trabajo en cuanto a número de consultas, puesto que no todos establecían una interpretación muy acorde con el mismo; pero también a través de la página web en Internet últimamente hemos hecho públicas las consultas más frecuentes para que también accediendo a ellas se pueda conocer el parecer de la Agencia y se les pueda ayudar en esta materia. En cuanto al problema que ha sugerido de pequeñas y medianas empresas por la poca actividad informativa de la Agencia, la verdad es que tratamos de dar la máxima difusión a la ley y además últimamente los medios de comunicación se han hecho eco de las actuaciones de la Agencia, y tanto en la prensa de ámbito nacional como local todos los días hay alguna noticia de la Agencia de Protección de Datos, con independencia de que también otros medios de comunicación social se hayan hecho eco de las cuestiones que los ciudadanos suscitan a la Agencia.

En todo caso, cualquier sugerencia de SS.SS. para poder incrementar nuestra presencia de cara a los ciudadanos será bien recibida. Cualquier cosa que usted desee, por supuesto estoy a su disposición para aclararla o ampliarla. Respecto a las palabras del señor Jané, tenemos como usted dice un régimen sancionador que es el más alto de Europa. La dificultad cuando se tiene un régimen sancionador alto es pasar al bajo, porque si bien para algunas empresas sobre todo pequeñas y medianas empresas puede resultar muy mal una multa de la Agencia, algunas grandes empresas llegarían a solicitar que les cobráramos varias sanciones y les dejáramos en paz porque aquello les resulta excesivamente barato. Es difícil establecer el límite. De ahí que yo ya hiciera una sugerencia en esta Comisión que fue recogida por el Grupo Parlamentario Popular y por el Grupo Parlamentario Vasco (PNV) y se incluyera una previsión en el artículo 45.5 de la nueva ley que posibilita al director de la Agencia para que atendiendo circunstancias especiales de menor culpabilidad o apreciación de una menor intencionabilidad, se pudiera reducir la sanción en un grado; es decir una falta muy grave sancionarse como grave, y una falta grave sancionarse como leve. Creo que es una previsión acertada, para estos temas que usted ha suscitado nos va a ser útil, y por supuesto ya estoy aplicándola en aquellos casos que concurren las circunstancias que rigurosamente en este aspecto ha establecido el legislador.

En cuanto a las sentencias que parece ser no revocan muchas, lo primero que hay que decir es que esas son las primeras sentencias, con lo cual son las primeras resoluciones de la Agencia, y tanto las primeras de unos como de otros tampoco se puede pedir que sean muy afinadas. Por supuesto, lo mejor será el día en que de 100 resoluciones todas sean confirmadas. También hay que tener en cuenta otra cuestión que por el distinto ámbito competencial jurisdiccional se observa, y puede usted ver en la memoria que una misma conducta que se ha sancionado de una misma forma por la Agencia, por una sala del Tribunal Superior de Justicia se considera que no existe infracción, y por otra en cambio se considera que sí existe, con lo cual esto también tendrá un mejor remedio toda vez que ahora tendremos una unificación de doctrina al conocer de los recursos contra las resoluciones del director de la Agencia la Audiencia Nacional. Por lo menos tendremos un criterio más unificador. En este sentido, yo creo que sí se ha notado en las últimas sentencias. Por supuesto, soy consciente y me preocupa si las resoluciones se confirman o no. Le advierto que en alguna ocasión en la que no había cuantía suficiente para recurrir al Tribunal Supremo estuve tentado de solicitar que se recurriera en interés de ley, lo que ocurre es que como iba a pasar inmediatamente la competencia a la sala de la Audiencia Nacional vi que era un esfuerzo tal vez desproporcionado y extemporáneo en ese momento y por eso no lo hice. Desde luego, si se mantuvieran estas discrepancias con el tribunal que ahora puede unificar la doctrina, indudablemente habría que hacerlo. Comparto su interés y preocupación por la disfunción entre la Ley de régimen general electoral y la Ley del comercio minorista que parecía posibilitar al menos que los empresarios dedicados al marketing obtuvieran los datos de los ciudadanos del censo electoral.

Esto no ha podido ser así. Sé que no todos están de acuerdo conmigo, pero sinceramente creo que el censo promocional es una buena solución; es una buena solución porque el censo promocional va a posibilitar que estén en él aquellos ciudadanos que lo deseen, aquellos que no lo deseen puedan no estar, y sólo a los que estén se les envíe publicidad, existiendo además la posibilidad de poder estar un año y darse de baja al año siguiente y no recibir esa publicidad. Efectivamente, como usted ha dicho, corresponde al INE el desarrollo del mismo. Como SS.SS. saben ha cambiado también la presidencia del INE, pero ya en el mes de julio me puse al habla con la nueva presidenta y le hice ver la necesidad de que esto se ponga en marcha, poniéndome a su disposición para que la Agencia pueda el censo promocional se establezca dentro de la legalidad de protección de la intimidad. Por otro lado, también mantengo reuniones con el colectivo del marketing, que me preguntan sobre el tema y les he aconsejado que se dirijan al INE, con independencia de que por supuesto nos tienen a su disposición para mejorar en lo que sea posible esta puesta en marcha. En cuanto a la sensibilidad y a no sancionar lo que resulta sancionable, yo creo que va a ser difícil porque la ley, como usted sabe, está para cumplirla.

Lo único que sí se podrá tener en cuenta es la previsión del artículo 45.5 dependiendo de las circunstancias, porque tampoco nos podemos olvidar que existen algunas empresas que han sido reiterativas en la comisión de este tipo de infracciones y pese a ser sancionadas han continuado sin borrar datos del censo electoral cuando ya por resoluciones que habían sido confirmadas por los tribunales sabían que no podían hacerlo. De todas formas, como S.S. conoce, soy sensible al problema y trataremos de que cuanto antes se regularice el censo promocional y que ello se produzca dentro del marco normativo adecuado para que se posibiliten ambos derechos, el de la intimidad de los ciudadanos y el ejercicio de un libre y lícito comercio por los empresarios, que es nuestro deseo. Finalmente, quiero agradecer las palabras del señor De Juan, compartiendo su opinión de que estamos dispuestos, dentro de nuestras posibilidades, a incrementar la función informativa de la Agencia; pero no podemos olvidar que son 62 funcionarios, que son 24 horas al día y 365 días al año. Tenemos los expedientes, tenemos el trabajo internacional y por supuesto es una preocupación pero hacemos lo que podemos; incrementaremos más nuestros esfuerzos, si ello resulta posible, para que se dé a conocer una ley nueva. Ésa ha sido mi función fundamental todas estas jornadas, seminarios y cursos a los que he asistido durante el pasado año. Antes de que la ley entrara en vigor procedía darla a conocer y sobre todo dará a conocer principales novedades que la misma incluía.

La señora **PRESIDENTA:**

¨Algún grupo y muy brevemente dado lo avanzado de la hora, quiere realizar alguna puntualización a la intervención segunda?

(Pausa.)

PROTECCIÓN DE LA INTIMIDAD PERSONAL Y FAMILIAR EN RELACIÓN CON INTERNET. A SOLICITUD DEL GRUPO PARLAMENTARIO SOCIALISTA. (Número de expediente 212/000080)

La señora **PRESIDENTA:**

Pasamos a la comparecencia relativa a la información del director de la Agencia de Protección de Datos sobre la protección de la intimidad personal y familiar en relación con Internet.

El señor Fernández López tiene la palabra.

(El señor López Garrido pide la palabra.)

Señor López Garrido.

El señor **LÓPEZ GARRIDO:**

No sé si estoy en lo cierto, pero tengo la sensación de que cuando se trata de una comparecencia pedida por un grupo, si no ha sido pedida simultáneamente por el compareciente tiene la palabra en primer lugar el grupo que pide la comparecencia.

La señora **PRESIDENTA:**

La praxis a que yo he asistido en distintas comisiones es que el compareciente tiene la palabra, pero si quiere hacer uso de ella en primer lugar el Grupo Parlamentario Socialista, y por tanto el señor López Garrido, por parte de la Mesa no existe inconveniente.

El señor **LÓPEZ GARRIDO:**

Muchas gracias, señora presidenta, y entre otras cosas para hacer conocer al compareciente el sentido de la petición de comparecencia, que no conoce en su integridad. Ante todo me sumo a la bienvenida a esta Comisión del señor Fernández López, director de la Agencia de Protección de Datos, agradeciéndole su presencia, como han hecho los portavoces de otros grupos y de nuestro propio grupo parlamentario. El sentido de la petición de comparecencia en relación con Internet y en lo que afecta a los derechos fundamentales y a las funciones de la Agencia de Protección de Datos tiene un punto de partida y es que en estos momentos Internet tiene casi 250 millones de usuarios; usuarios que utilizan Internet para informarse, para divertirse, para comunicarse o para desarrollar actividades económicas. Lo cierto es que esto crece a un ritmo enorme, un 15 por 100 anual de crecimiento del uso de Internet. Además, tiene sentido porque ha habido sucesivos hechos haré alusión a algunos de ellos en nuestro país y fuera de nuestro país que ponen de manifiesto la importancia de Internet en relación con la problemática general de la protección de datos personales y tiene sentido que nosotros, en esta comparecencia del director de la Agencia de Protección de Datos, queramos dedicar una específica atención a Internet. Cuando se hicieron las primeras leyes de protección de datos en relación con la informática no existía el fenómeno de Internet y en estos momentos por supuesto Internet ha revolucionado ese mundo, aparte de haber revolucionado incluso la vida diaria. Nuestro objetivo con esta comparecencia era solicitar su opinión, su información y su explicación sobre medidas que se pueden adoptar en relación con Internet, específicamente sobre lo que consideramos dos aspectos esenciales que interesan especialmente en esta Comisión como es el tema de los derechos fundamentales y el tema de la seguridad en Internet.

Son conocidos algunos hechos que a veces tienen incluso el aspecto de anécdota, pero que es la punta del iceberg. En Estados Unidos que es donde estas cosas se conocen primero, ha habido múltiples ataques de lo que ya se ha denominado, con una terminología inevitablemente anglosajona, los **hacker**s, que han realizado acciones realmente sorprendentes y muy dañinas en ocasiones.

Han entrado en la web de importantes instituciones y por supuesto en la web de Bush y de Al Gore, los candidatos a la Presidencia de los Estados Unidos en estos momentos, intentando poner en ridículo las medidas de seguridad de estas web. Es conocido que, en España, los **hackers** entraron en la web de La Moncloa y que, durante un cierto tiempo, concitaron la atención por las cosas que hacían en esa web. También es conocido que, hace poco, los **hackers** entraron en la web del Real Madrid logrando poner al lado del escudo del Real Madrid el escudo del Barcelona, al grito de: Somos más vulnerables en la red que la defensa del equipo.

Esta frase de que era más vulnerable el Real Madrid en la red que la defensa del equipo, que lo era mucho en ese momento, pone de manifiesto el sentido de fondo de la inseguridad de la red. Aparte de estos datos, que hasta pueden ser anecdótico lúdicos, no se puede ocultar que la falta de seguridad y los ataques de los **hackers** producen unas pérdidas anuales de 1.600 millones de dólares, que van en aumento, y que ha habido violaciones de sistemas informáticos enteros, robos de tarjetas de crédito para múltiples usos, robos de información, bloqueos de empresas importantísimas de la red vinculadas a Internet, empresas vinculadas a la llamada nueva economía, e incluso se ha llegado a

hablar de ciberealismo. El presidente Clinton convocó una reunión deprisa y corriendo para tratar este asunto. Es conocido que el grupo de delitos informáticos de la Guardia Civil considera que la posibilidad de un ataque de ciberterroristas en nuestro país no es muy lejana y habla de que las nuevas tecnologías posibilitan la comunicación entre grupos terroristas. Incluso, el jefe de seguridad informática del Cesid manifestó que los equipos de nuestro país son, en su mayoría, muy vulnerables; vulnerables para todo y vulnerables también para el derecho a la intimidad y otros derechos fundamentales.

En relación con la intimidad concretamente, recientemente se conoció la filtración a la red antes, estas cosas se filtraban a los periódicos; ahora, se ponen inmediatamente en al red, que es la forma de hacer más daño si se quiere hacer de los datos personales de 1.700 concursantes de un muy conocido concurso, **Gran Herman**o, que se situaron en la red por el robo de esos datos personales por un **hacke**r, según la empresa productora. Lo cierto es que la afectación a la intimidad es absolutamente posible, más aún en la era de Internet. El año pasado salió un artículo en la **Minneapolis Star Tribun**e, una revista estadounidense. Escogieron una persona al azar y los redactores de esa revista, a partir de las informaciones que surgían de grupos de discusión, los famosos **chats** donde participaba esa persona, lograron conseguir la dirección y el número de teléfono de esa persona, el lugar de nacimiento, el lugar donde había estudiado, su profesión, lugar actual de trabajo, interés por el teatro amateur, su cerveza preferida, los restaurantes y destinos de vacaciones favoritos, incluso su opinión sobre temas tales como Bill Gates o el Estado de Indiana, al que considera especialmente represivo. Es decir, se podía saber prácticamente todo a través de la entrada en la red porque Internet, como es sabido, genera muchos datos personales. Usted ha hecho una cita ahora mismo en contestación a preguntas de alguno de los portavoces que ha intervenido antes.

Este medio es muy interactivo, no es como la televisión, es un medio que deja muchas trazas personales. También como el comercio electrónico, en auge, utiliza mucho los datos personales, requiere datos personales a veces innecesariamente. Hay empresas en la red que, para cualquier cosa, te piden el dato personal, cuando es absolutamente innecesario, para luego comerciar con él. Incluso, es conocido un invento informático, las famosas **coockie**s, que no se sabe cómo traducir al castellano; es una palabra que no ha podido traducir ni el Consejo de Europa pues utiliza la expresión **coockies** en su recomendación al respecto.

Es una fórmula para, en todo momento, poder atraer, conocer, los datos personales de una persona, dónde ha estado antes, qué webs ha visitado, etcétera. Todo esto pone de manifiesto que, con Internet, está cambiando absolutamente la dimensión de la protección, del objeto a proteger o de quién defenderse. En estos momentos, probablemente porque en la nueva economía tiene un gran protagonismo la empresa privada, las empresas privadas tienen un papel muy creciente en el manejo de los datos personales. Hace años, nos preocupaba más lo que hacía el sector público, pero ahora lo importante sobre todo es lo que hacen las grandes empresas privadas, que intervienen enormemente en actividades en Internet, lo cual afecta a la seguridad o a la intimidad. Y ello con una gran contradicción porque, por un lado, esas empresas privadas necesitan unos datos personales determinados para los pagos electrónicos, aunque seguridad, pero al mismo tiempo todo eso provoca que se meta en la red una enorme cantidad de datos personales y que las empresas cada vez manejen más datos personales. Esos datos personales se convierten, como usted ha dicho hace un momento, en un apetitoso bocado de comercialización. Es una retroalimentación porque los datos personales se convierten probablemente en uno de los más potentes comercios, lo que da más rédito a las empresas en la red, que a su vez los revenden para múltiples objetivos, comerciales o no comerciales.

Junto a este creciente papel de las empresas privadas en el campo de Internet, que afecta a la seguridad y a la intimidad, no hay un paralelo sistema jurídico de responsabilidad de esas empresas. La responsabilidad que tienen esas empresas sobre la filtración posible de esos datos no ha crecido a la misma velocidad que el papel fáctico de esas empresas en el manejo de datos personales. Incluso, se discute sobre quién es el responsable de una filtración de datos personales o de delitos informáticos, como pornografía infantil.

¨Es el responsable el que lo envía, el que lo pone en la web, que a veces no se sabe quién es? ¨Es responsable el servidor o el proveedor de servicios que no investiga adecuadamente las cosas que está permitiendo que aparezcan en la red? ¨Se le puede exigir a un proveedor que investigue todo aquello que pasa por sus instalaciones informáticas? A nosotros nos preocupa sobre todo la reacción de los poderes públicos, la reacción política, ante esta situación. Nos preocupa porque, aunque hay un cierto consenso en que lo ilegal fuera de la red tiene que ser ilegal también en la red y en principios básicos como la libertad de circulación o la libertad de expresión y la intimidad, lo cierto es que la evolución de la reacción política ante este fenómeno ha sido lógica teniendo en cuenta los avances tecnológicos, pero también preocupante porque de un control a priori, que por ejemplo en España era el centro del mecanismo de las primeras leyes de protección de datos, se ha ido pasando cada vez más a un control a posteriori, es decir, a una posición mucho más flexible desde el punto de vista de la política. Lo ponen de manifiesto modificaciones que ya hemos visto en la propia Directiva europea 45/96 ó el hecho de que, en la memoria que usted nos ha presentado esta mañana, aparezcan resoluciones del Consejo de Europa, por ejemplo la Resolución 99/5, o del grupo de trabajo del artículo 29 en la memoria están dos o tres de ellas, un documento de trabajo y dos recomendaciones, la 1/99 y la 3/99, pero todas son recomendaciones, lo cual no parece una casualidad. Es decir, ya no son normas coactivas, vinculantes, son recomendaciones, por tanto no vinculantes y muchísimo más flexibles; se recomienda ser justos y benéficos a las personas que están en Internet, a los proveedores, son meras recomendaciones.

Es decir, da la sensación de impotencia de los poderes públicos para poder regular esta cuestión mediante normas coactivas con las carácterísticas de una intervención pública adecuada. Parece que se va imponiendo un poco la filosofía americana de decir que para combatir esto no hay posibilidad ninguna de establecer normas. Hay que ir simplemente a códigos de conducta, códigos deontológicos, la contractualidad privada y otras técnicas, pero desde luego siempre en un sentido muy **ligh**t, en un sentido muy flexible, que abandona lo anterior. Todo esto es para explicarle por

qué hemos pedido que usted nos informe sobre esta cuestión. Sobre todo, con este preámbulo querríamos que nos contestara a las tres cosas. Primero, nos gustaría saber cuáles son las acciones que piensa desarrollar al respecto la Agencia de Protección de Datos.

Desearía que profundizase algo más en una instrucción que, al parecer, están preparando al respecto. Es decir, ante la problemática de Internet y los efectos en los temas de la seguridad y de la intimidad y en otros derechos fundamentales, querríamos saber qué es lo que piensa hacer la Agencia de Protección de Datos, cuál es su política futura al res pecto y cuáles son las medidas que considera que debe adoptar. En segundo lugar, nos gustaría saber su opinión sobre la reacción política que ha habido hasta ahora a este respecto, esencialmente sobre la defensa de los derechos fundamentales, la seguridad, las actividades delictivas a través de Internet y los efectos que también me parece muy importante que puede tener esto en la actividad de la Hacienda pública que, por una parte, necesita cierta transparencia y, por otra parte, también estamos frente una contradicción ante determinados derechos de intimidad.

¨Usted considera que lo que se ha hecho hasta ahora, que la regulación que hay, que las iniciativas en el campo internacional y nacional son suficientes o habría que ir mucho más allá? En tercer lugar, y ya de forma mucho más concreta, también nos gustaría saber qué se puede hacer en relación con las normas de seguridad exigibles a las empresas que trabajan en Internet, y si la violación de esas normas de seguridad, con esos efectos tan dañinos, debería llevar aparejado algún tipo de sanción más fuerte que la mera multa. Porque aquí se ha hablado antes por el portavoz del Grupo de Convergéncia i Unió de que puede haber multas excesivas, pero la verdad es que en la práactica a esas multas para algunas empresas son de risa, es decir, es una mera cuestión de cuenta de resultados. Ganan mucho más con las infracciones que con las multas que les pueden imponer, que yo creo que ya está como se dice en la jerga financiera bolsística descontado por los mercados. Quizá una sanción mucho más adecuada podría ser la de prohibir a esas empresas trabajar en Internet. Si esas empresas violan las normas de seguridad o violan los derechos fundamentales, aprovechando las facilidades que para ello les da Internet, no se les deberían permitir ejercer su actividad comercial en Internet, ya sea de venta o de compra, etcétera. En definitiva, con esta petición de comparecencia lo que queríamos saber era la opinión de la Agencia de Protección de Datos sobre esas dos asignaturas pendientes que tiene Internet, que son la seguridad y la intimidad.

La señora **PRESIDENT**

A: Tiene la palabra el director de la Agencia de Protección de Datos.

El señor **DIRECTOR DE LA AGENCIA DE**

PROTECCIÓN DE DATOS

(Fernández López): Tengo que comenzar por decir que comparto las inquietudes del señor López Garrido, ya que no en vano se ha dicho muchas veces que tratar de regular Internet es como poner barreras al campo porque estamos en un mundo globalizado. Comienzo por contestar su última pregunta sobre si tenemos que prohibir el trabajar en Internet a una empresa que viole el derecho a la intimidad. Bueno, ¨y de qué sirve? Se va a un país donde no hay control y se puede acceder igual. En el mundo glo balizado en el que vivimos es difícil, por un lado, regular Internet y, por otro, es una herramienta útil, está ahí, es algo ya imprescindible, está ya en la propia cultura del siglo que comenzará el año que viene. También tenemos que analizar cuáles son los deseos o cuáles son los comportamientos de los ciudadanos al respecto. Fíjese que en una encuesta reciente sobre internautas europeos se llega a la conclusión de que los más preocupados por su intimidad son los internautas holandeses y los menos preocupados de todos son los internautas españoles. Esta es una realidad que está ahí y me hace reflexionar que si vamos a una regulación muy rigurosa podríamos estar en contracorriente de lo que nos piden nuestros propios ciudadanos. En cualquier caso, lo que sí que hay que permitir es que aquel ciudadano que desee guardar su intimidad, también lo pueda hacer en el llamado mundo de Internet. No tiene por qué ser distinto el mundo de Internet del conocido mundo convencional. De ahí que ya las autoridades de control de la Unión Europea, reunidas, como usted bien ha dicho, por imperativo del artículo 29, hayamos declarado que tanto la Directiva 95/46 como la 97/66, es decir, la de protección de la intimidad en materia de las telecomunicaciones, son absolutamente aplicables también a los supuestos de Internet. Lo que ocurre es que hay dificultades en la aplicación.

Para ello, a mi modo de ver, lo primero que hay que hacer es informar, es decir que el ciudadano que accede a Internet sepa cuál es el medio que está manejando y cuáles son las posibilidades que ese medio le da y cuáles son las posibilidades que fuera del medio tiene para aplicar al mismo. De ahí que la Agencia de Protección de Datos ya en el año 1997 editara unas recomendaciones para usuarios de Internet que, en definitiva, les advierte de los peligros. Porque como usted ha señalado, a través de unas **cookies** se está en un **chat** o en un foro de opinión, con unas **cookies** que muchas veces son invisibles, pueden captar nuestros datos y esos datos no saben dónde van, etcétera. Ni qué decir tiene que si encima lo que estamos haciendo es una transacción comercial y damos nuestro número de tarjeta de crédito o de cuenta corriente sin que esos datos vayan cifrados o encriptados, verdaderamente estaremos ante una situación prácticamente suicida contra nuestra economía, porque el descalabro que podrá producirnos puede ser tremendo. Por tanto, lo primero que hay que hacer es informar. La Agencia ha estado presente en todos estos foros, como en el del artículo 29, que el año pasado, como usted bien ha dicho, produjo una recomendación y dos dictámenes que, en definitiva, vienen a recoger lo que ya decía la Agencia de Protección de Datos en el año 1997, y que para no cansarles no les voy a leer, aparte de que lo tienen en la memoria; igualmente, en el Consejo de Europa hay una importante recomendación. Pero como usted ha podido comprobar, estos son más bien buenos consejos, hay poco práctico, poco que sea obligatorio. Tampoco podemos olvidar que incluso en los foros europeos no todo en con nosotros el mismo interés por la protección de la intimidad. El grupo anglosajón y los que le siguen, como holandeses, etcétera, son mucho más abiertos a que Internet hay que usarlo y que si no ocurre una grave infracción de los datos, pues

que no pasa nada o casi nada.

Personalmente, no estoy de acuerdo. Creo que cada uno debe tener el derecho, dentro de su libertad, a usar o no sus datos personales según su propia apetencia. En este aspecto la Agencia, aparte, vuelvo a repetir, de las recomendaciones, ha tocado otros puntos para proteger a los ciudadanos y unos de ellos ha sido la promoción de códigos éticos para Internet. Nosotros hemos sido el primer país de la Unión Europea que hemos inscrito un código ético para la Asociación Española de Comercio Electrónico. En la confección de este código al que se ha adherido una cantidad importante de empresas de diversos sectores como el bancario, los medios de comunicación audiovisual y escrita, correos, establecimientos comerciales, edición y distribución de libros, informática, telecomunicaciones, marketing, consultoría, incluso asesoría jurídica y empresarial no sólo ha participado la propia Asociación Española de Comercio Electrónico, sino también las tres principales asociaciones de consumidores españolas y la asociación de autocontrol de la publicidad, estando, además, ellas presentes en un comité regulador que se establece. De lo que se trata es de que el derecho a que se informe a los afectados de que sus datos han sido recabados o capturados por los anunciantes debe encontrar su primera manifestación en la obligación que se impone de informar de ello en su página web mediante un aviso de que se está produciendo este tratamiento de datos. El consumidor en tal su parecer podrá oponerse total o parcialmente incluso al tratamiento de sus datos, exceptuando los casos en los que resulte necesario tener unos datos para la perfección de una relación contractual. El consumidor podrá, de igual forma, seleccionar o excluir finalidades para las que consiente que sean destinados sus datos. En el caso de terceros, además deberá informárseles sobre la identidad de los cesionarios y sobre la finalidad perseguida con la cesión.

Asimismo, este derecho de oposición se podrá realizar **on lin**e, es decir, en el momento en que se está realizando la comunicación. En las relaciones con terceros contratantes, las empresas involucradas en la cesión de datos para realizar ofertas por email deberán garantizar el cumplimiento de los principios de este código ético. También incluso se ocupa el código de la relación en el tratamiento de datos de menores ante la dificultad de conocer cuándo un menor facilita sus datos o si verdaderamente los está realizando el titular o titulares de la patria potestad. Por eso, en el código se avisa a éstos de la obligación que tienen de controlar a sus hijos, y con independencia de ello se comprometen las empresas en los temas dirigidos a los menores a que la publicidad sea adecuada con la Ley orgánica de protección al menor, donde ya, como SS.SS. saben, se les da a los menores una cierta posibilidad de decisión, pero con unos límites sobre todo en aspectos que no sean perjudiciales para su desarrollo integral. Y se concede preventivamente a los padres que puedan ejercitar los derechos de acceso, cancelación o rectificación de forma que, en el supuesto de que conecten los hijos, no se les envíe ningún tipo de publicidad ni se retengan sus datos. Es una de las fórmulas, en definitiva, para que a través de una marca identificar a todas estas empresas que se comprometen al código ético, quienes comercien en Internet puedan saber qué empresas o qué grupos de empresas están dispuestas a mantener su intimidad sin violación de ningún tipo. Pero es indudable que desgraciadamente se producen violaciones en Internet y les voy a resumir algunas a SS.SS. porque creo que pueden ser significativas de lo que ocurre y de los medios que tenemos para defendernos.

En un supuesto de publicidad no deseada a través de la dirección de un correo electrónico, el usuario de Internet recibe mensajes publicitarios los hechos vienen a ser estos en su dirección de correo electrónico remitidos de otras direcciones de correo electrónico de una empresa dedicada a esta actividad. El usuario solicitó información sobre la procedencia de su dirección de correo electrónico y pidió la baja en la lista de distribución, ejercitando su derecho de acceso y de cancelación. Inmediatamente volvió a recibir mensajes publicitarios a su dirección de correo electrónico.

Asimismo, recibió un mensaje amenazante personalizado con destino a la misma dirección de correo electrónico. Aquí la cuestión relevante consiste en determinar si la dirección de correo electrónico del usuario puede ser o no considerada como un dato personal. La Agencia, teniendo en cuenta (porque el correo electrónico puede estar explicitando el nombre y apellidos de una persona vinculado sólo a una enumeración, con lo cual queda identificada, o puede tener un nombre figurado, en cuyo caso no quedaría identificada) este supuesto, toda vez que se posibilitó vincular el correo electrónico a una persona, en concreto al enviar la nueva publicidad y la carta insultante, consideró que era un dato personal, que se había violadp y, y se impuso la correspondiente sanción. Otro tema de gran importancia es la obtención de datos a través de la página web de terceros países y la cesión posterior a filiales españolas. Aquí los usuarios de Internet residentes en España acceden a la página web de una importantísima empresa líder en el sector de software, ubicada en los Estados Unidos de Norteamérica, país que, como saben, no tiene nivel de protección equivalente. Los usuarios consultan la información contenida en la página web de la empresa norteamericana interesándose por nuevos productos y servicios que ofrece. Para ello registran sus datos personales, que se incorporan a la base de datos de dicha empresa. No obstante, y dicho lo anterior, hay que tener en cuenta que la empresa americana mantiene una política propia de protección de la privacidad que sólo puede ser conocida por el usuario si accede a otras páginas web, a las que hablan de privacidad, pero no a donde está consultando. Al no ser obligatorio este acceso a las páginas web de publicidad, si se accede a las otras directamente, la empresa americana entiende que se ha dado el consentimiento tácito.

Una vez incorporados los datos a los sistemas informáticos de la empresa, ésta permite a las filiales residentes en otros países, entre ellos España, que accedan a las bases de datos, transfieran telemáticamente e incorporen a sus propios ficheros informáticos, ubicados en este caso en España, los datos que han sido recabados y tratados en Estados Unidos.

En resumen, se obtienen datos a través de Internet en ficheros ubicados en un país sin nivel de protección adecuado y posteriormente son enviados a España. La Agencia de Protección de Datos inició un procedimiento sancionador que ha concluido con una result en la que señala la insistencia de infracción y se impone una multa de diez millones y una peseta a la filial española. Toda vez que el derecho territorial aplicable en la recogida de datos fuera el americano, puesto que se recaban en los Estados Unidos, al venir los datos aquí y ser tratados, en ese momento entra en aplica-

ción la legislación española y esos datos, que han sido recabados sin consentimiento del ciudadano evidentemente, conforme a nuestra ley, no pueden ser tratados, por lo que, aplicando la misma, impusimos la sanción. Los casos son múltiples. Recientemente hemos tenido otro importante de una asociación privada que presenta un informe anual en un servidor de otra asociación y que incluye ficheros identificativos de 300 personas aproximadamente, miembros de Cuerpos y Fuerzas de Seguridad del Estado, de funcionarios de prisiones y de políticos, que en algunos casos han sido denunciados por delitos de tortura, en otros casos condenados por sentencia firme o no y, en otros, absueltos, y mantiene ese fichero. Después de las correspondientes diligencias de inspección, la Agencia inició un procedimiento sancionador a la asociación responsable del fichero por entender que se estaban tratando datos sensibles y sin el consentimiento de los ciudadanos, y que además se estaban cediendo de una forma masiva, como supone Internet, a todos.

De ahí que se adoptaran medidas cautelares, que fueron atendidas, y al final se dictara una resolución. Se cuestionaba si la Agencia estaba interfiriendo el derecho a la libre información y libre expresión de la citada asociación. Esto no era así, porque la agencia en ningún caso cuestionó ni entró a valorar el informe de dicha asociación. Lo único que se sancionaba es que se mantuviera un fichero con datos sobre infracciones penales cuando el artículo de la ley vigente establece que sólo las administraciones públicas, no cualquier Administración pública sino aquellas que están en el ejercicio de sus respectivas competencias, pueden mantener ficheros con datos sobre infracciones penales o administrativas. Eso es lo que se cuestionó y eso es lo que se sancionó. Aquí se nos ha planteado, señorías, un grave problema, porque el fichero ha sido copiado por otros servidores que se encuentran fuera del territorio nacional. Concretamente, en el supuesto de Bélgica, de Suiza, de Suecia y de Nueva Zelanda me he dirigido todos tienen autoridad de control a las autoridades de control y he solicitado cooperación para que se proceda de igual forma al borrado de estos ficheros.

Estoy pendiente de las resoluciones. Sí puedo decirles que tanto el comisionado italiano como el sueco y el neozelandés, que me visitó el pasado mes de junio para recabar más datos, estaban interesados en realizar alguna función en este aspecto. Aún está sin terminar. Pero este es el problema que tenemos en Internet. Podemos sancionar en un sitio, pero los datos aparecen en otro, sin que podamos acreditar si esos datos han sido cedidos porque entonces se podría seguir sancionando o han sido cogidos por el otro y de qué forma. Ese es uno de los graves problemas que tiene Internet. De todas formas, nosotros seguimos en este aspecto, con las autoridades de control, insistiendo y esperamos ver qué resolución dan. Por lo que respecta al tema que se ha referido usted de Gran Hermano, como consecuencia, al parecer, de un **hacker** que pudo acceder a uno de los ficheros, estos se publicaron en Internet. La Agencia intervino inmediatamente, pero lo que se descubrió y se lo voy a contar muy sintéticamente, porque el procedimiento no está terminado es que había recogida de datos sin informar a las, que además esos datos de una empresa se cedían a otras, que esas otras enriquecían los datos y los enriquecían pasando test psicológicos, incluso se aportaba información sobre enfermedades psíquicas de algunos de los concursantes. En definitiva, por una cadena de seis o siete, todos tenían su fichero y todos tenían esos datos, sin el conocimiento, sin el consentimiento de los ciudadanos, ni tan siquiera para su tratamiento ni para cesión. De ahí que la Agencia haya abierto el correspondiente procedimiento sancionador.

Es un tema similar al de una asociación, al que antes me referí y que les sonará porque este verano tuvo un gran eco en los medios de comunicación, una asociación médica de defensa de pacientes, que pretende aperturar una página web con sentencias en las que se recojan las condenas a los médicos por mala praxis. Indudablemente, por los motivos que les he señalado antes, nuestra ley es terminante. Una asociación privada no podrá establecer este tipo de ficheros. A la asociación se le ha emitido un dictamen escrito, también a su petición. Hasta ahora no han hecho esta publicidad, pero se les ha advertido de la ilegalidad, porque se plantea luego la posibilidad de que esas sentencias se publicaran, en vez de con nombre y apellidos, con las iniciales. Y eso depende, porque la ley protege en los supuestos de que la persona se haya identificado o sea identificable. Si la sentencia dice, el médico don A. S., jefe de traumatología del Gregorio Marañón, no hace falta que diga el nombre para poder identificar a la persona.

En ese supuesto está claro que no pueden mantenerse estos ficheros porque en un Estado de derecho, donde hasta el mayor delincuente puede, pasado el tiempo y cumplida su condena, borrar sus antecedentes del registro de penados y rebeldes para poder reinsertar realmente, si permitiéramos este tipo de ficheros, estaríamos creando un problema de ilegalidad y de inseguridad tremendo. Los ficheros y las condenas sólo pueden establecerse por los jueces y no podemos los particulares establecer ficheros que los contengan. De ahí que, como SS.SS. conocen, las colecciones legislativas contengan las sentencias anónimas, para que todos podamos utilizarlas pero sin que se viole la intimidad de los ciudadanos. Nada más, muchas gracias.

La señora **PRESIDENTA**

A: Muchas gracias, señor director de la Agencia de Protección de Datos.

¨Señor López Garrido?

(Pausa.)

¨Algún grupo desea intervenir?

(Pausa.)

Por el Grupo Parlamentario Popular, el señor De Juan tiene la palabra.

El señor **DE JUAN I CASADEVAL**

L: Señora presidenta, dado lo avanzado de la hora, intervengo muy sucintamente para agradecer, en nombre del Grupo Parlamentario Popular, las aclaraciones del señor director de la Agencia de Protección de Datos y también para dejar patente la preocupación de nuestro grupo por la protección de la intimidad en el ámbito de Internet, por las propias características que tiene la red en términos de infraestructura basada en datos personales, en términos de instrumentos técnicos que le sirven de soporte y que evolucionan, de extensión del comercio electrónico, de difusión de información o de la propia dimensión global que tiene la red.

Entendemos que hay una dificultad intrínseca, consustancial, inherente a lo que es Internet en la protección de la intimidad, pero consideramos positivas y esclarecedoras las aclaraciones vertidas por el señor director de la agencia y en ese sentido consideramos que es necesario continuar avanzando en la protección del derecho a la intimidad en el ámbito de Internet, para lo cual yo reitero la colaboración de nuestro grupo en este tema.

La señora **PRESIDENT**

A: ¨El señor director de la Agencia de Protección de Datos quiere realizar alguna intervención? El señor

DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

(Fernández López): Nada más deseo agradecer a SS.SS. sobre todo la paciencia que han tenido en una sesión tan larga. Para mí ha sido de gran utilidad y por supuesto las sugerencias que SS.SS. me puedan hacer serán de gran utilidad, porque en definitiva están transmitiendo el sentir de los ciudadanos, cuyo derecho a la intimidad me corresponde especialmente proteger.

La señora **PRESIDENTA**

A: Con el agradecimiento de la Comisión al director de la Agencia de Protección de Datos por la comparecencia efectuada esta mañana, sin más, se levanta la sesión.

**Era la una y cuarenta minutos de la tarde.

**

MEMORIA DE 2000 - ANEXO VI - CÓDIGO TIPO FICHERO HISTÓRICO DE SEGUROS DEL AUTOMÓVIL

(Código Inscripción Registro Agencia Protección de Datos N§ 1982110017)

1. EXPOSICION DE MOTIVOS

Las entidades que operan en seguro del automóvil han trabajado durante estos últimos años en la elaboración de estadísticas sectoriales de siniestralidad, amparadas en el artículo 24.3 de la Ley 30/1995 de Ordenación y Supervisión de los Seguros Privados, que han permitido aplicar cada vez técnicas actuariales más depuradas para el conocimiento de los riesgos a asegurar, así como para que las entidades puedan, de forma individual, adecuar sus primas en función del riesgo asumido, dada la obligación establecida en la precitada Ley y en su Reglamento de desarrollo (Real Decreto 2486/98) relativa a la equidad y suficiencia de la prima de tarifa como garantía del equilibrio y solvencia de la entidad aseguradora.

Los avances en la técnica actuarial concebidos para personalizar la prima en función de cada riesgo asegurado y la aplicación de criterios tarifarios equitativos, tal y como se viene haciendo en todos los países de nuestro entorno, requiere dentro del ramo de automóviles, para que sea verdaderamente efectivo, el conocimiento del comportamiento de la siniestralidad de quienes contratan el seguro del automóvil, lo cual únicamente puede llevarse a cabo mediante la creación de un "Fichero Histórico", de las características del regulado en este Código Tipo, y su correlativo beneficio en el favorecimiento de los asegurados que, sin duda son la mayoría, que por tener un buen historial de siniestralidad se van a favorecer de la transparencia del mercado.

El Fichero, recogerá los datos relativos a los contratos así como el historial de siniestros de cada tomador o contratante de seguro de automóviles durante los últimos cinco años de vigencia de su póliza, al objeto de facilitar al momento de la suscripción del contrato información rigurosa y contrastada de los datos de siniestralidad mediante la puesta en común de la información obtenida a través de pólizas y siniestros, que permitirá completar la facilitada por el propio tomador y que puede no ser conocida o recordada por éste.

Unicamente tendrán acceso a los datos las entidades adheridas al Fichero, quienes lo podrán utilizar para realizar consultas en el momento de la solicitud para la suscripción de nuevas pólizas, y de este modo, poder hacer una valo - ración técnica y objetiva del riesgo, así como la correcta aplicación de las tarifas de prima que tengan recogidas en sus bases técnicas..

El Fichero Histórico, cuya regulación se desarrolla en este Código Tipo, se fundamenta jurídicamente en el párrafo segundo del artículo 24.3 de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados que, textualmente dice: "Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora".

El contenido del Fichero está adecuado a la Ley 30/1995, así como a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a su normativa de desarrollo, especialmente en todo lo previsto en cuanto a garantizar los derechos de las personas cuyos datos son tratados en el mismo.

El Fichero se rige por el presente "Código Tipo" que se formula a los efectos y en los términos del artículo 32 de la LOPD, por lo que será depositado en el Registro General de Protección de Datos.

2. OBJETO

El Fichero Histórico, cumple con la finalidad descrita en el artículo 24.3, párrafo segundo de la Ley 33/1995 en cuanto a fichero de colaboración estadístico-actuarial para la tarificación yselecciónde riesgos, recogiendo información sobre los contratos de seguros del automóvil que el tomador ha suscrito en los últimos cinco años así como de los siniestros vinculados a dichos contratos.

Igualmente, el Fichero contribuirá a promover la transparencia en el mercado del seguro del automóvil y la aplicación equitativa y suficiente de las tarifas a los riesgos asegurados. Los asegurados tendrán un mayor acceso al conjunto de ofertas del sector y podrán buscar la que más se adecue a sus necesidades al permitírsele tener conocimiento de sus propios datos de siniestralidad, factor esencial para el cálculo de la prima del seguro. Por su parte las entidades aseguradoras tendrán una información exacta y precisa del riesgo que complementará la facilitada por el tomador en la solicitud de seguro, en su deber de declaración del riesgo.

Se entiende por siniestro elacaecimiento del hecho que, previsto en el contrato, es susceptible de dar lugar al pago de la indemnización por la entidad aseguradora con cargo a la póliza suscrita por el tomador.

3. AMBITO SUBJETIVO

3.1. Titular - Responsable del Fichero

Del presente fichero es titular la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA), domiciliada en Madrid, c/ Núñez de Balboa, 101, que como Asociación Profesional de empresarios, se constituye al amparo de la Ley 19/1977 y el Real Decreto 873/1977 de 22 de abril, para la representación, gestión y defensa de los intereses económicos, sociales y profesionales, comunes, de sus asociados. (artículo 1 de los Estatutos de esta Asociación), sin perjuicio del régimen de responsabilidad de las entidades aseguradoras adheridas al fichero descrito en el artículo 6 .

UNESPA tiene personalidad jurídica, autonomía y plena capacidad de obrar para el cumplimiento de sus fines, dentro de las disposiciones legales y estatutarias y como responsable del Fichero, cumplirá lo establecido en la Ley Orgánica de protección de datos de carácter personal y en sus normas de desarrollo, fundamentalmente en lo relativo a preservar los derechos individuales de los afectados, en cuanto al acceso, rectificación y cancelación y oposición, con independencia de lo previsto en el artículo 8 en cuanto a las obligaciones que recaen sobre las entidades aseguradoras

3.2. Empresa de servicios de tratamiento automatizado

La gestión informática y el tratamiento de datos del Fichero se realizará por Tecnologías de la Información y Redes para las Entidades Aseguradoras, S.A. (TIREA), en cuyo domicilio social, c/ García de Paredes n§ 55, de Madrid, se emplazará físicamente el mismo y se encargará de llevar a cabo las actividades que garanticen la prestación de los servicios informáticos, incluyendo la realización de los controles necesarios para asegurar que no se realiza un uso indebido del Fichero.

En el contrato de servicios suscrito por UNESPA y TIREA, ésta se compromete a mantener la más absoluta confidencialidad sobre los datos almacenados, intercambiados, o que se obtengan como consecuencia del procesamiento de los mismos, así como incorporar al Servicio estrictos controles de seguridad que eviten un uso indebido de la información por cualquier entidad, garantizando en todo caso el cumplimiento de la legislación vigente en materia de la protección de datos de carácter personal y de las normas de seguridad de los sistemas informáticos recogidas en el Real Decreto 994/1999, de 11 de junio.

3.3. Entidades usuarias del servicio

Podrán adherirse al Fichero todas las entidades aseguradoras autorizadas para operar en España en el ramo de responsabilidad civil de automóviles, sean o no asociadas a UNESPA, teniendo como único requisito imprescindible que estén inscritas en el Registro Especial de la Dirección General de Seguros.

Las entidades aseguradoras que quieran incorporarse al Fichero deberán firmar, a través de representante legal con poder suficiente, contrato con UNESPA y TIREA en el que se incorpora a todos los efectos este Código Tipo que deberá ser aceptado expresamente, comprometiéndose a cumplir estrictamente todos y cada uno de sus preceptos.

En el contratose incluirá, además**,** la designación de las personas que actuarán como interlocutores (titular y suplente) y el Responsable de Seguridad de la entidad, al objeto de coordinar más eficazmente la canalización de las informaciones, así como para agilizar los trabajos de campo y toma de decisiones.

La entidad aseguradora adherida quedará identificada mediante un código de compañía que figurará en toda recepción y envío de información que realice, comunicándose las altas en el Fichero a la Agencia de Protección de Datos, al objeto de que queden incorporadas al Código Tipo.

4. COMISION DE CONTROL

Se constituye una Comisión de Control en UNESPA integrada por 1 representante de ésta Asociación, 2 representantes de TIREA y 6 representantes de entidades aseguradoras adheridas al Fichero, estos últimos serán elegidos entre las entidades adheridas y su mandato será por dos años, pudiendo ser reelegidos por períodos de igual duración.

Además de las competencias que expresamente se le asignan en este Código Tipo, le corresponden a la Comisión las que siguen:

* Potestad para determinar, tanto al inicio de funcionamiento del Fichero como durante su vigencia, la adhesión de entidades o su exclusión por falta de adecuación a los requisitos técnicos o de seguridad de los datos.

* Establecer las directrices y comunicar las instrucciones a las entidades aseguradoras para el correcto funcionamiento del Fichero.

* Controlar el cumplimiento de las normas de funcionamiento en cuanto al acceso y transmisión de datos de las entidades, así como en los requerimientos de información en el ejercicio de los derechos de acceso, oposición, rectificación y cancelación por parte de los asegurados.

* Vigilar, mediante los mecanismos de control y seguridad establecidos, el respeto al buen uso del Fichero.

* A partir de los datos facilitados por el Servicio, decidir y calificar sobre posibles infracciones que se produzcan, así como establecer las sanciones a que den lugar, las cuales se comunicarán al responsable de la entidad aseguradora infractora. Cuando la infracción pueda afectar al régimen jurídico de la protección de datos, se pondrá en conocimiento de la Agencia de Protección de Datos.

* Recabar información de las entidades aseguradoras sobre el funcionamiento y prestación del Servicio, así como anomalías, dudas y sugerencias que sobre el mismo puedan realizarse.

* Resolver, a solicitud del afectado, las controversias que pueden surgir entre éste y la entidad aseguradora respecto a la procedencia de la rectificación, cancelación y oposición de los datos, en los términos expresados en el artículo 8.2. de este Código Tipo.

La Comisión se constituirá formalmente cuando todos los trámites y pruebas estén concluidos y el Fichero en disposición de comenzar su funcionamiento.

5. SEGURIDAD

5.1. Seguridad del fichero

El Fichero Histórico tiene implementado un sistema de seguridad que garantiza el cumplimiento estricto de la Ley Orgánica de Protección de Datos y que consisten en:

1. Los datos del Fichero no pueden ser objeto de volcado en la base de datos de la Entidad, su consulta únicamente puede realizarse caso a caso. La Entidad se compromete a no imprimir o grabar los datos a que acceda a través de consulta al Fichero.

2. Tras permitir el acceso, sólo se podrá obtener información del Fichero cuando media petición de aseguramiento por el tomador, quien deberá aportar imprescindiblemente su número de póliza y cualquiera de los tres datos siguientes: nombre y apellidos; DNI o cualquier otro documento de identificación, y/o matrícula del vehículo. Sin el dato del número de póliza no se puede acceder al Fichero.

3. Para preservar la confidencialidad de los datos y poder depurar responsabilidades en caso de mal uso de los mismos, en toda la información extraída del Fichero quedará reflejada: fecha, hora y entidad que accede.

4. Registro de incidencias. Si se produce un incidente de seguridad TIREA se pondrá en contacto inmediatamente con el Responsable de Seguridad de la entidad aseguradora. Por TIREA se recogerá la incidencia en la Aplicación de Consultas de Incidencias, conde se hará constar: tipo de incidencia, momento en el que se ha producido y persona que la ha detectado.

5. Gestión de soportes. Todos los soportes que necesitan ser almacenados son inventariados de modo que se conoce la información que contiene. Existe un registro de entrada y salida de soportes en el que se incluye la fecha de entrada y salida. Cuando un soporte va a ser desechado o inutilizado se usan procedimientos de borrado o inutilización que impiden su legibilidad o reutilización.

6. Bloqueo y cancelación de datos. Si el afectado, tras la solicitar el acceso a sus datos, del que queda constancia informática y documental, ejerce el derecho de rectificación, cancelación u oposición, sus datos bloqueados hasta que se resuelva. Si se acepta la solicitud, se procede al borrado inmediato de los datos.

Por su parte, las entidades adheridas deberán adoptar medidas de seguridad de nivel medio e incluir en el documento de seguridad a que obliga el Real Decreto 994/1999, un capítulo específico sobre los medios empleados para garantizar la seguridad de los datos del Fichero Histórico, especialmente la relativa a funciones y obligaciones de las personas autorizadas por la entidad para acceder al Fichero

Cuando la información contenida en el fichero vaya a ser utilizada por UNESPApara la elaboración de informes de técnica aseguradora o con fines únicamente estadísticos, se presentará de forma disociada para que sea imposible relacionarla con ninguna persona en particular.

6. RESPONSABILIDAD

Cada Entidad cedente asume la total responsabilidad sobre la veracidad de los datos e informaciones que facilite al Ficheroasí como por el incumplimiento de cualesquiera obligaciones derivadas de éste Código Tipo, comprometiéndose a enviar la información que se detalla en el artículo 7, y a remitir, cuando lo solicite UNESPA, los documentos necesarios para acreditar la exactitud de los mismos.

A tal efecto, se establece un régimen sancionador en el presente Código Tipo a fin de garantizar la observancia de la Legislación de Protección de Datos por las entidades adheridas.

Igualmente se responsabiliza de la confidencialidad y del buen uso que, por su parte, se realice de la información,

evitando el tráfico de ésta o su uso inadecuado. Además, la Entidad impedirá la utilización de la información del Fichero para cualesquiera otras finalidades que no sean las previstas en este Código Tipo así como divulgar información personal o confidencial. Especialmente a no publicar en medios públicos o privados las informaciones obtenidas a través del Fichero.

7. NORMAS DE FUNCIONAMIENTO

La Entidad adherida se compromete a enviar la información a que se refiere este artículo, según la periodicidad y procedimientos informáticos que se detallan a continuación:

Al inicio se deben enviar todas las pólizas vigentes y los siniestros de dichas pólizas en cinco años, correspondientes al primer mes vista de vencimiento, dado que la carga total de datos se realizará en doceavas partes. En cada envío mensual además se remitirá información sobre los nuevos contratos que formalice la entidad, así como las modificaciones de los datos ya incluidos en el fichero.

Esto permitirá la implantación paulatina del fichero y que se puedan hacer debidamente las comunicaciones a los afectados.

Una vez concluida esta primera etapa, mensualmente se enviará la información de nuevos contratos y modificaciones de pólizas y siniestros que ya estuvieren en el Fichero.

En todos los procesos se efectúan las necesarias modificaciones y altas de los movimientos correctos y se devuelven a la entidad aquellos que no hayan satisfecho los controles de validación.

En cualquier momento las entidades pueden mandar procesos de actualización especiales para atender las solicitudes de los afectados en ejercicio de los derechos que la Ley Orgánica les otorga.

TIREA bloqueará automáticamente los datos que tengan más de cinco años de antiguedad.

Para garantizar la veracidad de los datos que se remiten al Fichero estos deben provenir, en todo caso, de los Registros de Pólizas y de Siniestros que, con carácter obligatorio se establecen en el artículo 65 del Reglamento de la Ley de Ordenación y Supervisión de los Seguros Privados y que están sometidos al control y supervisión de la Dirección General de Seguros.

7.1. Datos del Fichero

El Fichero contendrá los siguientes datos:</U>

* Vehículo asegurado

* Datos del tomador:

* Nombre y Apellidos o razón social; D.N.I., N.I.F., Pasaporte o Tarjeta de Residencia del tomador del seguro.

* Datos del contrato:

* Coberturas que se incluyen dentro del grupo de ramos denominado "Seguro del Automóvil" así como las coberturas recogidas en los ramos "Asistencia"

* "Defensa Jurídica".

* Período de vigencia del contrato

* Datos del siniestro:

* Cobertura afectada por cada siniestro

* Fecha del siniestro

* Existencia de daños materiales y/o corporales

* Importe del siniestro (en los supuestos en los que el siniestro esté pendiente de liquidación o pago el campo relativo a importe quedará en blanco poniéndose de este modo de manifiesto su situación de pendiente)

Las Entidades se comprometen a informar al Sistema de todas las variaciones de la producción de pólizas y de la situación de los siniestros, a fin de mantener correctamente actualizadas las informaciones contenidas en el Fichero.

7.2. Procesos de Consultas

Las Entidades adheridas podrán realizar consultas al Fichero, según los modelos propuestos en la plataforma tecnológica, que no permite en ningún caso volcar el fichero en su base de datos**.** Para efectuar las consultas, la entidad, ante la solicitud de aseguramiento del interesado, deberá identificarle correctamente debiendo informar al Sistema mediante las claves necesarias:

* Cinco últimos dígitos de la póliza en vigor

* Y, Al menos uno de los tres datos siguientes:

* Nombre y apellidos del tomador

* Número del Documento identificativo

* Matrícula del vehículo

Como respuesta a la consulta efectuada, el Sistema facilitará a la Entidad la información que se encuentre en el Fichero relativa a pólizas suscritas, sus correlativos períodos de cobertura, así como de los siniestros y las garantías afectadas. En la información que arroja el Sistema no aparecerán datos personales del tomador del seguro ni valoraciones personales de ningún tipo.

Desde el Servicio se realizará el registro y notaría de todas las consultas realizadas clasificadas por entidad.

7.3. Deber de comunicación al afectado

En cumplimiento de lo establecido por el artículo 24.3. de la Ley 30/1995, de ordenación y supervisión de los seguros privados, y previamente a ceder datos a los ficheros comunes, las entidades aseguradoras vendrán obligadas a informar a los afectados de la intención de ceder sus datos al fichero, de la finalidad de éste**,** con indicación de su responsable y del procedimiento para ejercitar los derechos de oposición, acceso, rectificación y cancelación.

Dicha notificación será uniforme para todas las entidades aseguradoras adheridas y se incluye el modelo de la misma en el presente Código Tipo.

8. DERECHOS DE LOS AFECTADOS

Los datos son personalísimos, por ello los derechos de acceso, rectificación, cancelación y oposición, únicamente pueden ser ejercidos por las personas físicas o sus representantes legales, debiendo acreditar su identificación frente al responsable del fichero, de acuerdo con lo previsto en la LOPD, y en su normativa de desarrollo.

8.1. Derecho de acceso

Para facilitar el acceso, se establecerá un documento normalizado que junto a la copia del D.N.I, NIF, Pasaporte o Tarjeta de Residencia o, poder notarial en caso de actuar mediante representante, identifique al tomador e impida el acceso al Fichero a quienes no estén debidamente acreditados.

Si la solicitud se formula correctamente, TIREA emitirá certificación en la que consten todos los datos que sobre esa persona contiene el Fichero.

En el supuesto de que no se adjunte copia del documento de identificación o del poder, o los datos no se correspondan con el solicitante, se remitirá escrito denegando el acceso en el que se indicará la causa de tal denegación, concediendo al interesado la posibilidad de subsanar los errores que existan en su petición.

El derecho de acceso sólo podrá ser ejercitado a intervalos no inferiores a doce meses.

8.2. Derecho de rectificación, cancelación y oposición

Si tras haber ejercitado el derecho de acceso, el afectado ejercita los derechos rectificación, cancelación u oposición, deberá formular su solicitud con la indicación de los datos que, por considerar incorrectos o inexactos, quiere que sean modificados o cancelados y aportando cuantos documentos avalan su pretensión. Si lo que se ejercita es el derecho de oposición deberá fundamentar la causa por la cual considera que sus datos no deben ser objeto de tratamiento automatizado.

Si la rectificación o cancelación afecta a datos personales de identificación y con la documentación aportada por el afectado resultare suficientemente probado el error o la inexactitud, se procederá automáticamente a su modificación o cancelación, comunicándolo a la Entidad aseguradora.

Cuando la solicitud verse sobre la existencia y/o cuantía de los siniestros, el responsable del fichero dará traslado de la

solicitud a la entidad aseguradora que haya facilitado el dato, al objeto de que en el plazo de ocho días resuelva de forma motivada sobre su procedencia. La información que sobre el afectado contenga el fichero quedará bloqueada hasta que se resuelva la solicitud.

Si la entidad no se pronuncia, TIREA mantendrá el bloqueo cautelar del dato, y se comunicará tanto al afectado como a la entidad aseguradora que deberá proceder a su rectificación o cancelación, en los términos de la solicitud, en la primera actualización de información. Realizada la necesaria comprobación por TIREA, si la entidad no hubiera procedido a dicha rectificación o cancelación, el dato quedará definitivamente bloqueado.

Si la entidad aseguradora resuelve oponiéndose a la rectificación o cancelación solicitada, deberá motivar su posición ante UNESPA, como responsable del Fichero. La respuesta de la entidad aseguradora será trasladada al afectado, indicándole que la misma puede ser recurrida ante la Comisión de Control en el plazo de quince días desde que recibió la comunicación, mediante presentación de escrito en que razone su petición y los documentos en que fundamenta la misma. Recibido el escrito de recurso, se resolverá por la Comisión de Control en el plazo de quince días.

8.3. Derecho de oposición

Cuando se ejercite el derecho de oposición habrá que atender a la causa de tal solicitud y a los motivos en que fundamenta su pretensión el solicitante. Se seguirá idéntico procedimiento que el descrito para los derechos de rectificación y cancelación. No obstante y, en los casos en que se desestime y acredite por la entidad aseguradora la improcedencia de la oposición, UNESPA podrá, tras comunicarlo al afectado, proceder de oficio al bloqueo de los datos y elevar consulta a la Agencia de Protección de Datos para clarificar la procedencia de tratamiento automatizado de los datos.

9. INCUMPLIMIENTO DEL CODIGO TIPO: RÉGIMEN SANCIONADOR

La Comisión de Control intervendrá en todos los supuestos en los que se ponga de manifiesto el incumplimiento de las normas que informan el Fichero, especialmente cuando se trate del uso desproporcionado, abusivo o, cualquier utilización distinta a los fines para los que ha sido creado. La Comisión actuará bien a instancia de cualquier entidad adherida o de oficio cuando se detecten anomalías a través de los Controles de Seguridad incluidos en la aplicación informática, porque se evidencia a través las solicitudes de rectificación y cancelación ejercidas por los tomadores, o por los informes de control y estadísticas de utilización.

Si la contravención fuera susceptible de constituir una infracción de la LOPD, la Comisión de Control pondrá los hechos en conocimiento de la Agencia de Protección de Datos, como órgano competente para inspeccionar y, en su caso seguir el procedimiento sancionador hasta la resolución del asunto.

Una vez adquiera firmeza la Resolución sancionadora, y atendiendo a la gravedad de la infracción, la entidad aseguradora podrá ser dada de baja del Fichero, con el consiguiente bloqueo de los datos aportados por la misma durante el plazo de cinco años, conservándose únicamente a efectos de los requerimientos que puedan formularse por las Administraciones Públicas, Jueces y Tribunales.

Corresponde a la Comisión de Control la imposición de sanciones por las conductas que a continuación se enumeran:

a) Infracciones leves, consistentes en:

* Retraso injustificado de la Entidad en la contestación al ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

* Error de la Entidad en los datos remitidos, puesto de manifiesto por el ejercicio del derecho de rectificación, cancelación u oposición del titular, que afecte a menos del 25 % de los supuestos de ejercicio de derecho de rectificación.

Por las infracciones leves se impondrá sanción de apercibimiento.

b) Infracciones graves, consistentes en:

* Utilización de los datos del fichero sin haberse formulado solicitud de aseguramiento por el tomador o para finalidad distinta de la contemplada en el artículo 2 de este Código Tipo, cuando tenga carácter ocasional o aislado.

* Error de la Entidad en los datos remitidos, puesto de manifiesto por el ejercicio del derecho de rectificación, cancelación u oposición del titular, que afecte a más del 25 % y menos del 50 % de los supuestos de ejercicio de derecho de rectificación.

* Comisión de tres infracciones leves en el plazo de un año natural.

Por la infracción grave se impondrá sanción de suspensión de la utilización del fichero por la Entidad de hasta un año.

c) Infracciones muy graves, consistentes en:

* Vulneración del deber de confidencialidad de los datos y la conservación y almacenamiento, por cualesquiera procedimientos, de los consultados al Fichero.

* Reincidencia en la utilización de los datos del fichero sin haberse formulado solicitud de aseguramiento por el tomador o para finalidad distinta de la contemplada en el artículo 2 de este Código Tipo.

* Error de la Entidad en los datos remitidos, puesto de manifiesto por el ejercicio del derecho de rectificación, cancelación u oposición del titular, que afecte a más del 50 % de los supuestos de ejercicio de derecho de rectificación.

* Comisión de tres infracciones graves en el plazo de un año natural.

Por las infracciones muy graves se impondrá sanción de baja en el fichero.

10. BAJA DE ENTIDADES PARTICIPANTES

Las Entidades podrán, por propia decisión, causar baja del Convenio mediante la notificación por escrito de su voluntad. En tal situación se procederá a dar de baja en el Fichero todas las referencias aportadas por cada Entidad; para ello, deberá enviar una notificación por escrito firmada por persona autorizada de la Entidad a la Comisión donde se exprese dicha intención. Esta comunicación deberá ser hecha, al menos con dos meses de antelación respecto a la fecha en que deseara causar baja.

La baja de cualquier Entidad deberá ser comunicada por escrito a la Agencia de Protección de Datos.

11. DURACION DEL CODIGO TIPO

El presente Código Tipo tiene una duración indefinida, si bien, por el propio desarrollo del Fichero o por imperativos legales, podrá ser modificado para su actualización o adecuación. Los cambios a introducir en tales situaciones, serán elaborados y propuestos por la Comisión de Control, para su aprobación por la Agencia de Protección de Datos y dándose posteriormente comunicación al resto de participantes.

MODELOS DE COMUNICACIÓN DE LA ENTIDAD ASEGURADORA AL TOMADOR

En virtud de la autorización que concede la Ley 30/1995, Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA) ha creado el Fichero Histórico de Seguros de Automóviles para la tarificación y selección de riesgos, constituido con la información aportada por las Entidades Aseguradoras.

Le comunicamos que los datos sobre su contrato de seguro del automóvil y los siniestros vinculados a éste, de los últimos cinco años, si los hubiere, serán cedidos al citado fichero común.

Si desea ejercitar los derechos de acceso, rectificación, cancelación y oposición puede dirigirse a TIREA, C/ García de Paredes, n§ 55, 28010 MADRID, debiéndose identificar mediante DNI, Pasaporte o Tarjeta de Residencia.

SOLICITUD DE ACCESO

Debe dirigirse a: TIREA

C/ García de Paredes n§ 55 28010 MADRID
D.
Con D.N.I. n§
Domiciliado en
C/

lo cual acredita mediante exhibición de

(Si actúa mediante representante legal)
en representación de con D.N.I.

En virtud de lo establecido en el artículo 15 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal sobre el derecho de acceso,

SOLICITA información respecto a los datos que sobre su historial de aseguramiento figuran en el Fichero Histórico de Seguros del Automóvil del que es Titular Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA).

En _____, a ____ de _____ de 200

CONTESTACION DE ESTIMACION DE ACCESO

Remisión por correo certificado con acuse de recibo o recoger en domicilio social de TIREA

Muy Sr. nuestro:

En contestación a su solicitud de acceso de fecha le informamos que los datos que constan respecto a Vd. en el Fichero Histórico de Seguro de Automóviles, **son los que se detallan en el Anexo adjunto.**

En caso de que sus datos personales sean inexactos o incompletos puede ejercitar los derechos de rectificación y cancelación de los datos o de oposición al tratamiento de datos, ante TIREA, mediante presentación de escrito de solicitud dirigido al domicilio que figura en este escrito, en el que fundamente su petición aportando documentación que acredite la veracidad de lo solicitado Tratándose de datos relativos a su historial de aseguramiento trasladaremos su solicitud a la entidad aseguradora al objeto de que ésta resuelva sobre la procedencia de la rectificación y en su caso de la cancelación u oposición. Desde TIREA le trasladaremos la contestación de la entidad aseguradora en el plazo de 10 días desde la recepción de su escrito. DENEGACION DE ACCESO

Muy Sr. nuestro:

En contestación a su solicitud de acceso de fecha le informamos que la solicitud de acceso a los datos contenidos en el Fichero Histórico de Seguros de Automóviles ha sido desestimada por:

( ) Falta de garantía de identificación.

( ) Ya fue ejercitado su derecho en un plazo inferior a doce meses

En el primer supuesto deberá cumplimentar nuevamente la hoja de solicitud adjunta aportando la documentación que en ella se indica y remitirla por correo certificado a:

TIREA

c/ García de Paredes n§ 55 28010 MADRID

ESTIMACION DE RECTIFICACION O CANCELACION POR ERRORES DE DATOS PERSONALES

Muy Sr. nuestro:

En contestación a su solicitud de rectificación (o cancelación) de los datos contenidos en el Fichero Histórico de Seguros de Automóviles, de fecha _____,le comunicamos que hemos procedido a la misma una vez analizados los documentos por Vd. aportados, por lo que los datos que quedan inscritos en el **Fichero** son los siguientes:

Por otro lado, le informamos que se ha cursado comunicación a la entidad aseguradora cesionaria de sus datos al objeto de que procedan a su rectificación (o cancelación). ESTIMACION DE RECTIFICACION, CANCELACION U OPOSICION

Muy Sr. nuestro:

En contestación a su solicitud de rectificación de fecha ,de los datos en relación con la siniestralidad que ha tenido con la entidad Aseguradora ....., contenidos en el Fichero Histórico de Siniestralidad de Conductores, le comunicamos que habiendo dado traslado de su solicitud a la entidad aseguradora,

* ésta a la vista de la documentación aportada por Vd., nos ha comunicado la procedencia de su solicitud, por lo que procederemos a (rectificar) (cancelar) sus datos (o a cancelar el registro informático en que Vd. aparece).
* no se ha pronunciado en el plazo establecido, por lo que procederemos a (rectificar) (cancelar) cautelarmente sus datos (cancelar el registro informático en el Vd. aparece).

DESESTIMACION DE RECTIFICACION, CANCELACIÓN U OPOSICION

Muy Sr. nuestro:

En contestación a su solicitud de rectificación (cancelación) (oposición al tratamiento informático) de los datos contenidos en el Fichero Histórico Seguros de Automóviles, de fecha ....., le comunicamos que ha sido desestimada su petición por:

( ) Falta de precisión de los datos que pretende sean modificados o cancelados.

( ) Oposición de la entidad aseguradora cedente de los datos de aseguramiento, adjuntándole escrito de denegación de su solicitud formulado por la misma.

Le adjuntamos escrito de contestación de la entidad aseguradora y le informamos que, de no estar conforme, puede

presentar recurso en el plazo de 15 días desde que reciba esta carta ante la Comisión de Control del Fichero, en este mismo domicilio. En el escrito debe exponer las causas por las cuales Vd. se opone a la decisión de la entidad y aportar cuantos documentos avalen su posición. La Comisión le contestará en el plazo de 15 días desde que reciba su escrito.

Igualmente, puede presentar reclamación ante la Agencia de Protección de Datos, de conformidad con lo previsto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personales. </BODY> </HTML>

MEMORIA DE 2000 - ANEXO VII - CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

Este documento se encuentra en la Base de Datos de legislación.

MEMORIA DE 2000 - ANEXO VIII - DICTAMEN 1/2000 SOBRE DETERMINADOS ASPECTOS DE PROTECCIÓN DE DATOS DEL COMERCIO ELECTRÓNICO

Presentado por el Grupo operativo sobre Internet Aprobado el 3 de febrero de 2000 **Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico**

1. Introducción

La UE está debatiendo la adopción de una propuesta de Directiva sobre determinados aspectos jurídicos del comercio electrónico 1 . Como ha venido haciendo hasta la fecha, el Grupo de trabajo sobre protección de datos del artículo 29 2 desea participar de manera constructiva en esta actividad de refuerzo de la normativa sobre comercio electrónico. Con este Dictamen, el Grupo de trabajo tiene la intención de poner de relieve un problema de protección de datos planteado por el comercio electrónico, así como explicar el tratamiento que recibe en la legislación europea. El marco jurídico para la protección del derecho fundamental a la vida privada y la protección de los datos personales ya está establecido en la Directiva 95/46/CE que define los principios generales de protección de datos y en la Directiva 97/66/CE que los complementa para el sector de las telecomunicaciones.

El Grupo de trabajo desea expresar su satisfacción porque el texto actualmente en fase de adopción contiene una aclaración expresa en un nuevo considerando y en la nueva letra b) del apartado 4 del artículo 1, relativos a la aplicación adecuada y plena de la legislación sobre protección de datos 3 en los servicios de Internet. Esto significa que la aplicación de la Directiva sobre comercio electrónico debe estar totalmente de acuerdo con los principios de protección de datos.

El Grupo de trabajo ya ha prestado mucha atención a los problemas de protección de datos relacionados con Internet, especialmente durante 1999 con la emisión de orientaciones generales sobre tres cuestiones importantes relacionadas con las características específicas de las nuevas tecnologías de la información. Ha emitido un dictamen sobre la información del sector público 4 y recomendaciones sobre el tratamiento invisible y automático de datos personales en Internet 5 , así como sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación 6 .

En el contexto del comercio electrónico surge una cuarta cuestión. El Grupo de trabajo desea ofrecer una interpretación sobre la aplicación de las normas europeas sobre protección de datos al tratamiento de los datos para envíos comerciales por correo electrónico.

2. La cuestión de los envíos por correo electrónico

Para lanzar una campaña publicitaria o de envíos comerciales, una empresa debe obtener una lista amplia y pertinente de direcciones de correo electrónico de posibles clientes. Las empresas tienen tres posibilidades para conseguir direcciones de correo electrónico en Internet: recopilación directa de los clientes o visitantes de los sitios web; listas preparadas por terceros 7 y recopilación en espacios públicos de Internet, tales como directorios públicos, foros o ® *chat-rooms* ¯.

Una característica particular de los envíos comerciales electrónicos es que, mientras que el coste para el remitente es extremadamente bajo en comparación con los métodos tradicionales de márketing directo, el destinatario debe hacer frente a un coste por tiempo de conexión. Esta situación supone un claro incentivo para utilizar esta herramienta de márketing a gran escala y hacer caso omiso de la protección de datos y de los problemas provocados por los envíos publicitarios mediante correo electrónico.

El problema desde la perspectiva del ciudadano tiene tres facetas: en primer lugar, la inclusión en una lista de su dirección de correo electrónico sin su consentimiento o conocimiento; en segundo lugar, la recepción de grandes cantidades de mensajes publicitarios no deseados; y, en tercer lugar, el coste del tiempo de conexión. Una cuestión fundamental en este ámbito es el bombardeo publicitario 8 . El bombardeo publicitario es la práctica de enviar mensajes electrónicos no solicitados, normalmente de tipo comercial, en gran número y repetidamente a particulares con los que el remitente no tenía ningún contacto previo. Suele ocurrir cuanto se ha obtenido una dirección electrónica en un espacio público de Internet. El problema desde la perspectiva del mercado interior es la posibilidad de que existan normativas nacionales divergentes sobre comunicaciones comerciales electrónicas que den lugar a obstáculos al comercio. Ambos tipos de problemas han influido en el desarrollo de la legislación comunitaria pertinente.

3. Legislación comunitaria y su aplicación a los envíos por correo electrónico

Ya se ha indicado la norma general de que la legislación sobre protección de datos se aplica al comercio electrónico 9 . Los envíos publicitarios electrónicos son un ejemplo concreto de la manera de resolver los problemas de protección de datos planteados por el comercio electrónico, empleando los principios jurídicos incluidos en las dos Directivas. La Directiva general afirma que los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y tratados de manera leal y lícita compatible con dichos fines 10 .

El tratamiento sólo podrá efectuarse con fundamentos legítimos, tales como el consentimiento, un contrato, una obligación jurídica o el equilibrio de intereses 11 .

Además, el interesado debe estar informado sobre los fines del tratamiento 12 y se le reconocerá el derecho a oponerse al tratamiento de sus datos personales con fines de prospección 13 . La Directiva de protección de la intimidad en el sector de las telecomunicaciones ofrece a los Estados miembros la posibilidad de elegir entre la aplicación de normas de aceptación voluntaria (® *opt-in* ¯) o exclusión voluntaria (® *opt-out* ¯) para las comunicaciones comerciales no solicitadas 14 . A estas normas sobre protección de datos se suman determinados requisitos inspirados por la protección al consumidor. La Directiva sobre venta a distancia, por ejemplo, exige proporcionar a los consumidores, como mínimo, el derecho a oponerse a las comunicaciones a distancia 15 mediante correo electrónico.

Una vez adoptada, la Directiva sobre comercio electrónico podrá establecer explícitamente en su artículo 7 dos aspectos *técnicos*: la obligación de que los correos electrónicos comerciales se identifiquen como tales y la obligación de consultar y respetar las listas de exclusión voluntaria (® *opt-out* ¯) cuando su existencia esté regulada en la legislación nacional. Sin embargo, un considerando y la letra b) del apartado 4 del artículo 1 establecen claramente que esta Directiva no tiene en modo alguno el objetivo de modificar los principios *jurídicos* ni los requisitos incluidos en el marco legislativo en vigor descrito anteriormente. Dado que la legislación sobre protección de datos se aplica plenamente al comercio electrónico, la aplicación de la Directiva sobre comercio electrónico deberá realizarse siguiendo los principios de protección de datos. Esto significa que, en lo que respecta a la protección de datos, el Derecho nacional aplicable al responsable del tratamiento de los datos personales seguirá siendo el del Estado miembro de establecimiento 16 . También significa que la Directiva sobre comercio electrónico no podrá impedir a los Estados miembros que exijan a las empresas el consentimiento previo para las comunicaciones comerciales 17 , ni tampoco la utilización anónima de Internet 18 .

En opinión del Grupo de trabajo, estas normas responden claramente a la cuestión de la vida privada planteada en la sección 2 anterior y ofrecen una imagen nítida de los derechos y obligaciones de los afectados. Se deben distinguir dos situaciones:

* Si una empresa ha obtenido una dirección de correo electrónico *directamente*

del interesado para envíos electrónicos que realizará dicha empresa o un tercero al que proporcione los datos, la empresa inicial debe informar al interesado de dicha finalidad en el momento de recibir la dirección 19 . Además, la empresa inicial y las que hayan recibido los datos posteriormente deberán proporcionar al interesado, como mínimo, en el momento de la recogida y en todo momento posterior, el derecho a oponerse a este uso de sus datos por medios electrónicos sencillos, tales como picar una casilla creada a tal efecto 20 .

Determinadas leyes nacionales por las que se aplican las Directivas pertinentes exigen incluso que la empresa obtenga el consentimiento del interesado.

Los requisitos del artículo relativo a las comunicaciones comerciales no solicitadas del proyecto de Directiva sobre comercio electrónico completarían estas normas en un nivel técnico imponiendo al proveedor de servicios la obligación de consultar una lista, pero no eliminarían ninguna de las obligaciones generales aplicables a los responsables del tratamiento de los datos.

* Si una dirección de correo electrónico se obtiene en un *espacio público de*

Internet, su utilización para envíos comerciales electrónicos sería contraria a la legislación comunitaria correspondiente, por tres motivos.

En primer lugar, se podría considerar tratamiento ® desleal ¯ de los datos personales en el sentido de la letra a) del apartado 1 del artículo 6 de la Directiva general. En segundo lugar, sería contraria al principio de la finalidad de la letra b) del apartado 1 del citado artículo 6, ya que el interesado proporcionó su dirección de correo electrónico para una finalidad muy distinta, como puede ser la participación en un foro, por ejemplo. En tercer lugar, dado el desequilibrio del coste y la interrupción para el destinatario, se puede considerar que estos envíos no superarían la prueba del equilibrio de intereses establecida en la letra f) del artículo 7 21 .

4. Conclusiones

Este Dictamen no se considera la posición definitiva del Grupo de trabajo sobre la interacción entre comercio electrónico y protección de datos. Su objetivo es sensibilizar sobre las cuestiones planteadas por un tipo concreto de tratamiento de los datos que actualmente es objeto de debate en numerosos círculos, así como contribuir a la comprensión del marco jurídico aplicable al comercio electrónico. Es perfectamente posible que existan otros problemas sobre comercio electrónico además de los ya abordados por el Grupo de trabajo que precisen una orientación interpretativa o un enfoque común. Por tanto, el Grupo de trabajo considera necesario desarrollar una política común sobre aspectos tales como el ® cibermárketing ¯, el pago electrónico o las Tecnologías para mejorar la protección de la vida privada. Ha encargado al Grupo operativo Internet que continúe sus tareas. Se esperan diversos resultados, incluidas recomendaciones sobre medidas técnicas relativas al bombardeo publicitario (® *spa*m ¯) o la validación de sitios web de conformidad con una lista europea común basada en las directivas de protección de datos.

NOTAS:

1 Propuesta modificada de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior, COM (1999) 427 final. El Consejo de Ministros del 7 de diciembre de 1999 alcanzó un acuerdo político sobre el texto y pronto se adoptará formalmente una Posición común, antes de la segunda lectura en el Parlamento Europeo. Véase el Comunicado de prensa IP/99/952, pp.1 y 4.
2 Creado en virtud del artículo 29 de la Directiva 95/46/CE, citada en la nota 3 siguiente.
3 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995, p. 31, y Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DO L 24 de 30.1.1998, p. 1. Se pueden consultar en http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm
4 Dictamen 3/99 relativo a la información del sector público y protección de los datos personales, aprobado el 3 de mayo de 1999: WP 20 (5055/99). Todos los documentos aprobados por el Grupo de trabajo se pueden consultar en http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm
5 Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, aprobada el 23 de febrero de 1999: WP 17 (5093/98).
6 Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999: WP 25 (5085/99).
7 Las listas preparadas por terceros pueden crearse con datos recopilados directamente de los clientes o con datos reunidos en espacios públicos de Internet.
8 Este asunto se ha tratado en el Informe sobre envíos por correo electrónico y protección de datos personales, adoptado por CNIL el 14 de octubre de 1999, que se puede consultar en www.cnil.fr. Las secciones 2 y 3 del presente Dictamen se basan en cierta medida en dicho informe.
9 Documento de trabajo: Tratamiento de datos personales en Internet. Aprobado el 3.2.1999: WP 16 (5013/99).
10 Artículo 6 de la Directiva 95/46/CE.
11 Artículo 7 de la Directiva 95/46/CE.
12 Artículo 10 de la Directiva 95/46/CE.
13 Artículo 14 de la Directiva 95/46/CE.
14 Artículo 12 de la Directiva 97/66/CE. Incluso se podría afirmar que el uso del correo electrónico para la venta directa se considerará equivalente al uso de dispositivos de llamada automática, que sí precisa el consentimiento del interesado.
15 Artículo 10 de la Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia, DO L 144 de 4.6.97, p. 19 (el correo electrónico se incluye expresamente en el apartado 4 de su artículo 2 y en el anexo I). Se puede consultar en http://www.europa.eu.int/eur-lex/en/lef/dat/1997/en_397L0007.html
16 Artículo 4 de la Directiva 95/46/CE.
17 Véase el artículo 12 de la Directiva 97/66/CE. 18 Véase el considerando 6a de la Propuesta modificada, nota 1. 19 Artículo 10 de la Directiva 95/46/CE.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

Grupo de trabajo sobre protección de datos del artículo 29

MEMORIA DE 2000 - ANEXO IX - DICTAMEN 2/2000 SOBRE LA REVISIÓN GENERAL DE LA NORMATIVA DE TELECOMUNICACIONES

Presentado por el Grupo operativo sobre Internet Aprobado el 3 de febrero de 2000 **Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones**

Introducción

El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales 1 ha tomado nota de la Comunicación de la Comisión Europea 2 sobre la revisión de la normativa vigente en el sector de las comunicaciones europeo.

Tras la consulta pública realizada por la Comisión Europea hasta el 15 de febrero de 2000, el Grupo de trabajo desea resaltar la importancia de las cuestiones que se plantearon.

Además, desea manifestar su deseo de participar y realizar aportaciones constructivas a la revisión de la normativa del sector de las telecomunicaciones.

Cuestiones pertinentes sobre protección de datos en el contexto de la revisión general

Dentro de la revisión general prevista de la normativa del sector de las telecomunicaciones, también se revisará y actualizará la Directiva en vigor sobre tratamiento de los datos personales y protección de la vida privada en el sector de las telecomunicaciones 3 . El apartado 3 del artículo 14 de dicha Directiva establece que el Grupo de trabajo establecido en la Directiva 95/46/CE ejercerá sus funciones también por lo que se refiere a la protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las telecomunicaciones, que son objeto de la Directiva 97/66/CE.

El artículo 30 de la Directiva general sobre protección de datos define los cometidos del Grupo de trabajo. Uno de ellos es asesorar a la Comisión Europea sobre cualquier proyecto de modificación de la Directiva o cualquier proyecto de medidas nuevas o especiales para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de los datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades.

En dictámenes anteriores, el Grupo de trabajo subrayó la necesidad de tener en cuenta los nuevos avances tecnológicos 4 , que podrían poner en peligro la protección de los datos personales y el derecho a la vida privada.

En este sentido, el Grupo de trabajo acoge favorablemente la actualización de esta Directiva en la medida en que permite abordar de manera más específica los problemas de protección de datos en el sector de las telecomunicaciones al tiempo que mantiene y, en caso necesario, mejora en actual nivel de protección.

Sin embargo, no se debe olvidar que la Directiva específica 97/66/CE se limita a completar la Directiva general 95/46/CE estableciendo disposiciones jurídicas y técnicas concretas 5 . Al revisar la Directiva específica, será necesario tener en cuenta, respetar y ser coherente con las disposiciones de la Directiva general sobre protección de datos 95/46/CE, que se aplica siempre al tratamiento de datos personales en este ámbito, independientemente de los medios técnicos utilizados.

Obviamente, la Directiva específica no sólo debe proteger los derechos fundamentales de las personas, sino que también debe tener en cuenta otros intereses legítimos, como los de secreto e integridad de las telecomunicaciones públicas.

El texto de la Comunicación de la Comisión Europea destaca que la revisión prevista prestará especial atención a la terminología utilizada por la Directiva 97/66/CE para dejar claro que los servicios y tecnologías nuevos están cubiertos por ella y evitar así posibles ambigüedades, facilitando la aplicación uniforme de los principios de protección de datos.

El Grupo de trabajo acoge favorablemente esta revisión de la terminología para tales fines.

Como bien se indica en la Comunicación de la Comisión Europea, la normativa de telecomunicaciones debería aplicarse a los servicios de Internet de la misma manera que se aplica a otras formas de comunicación.

El Grupo de trabajo abordó ya esta cuestión en dictámenes anteriores y ha afirmado claramente que el tratamiento de los datos personales en Internet tiene que respetar los principios de protección de los datos exactamente igual que se hace fuera de línea 6 . Por tanto, el tratamiento de los datos personales en Internet debe considerarse desde la perspectiva de las dos Directivas sobre protección de datos.

El Grupo de trabajo, y en particular el Grupo operativo Internet creado en su seno, desearía poner al servicio de la Comisión sus conocimientos especializados sobre protección de datos para las cuestiones relacionadas con Internet que deben abordarse en el marco de la revisión general de la legislación del sector de las telecomunicaciones.

Otra interesante cuestión tratada en la Comunicación de la Comisión es el creciente impacto de los programas informáticos y las configuraciones tecnológicas controladas por ellos.

El Grupo de trabajo prestó cierta atención a este asunto en el pasado, en concreto en su Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware* 7 . En esta Recomendación, el Grupo de trabajo anima a la industria informática *(software* y *hardwar*e) a trabajar en productos de Internet que respeten la vida privada y que faciliten los instrumentos necesarios para ajustarse a la normativa europea sobre protección de datos.

El Grupo de trabajo considera que la función cada vez más importante del *software* en el campo de las telecomunicaciones debe tenerse en cuenta en la revisión de esta Directiva, especialmente al abordar las responsabilidades de todos agentes de las operaciones de tratamiento de datos.

La revisión de la Directiva también podría ser una buena oportunidad para volver a analizar las diversas responsabilidades que corresponden a los operadores de la red y los proveedores de servicios en este ámbito.

Uno de los objetivos de la revisión de la normativa del sector de las telecomunicaciones es desarrollar la legislación europea en una dirección tecnológicamente neutra. El Grupo de trabajo está de acuerdo con este objetivo. No obstante, esta intención no debería impedir al legislador europeo elaborar una normativa nueva que aborde de manera suficiente los problemas específicos planteados por los nuevos avances tecnológicos en este ámbito.

También desea destacar que la nueva directiva debería hacer hincapié en que todas las tecnologías, independientemente del tipo de medios técnicos empleados, deben respetar la vida privada y, cuando sea posible, protegerla.

Conclusión

En general, el Grupo de trabajo acoge con satisfacción la actualización de la Directiva 97/66/CE en la medida en que permite abordar de manera específica los problemas de protección de datos en el sector de las telecomunicaciones, al tiempo que mantiene o mejora, en su caso, el actual nivel de protección. El Grupo de trabajo concede gran importancia a conseguir un alto nivel de protección de datos en el sector de las telecomunicaciones y, en concreto, a garantizar el secreto y la integridad de las comunicaciones.

Al tiempo que favorece la actualización y mejora de la normativa de telecomunicaciones, el Grupo de trabajo desea destacar la importancia de que, en los Estados miembros, se incorpore a su debido tiempo la Directiva en vigor sobre el sector de las telecomunicaciones. Por tanto, el Grupo invita a la Comisión a indicar claramente en sus comunicaciones que la nueva normativa comenzará a ser de aplicación dentro de unos años y que, mientras tanto, los Estados miembros deben continuar redactando sus leyes de conformidad con la normativa vigente.

El Grupo de trabajo desea animar a la Comisión a que, en el proceso de revisión, tenga en cuenta todas las Recomendaciones, Dictámenes y documentos de trabajo preparados por él sobre las cuestiones tratadas en la Comunicación.

El presente Dictamen no pretende expresar la posición definitiva del Grupo de trabajo sobre la materia. El Grupo desea contribuir a la ampliación del debate sobre este asunto y proporcionar sugerencias concretas, si así se desea, sobre las próximas fases del procedimiento de revisión.

NOTAS:

1 Creado en virtud del artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995, p. 31. Se puede consultar en http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm
2 Documento COM (1999) 539.
3 Directiva 97/66/CE, de 15 de diciembre de 1997, DO L 24 de 30.1.1998.
4 Entre otros, en el Documento de trabajo *Tratamiento de datos personales en Interne*t, aprobado el 23 de febrero de 1999, documento 5013/99/ES/final WP 16. Todos los documentos aprobados por el Grupo de trabajo se pueden consultar en http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm
5 Para todos los asuntos que no están cubiertos específicamente en la Directiva 97/66/CE, tales como las obligaciones del controlador y los derechos de las personas, o los servicios de telecomunicaciones que no estén disponibles para el público, se aplica la Directiva 95/46/CE (véase el considerando 11 de la Directiva 97/66/CE).
6 Véase también la Declaración ministerial de la Conferencia de Bonn sobre Redes mundiales, junio de 1997, en http://www2.echo.lu/bonn/conference.html.
7 Recomendación 1/99, aprobada por el Grupo de trabajo el 23 de febrero de 1999, documento 5093/98/ES/final WP 1

7. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

MEMORIA DE 2000 - ANEXO X - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE LOS DATOS PERSONALES RECOMENDACIÓN 1/2000 SOBRE LA APLICACIÓN DE LA DIRECTIVA 95/46/CE APROBADA EL 3 DE FEBRERO DE 2000

EL GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE LOS DATOS PERSONALES

creado por Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 1 , Vistos los artículos 29 y los apartado 1 (a) y 3 del artículo 30 de la mencionada Directiva, Visto su reglamento interno y, en particular, sus artículos 12 y 14, Considerando que entre los objetivos que asigna a la Comunidad el Tratado, modificado por el Tratado de Amsterdam, se incluye el de crear una unión cada vez más estrecha entre los pueblos de Europa, facilitar el progreso económico y social mediante una acción común encaminada a suprimir los obstáculos que dividen Europa, fomentar la mejora constante de las condiciones de vida de las personas, conservar y fortalecer la paz y la libertad, y fomentar la democracia sobre la base de los derechos fundamentales reconocidos en el Tratado, las constituciones y las leyes de los Estados miembros, así como en el Convenio Europeo de Protección de los Derechos Humanos y Libertades Fundamentales; Considerando que en la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos se insta a los Estados miembros a proteger los derechos y libertades fundamentales de la persona y, en particular, su derecho a la vida privada en lo que toca al tratamiento de los datos personales; Considerando que la Directiva forma parte de las medidas comunitarias que son necesarias para suprimir los obstáculos a los flujos de datos personales en las diversas esferas de actividad económica, administrativa y social del Mercado Interior; que a este efecto, la Directiva pretende armonizar las normativas sobre tratamiento de datos personales garantizando un elevado nivel de protección en la Comunidad; Considerando que el Consejo y el Parlamento Europeo acordaron unánimemente que la Directiva se incorporase en los ordenamientos nacionales hasta el de 24 de octubre de 1998, **ha aprobado la presente recomendación:**

El Grupo de trabajo señala que buena parte de los Estados miembros no ha promulgado todavía la legislación necesaria para incorporar la Directiva 95/46/CE en el Derecho nacional 2 . El Grupo de trabajo, que se creó por Directiva 95/46/CE, es el órgano independiente de asesoramiento a la UE en materia de protección de datos y vida privada 3 . Su mandato principal es analizar cualquier problema relacionado con la aplicación de las medidas nacionales aprobadas de conformidad con la Directiva para contribuir a su aplicación uniforme 4 . El Grupo de trabajo lamenta que no todos los Estados miembros hayan incorporado la Directiva a su debido tiempo. La consecuencia de este retraso es la persistencia de regímenes divergentes, que perpetúan la inseguridad jurídica en lo relativo a las obligaciones de los responsables del tratamiento de datos personales (empresas y administraciones públicas) y a los derechos de los particulares.

En los trabajos que ha realizado hasta la fecha 5 , el Grupo de trabajo ha fundamentado sus consideraciones en la Directiva y, en la medida de lo posible, en las disposiciones nacionales de aplicación. No obstante, el Grupo de trabajo sólo puede dar plena eficacia a su mandato y, por consiguiente, contribuir a la aplicación uniforme de las medidas nacionales para facilitar el libre flujo de los datos personales dentro y fuera de la Unión, si tiene un conocimiento preciso de las normas nacionales.

El Grupo de trabajo desea llamar la atención también sobre los esfuerzos que han hecho algunos países terceros para proteger el derecho fundamental a la vida privada en su ámbito de jurisdicción y, por añadidura, proporcionar un nivel adecuado de protección en las transferencias de datos personales realizadas desde la Unión Europea 6 , como exige la Directiva.

Al Grupo de trabajo le preocupa que en aquellos países en que no se haya hecho tal esfuerzo, y en ausencia de incorporación de la Directiva, las transferencias de datos personales puedan originar vulneraciones de los derechos y libertades fundamentales de la persona garantizados por dicha Directiva.

Dadas las circunstancias mencionadas, el Grupo de trabajo recuerda a los Estados miembros la vital importancia que tiene su obligación de cumplir la Directiva para la protección de los derechos y libertades fundamentales. El Grupo de trabajo tiene conocimiento de las actuaciones emprendidas por la Comisión Europea, que ha abierto procedimiento de infracción contra los Estados miembros que han incumplido la obligación de notificar las medidas de incorporación 7 , y apoya plenamente todo esfuerzo encaminado a garantizar una rápida incorporación de la Directiva.

El Grupo de trabajo recomienda por tanto a los Estados miembros, a sus gobiernos y sus parlamentos la adopción urgente de las medidas necesarias para que la Directiva se incorpore al Derecho nacional tan pronto como sea posible.

NOTAS:

1 Diario Oficial n§ L 281 de 23/11/1995, p. 31; se puede consultar en: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm
2 Véase el cuadro de la DG Mercado Interior sobre la aplicación de la Directiva, disponible en la dirección Internet señalada en la nota 1.
3 Véase la segunda frase del apartado 1 del artículo 29 de la Directiva 95/46/CE.
4 Véase el apartado 1 (a) del artículo 30 de la Directiva 95/46/CE.

5 Véanse los dictámenes, recomendaciones y documentos de trabajo aprobados por el Grupo de Trabajo, en las señas Internet de la nota 1.
6 Véase el principio de protección adecuada que se establece en el apartado 1 del artículo 25 de la Directiva 95/46/CE. Véanse asimismo, los dictámenes 5/99, relativo al nivel de protección en Suiza, y el dictamen 6/99 relativo al nivel de protección en Hungría, así como los dictámenes 1/99, 2/99 y 4/99 y demás documentos relativos al diálogo con los Estados Unidos sobre el ® Puerto seguro ¯. Pueden consultarse también en las señas Internet de la nota 1. En la actualidad, muchos otros países refuerzan o desarrollan sus políticas de protección de los datos y de la vida privada.
7 Véase el apartado 4 del artículo 32 de la Directiva 95/46/CE. La Comisión ha enviado dictámenes motivados a los Estados miembros incumplidores y se prepara para continuar el procedimiento (véase el comunicado de prensa de 29 de julio, que se puede consultar en las señas Internet de la nota 1).

8. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

MEMORIA DE 2000 - ANEXO XI - GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado en virtud del artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 1 , Vistos el artículo 29 y los apartados 1, letra (a), y 3 del artículo 30 de dicha Directiva Visto su reglamento interno y, en particular, sus artículos 12 y 14, **ha aprobado el presente dictamen:**

Durante los dos últimos años, el Grupo de trabajo ha dedicado buena parte de su tiempo a debatir el Acuerdo de Puerto Seguro, dada la importancia de esta cuestión para la protección de los ciudadanos europeos en lo que respecta al tratamiento de datos personales. En cada fase de los debates, el Grupo de trabajo ha aprobado los dictámenes oportunos sobre los documentos disponibles. El último se refiere a las versiones de los documentos disponibles en noviembre (Dictamen 7/99, aprobado el 3 de diciembre), que no se consideraron satisfactorias.

Antes de que la versión final del acuerdo se presente al Comité del artículo 31, el Grupo de trabajo espera tener la oportunidad de estudiar todos los documentos y de expresar su punto de vista sobre la adecuación del régimen estadounidense al artículo 30.1(b) de la Directiva.

El Grupo de trabajo invita por tanto al Comité del artículo 31 y a la Comisión a velar por que las fases finales de este importante proceso se acometan sólo a la luz del dictamen final del Grupo de trabajo, ya que su resultado tendrá importantes consecuencias para las autoridades nacionales representadas en él.

El Grupo de trabajo recuerda que algunos parlamentarios europeos han solicitado ver el dictamen final del Grupo de trabajo antes de que el Parlamento exprese su punto de vista.

NOTAS:

1 DO L 281 de 23.11.1995, p. 31. Se puede consultar en http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

MEMORIA DE 2000 - ANEXO XII - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 DICTAMEN 4/2000 SOBRE EL NIVEL DE PROTECCIÓN QUE PROPORCIONAN LOS "PRINCIPIOS DE PUERTO SEGURO" APROBADO EL 16 DE MAYO DE 2000 SOBRE EL NIVEL DE PROTECCIÓN QUE PROPORCIONAN LOS "PRINCIPIOS DE PUERTO SEGURO"

Introducción

El presente dictamen se refiere a los principios de puerto seguro y a las preguntas más frecuentes (FAQ) transmitidos por los servicios de la Comisión el 27 de abril y el 2 de mayo, y otros documentos recibidos entre el 9 y el 11 de mayo.

El Grupo de trabajo considera que se han hecho avances considerables en la mejora de la protección de los datos personales tras dos años de conversaciones con el Departamento estadounidense de Comercio, y que podrían hacerse todavía algunos avances en algunos de los problemas fundamentales. En particular, observa que las últimas modificaciones de los principios y los documentos relacionados incorporan algunas de las sugerencias formuladas por el Grupo de trabajo en anteriores dictámenes.

Para elaborar el presente dictamen, el Grupo de trabajo ha tenido también en cuenta la "Respuesta del Departamento estadounidense de Comercio" a su dictamen 7/99 1 , recibida por fax el 26 de abril.

El Grupo de trabajo recuerda que la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales forma parte de las "libertades y derechos fundamentales": esta dimensión, ya consagrada en el Convenio Europeo para la Protección de los Derechos Humanos y que se recoge en el artículo 1 de la Directiva 95/46, se ve confirmada por la orientación de los trabajos del Convenio sobre la Carta de los Derechos Fundamentales de la Unión Europea. El Grupo de trabajo reafirma su opinión de que, para que sea adecuado, un sistema de protección de datos debe satisfacer los criterios que resume en su documento de trabajo de 24 de julio de 1998 (WP 12).

Asimismo, el Grupo de trabajo recuerda que los Estados Unidos han firmado las Directrices sobre protección de la vida privada *(Privacy Guideline*s) de la OCDE (1980), y volvieron a ratificar su apoyo a las mismas en la Conferencia Ministerial de Ottawa.

El Grupo de trabajo desea destacar el impacto de la Directiva 95/46 en el contexto internacional. El Grupo de trabajo es consciente de la importancia económica y comercial del acuerdo de puerto seguro. No obstante, está convencido de que dichas consideraciones no pueden prevalecer sobre los derechos fundamentales de las personas en relación con el tratamiento de sus datos personales.

Por otro lado, también es importante tener en cuenta las consecuencias de cualquier decisión sobre el nivel de adecuación para las futuras negociaciones en foros internacionales como la OMC. El Grupo de trabajo suscribe la afirmación, hecha en el proyecto de carta de los servicios de la Comisión al Departamento de Comercio, de que el ordenamiento jurídico estadounidense tiene características muy específicas y no sienta precedente: el Grupo de trabajo concuerda con los servicios de la Comisión en la preferencia por las normas de carácter imperativo, cuyas principales referencias son la Directiva y las Orientaciones de la OCDE El Grupo de trabajo ha formulado ya sus observaciones sobre todas las versiones publicadas en las diversas fases del diálogo. En particular, el Grupo de trabajo ha emitido los siguientes dictámenes 2 :

* Dictamen 1/99 de 26 de enero de 1999 (WP 15);

* Dictamen 2/99 de 3 de mayo de 1999 (WP 19);

* Dictamen 4/99 de 7 de junio de 1999 (WP 21) al que complementa el documento de trabajo de 7 de julio de 1999 (WP 23);

* Dictamen 7/99 de 3 de diciembre de 1999 (WP 27).

Tras examinar la nueva versión de los documentos recibidos el 28 de abril y 2 de mayo, el Grupo de trabajo confirma sus anteriores dictámenes y considera esencial que se tengan debidamente en cuenta las siguientes cuestiones y recomendaciones:

1. ALCANCE

1.1 Legislación aplicable

En su dictamen 7/99, el Grupo de trabajo ya puso de relieve los posibles malentendidos que podrían derivarse del principio de notificación y expresó su preocupación por la posibilidad de que los responsables del tratamiento interpreten erróneamente que los principios de puerto seguro sustituyen a las disposiciones legislativas de los Estados miembros. El Grupo de trabajo sugirió, por consiguiente, que se esclareciera la cuestión en una FAQ específica. Esta sugerencia no se ha tenido en cuenta y el apartado 2 de los principios (versión de 28 de abril) se ha modificado de una forma que no aclara la cuestión. No obstante, en su Respuesta al dictamen 7/99, el Departamento estadounidense de

Comercio declara que "claramente, la legislación europea regulará todos los aspectos relativos a la recogida y utilización de información personal por parte de las empresas que operan en Europa". El Grupo de trabajo recuerda que, en el marco de la Directiva (apartado 1 del artículo 4), los Estados miembros deberán aplicar las disposiciones nacionales no sólo a todo tratamiento de datos personales efectuado por responsables del tratamiento establecidos en el territorio del Estado miembro, sino también cuando los responsables del tratamiento (aunque no estén establecidos en su territorio) recurran a medios situados en el territorio de dicho Estado miembro, especialmente para recoger datos personales. El Grupo de trabajo invita a la Comisión a dejar claro, en la propuesta de decisión o en la carta que remitirá al Departamento de Comercio, que el puerto seguro no tendrá efectos sobre la aplicación del artículo 4 de la Directiva.

1.2 Transferencias de datos no sujetas a una jurisdicción similar a la FTC

De acuerdo con el proyecto de Decisión elaborado por los servicios de la Comisión (letra b) del apartado 1 del artículo 1), estar sujeto a la jurisdicción de un organismo similar a la FTC es una de las condiciones que deben cumplir las entidades estadounidenses que deseen beneficiarse del puerto seguro. Dado que la adhesión al puerto seguro se basa en la autocertificación, sin que exista ningún tipo de verificación a priori, las facultades de supervisión de un organismo público son esenciales para la credibilidad del acuerdo.

En su dictamen 7/99, el Grupo de trabajo ya señaló que, de acuerdo con la correspondencia de la FTC dirigida a los servicios de la Comisión, la jurisdicción de la FTC abarca únicamente *actos desleales o fraudulentos si afectan al comercio* y que sectores como los servicios financieros (bancos y entidades aseguradoras), las telecomunicaciones, los transportes, las relaciones laborales y las actividades no lucrativas quedan excluidas de sus competencias. En consecuencia, el Grupo de trabajo está de acuerdo con la nueva redacción del proyecto de Decisión de la Comisión (letra b) del apartado 1 del artículo 1), según el cual en un nuevo anexo 3 se recogerán todos los organismos públicos estadounidenses que satisfacen los criterios de la letra b) del apartado 1 del artículo 1, y que los sectores u operaciones de tratamiento no sujetos a la jurisdicción de los organismos enumerados no entrarán en el ámbito de aplicación de la Decisión (tal como se indica en el considerando 9).

Por otro lado, el Grupo de trabajo observa que en la versión de los principios de 28 de abril las entidades no sujetas a la *Federal Trade Commission Act* puedan participar en los beneficios del puerto seguro sin que tengan claramente la obligación de autocertificarse ante el Departamento de Comercio, por lo que considera necesario eliminar esta ambigüedad volviendo a insertar el texto borrado.

Respecto a la FAQ 13 (reservas de billetes de avión), el Grupo de trabajo ha examinado el proyecto de carta al Departamento de Transporte de 9 de mayo y observa que se hace referencia a la posibilidad de presentar recursos individuales, así como a la intención de notificar al Departamento de Comercio las acciones emprendidas.

En estas condiciones, el Grupo de trabajo no se opone a la inclusión del Departamento de Transporte en la lista a que hace referencia la letra b) del apartado 1 del artículo 1, siempre que se reúnan las condiciones establecidas en el artículo 1 de la propuesta de decisión.

Respecto a los datos laborales, el Grupo de trabajo observa que, de acuerdo con la versión de 28 de abril de la FAQ 6, "si la entidad desea que los beneficios de puerto seguro cubran la información sobre recursos humanos (...)

la entidad deberá indicarlo en su carta y declarar su compromiso a cooperar con la autoridad comunitaria (...) de conformidad con la FAQ 9 y la FAQ 5". No obstante, la respuesta a la pregunta 1 de la FAQ 9 dice así: "Los principios de puerto seguro solamente son pertinentes cuando se transfieran registros identificados de manera individual." El Grupo de trabajo recuerda que, en línea con la Directiva, los principios de puerto seguro definen como datos personales toda información sobre una persona física identificada o identificable, y considera necesario que la FAQ 9 se ajuste a la definición correcta. También preocupa al Grupo de trabajo que la ejecución de las normas sobre datos laborales dependa sólo de la cooperación de las autoridades de protección de datos y no de los organismos de resolución alternativa de litigios

1.3 Fusiones, adquisiciones y quiebras

Como norma general, las disposiciones legislativas se aplican a toda entidad establecida en el territorio de un país o Estado determinado. Los principios de puerto seguro se aplicarán únicamente a aquellas entidades que se hallan adherido voluntariamente, lo cual plantea cuestiones específicas que se resumían en el dictamen 7/99 del Grupo de trabajo. El Grupo de trabajo acoge favorablemente las mejoras introducidas en la FAQ 6 (nuevo apartado añadido el 28 de abril). En la "nueva economía", las fusiones, adquisiciones y quiebras son acontecimientos cotidianos. En su dictamen 7/99 (página 5 de la versión española), el Grupo de trabajo invitaba a la Comisión a considerar la eliminación o supresión de los datos transmitidos por antiguos participantes en el puerto seguro, y observa con satisfacción que se ha tenido en cuenta la sugerencia.

2. EXCEPCIONES

* **2.1** El Grupo de trabajo lamenta que los principios de puerto seguro se vean debilitados, por un lado, por una serie de excepciones introducidas por las preguntas más frecuentes y, por otro, por el apartado 5 de los principios (la adhesión a estos principios puede limitarse por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas).

Respecto al último punto, el Grupo de trabajo reitera su opinión 3 de que la adhesión a los principios solamente debería limitarse en la medida necesaria en caso de conflictos de obligaciones y que, por motivos de transparencia y seguridad jurídica, el Departamento de Comercio debería informar a la Comisión de toda normativa legal o administrativa que pueda influir negativamente en la adhesión a los principios.

Las autorizaciones explícitas sólo se podrán aceptar como motivo de excepción si los legítimos intereses esenciales que subyacen en tales autorizaciones no difieren sustancialmente de las excepciones y exenciones que conceden los Estados miembros de la UE en situaciones comparables, conforme a las disposiciones por las que hayan incorporado la Directiva.

Respecto a las excepciones introducidas por las FAQ, el Grupo de trabajo opina lo siguiente:

* **2.2** Datos de dominio público (FAQ 15): el Grupo de trabajo reitera su parecer de que una excepción para la información extraída de registros públicos y la información de dominio público no se ajusta a los instrumentos internacionales sobre protección de datos y, en particular, a las Directrices de la OCDE 4 . Observa que se ha modificado la redacción y que ello puede contribuir a evitar que se abuse de la excepción pero lamenta que no se haya intentado definir con mayor precisión la categoría de información cubierta. Por otro lado, el Grupo de trabajo recuerda que el acuerdo de puerto seguro no puede prevalecer sobre el marco jurídico existente en relación con la responsabilidad (ya se trate de Derecho civil o de Derecho consuetudinario), ni prever que "las entidades no tendrán ninguna responsabilidad" (tal como dice el apartado 3 de la respuesta a la FAQ 15, que por tanto debería suprimirse).

* **2.3** Acceso (FAQ 8): el Grupo de trabajo confirma las objeciones ya señaladas en su dictamen 7/99 (página 9 de la versión española) ante la larga lista de excepciones prevista en la sección 5. Cabe señalar al respecto que similares objeciones figuran en la presentación del Diálogo Transatlántico de los Consumidores (DTAC) 5 . El Grupo de trabajo considera que el recurso a excepciones deberá controlarse cuidadosamente y que debería buscarse la cooperación con las autoridades estadounidenses para garantizar que las excepciones no se utilicen de forma que debiliten la protección que proporcionan los principios. En particular, el Grupo de trabajo opina que en un sistema adecuado de protección de datos el derecho de acceso no puede limitarse o denegarse de forma incompatible con la Directiva.

3. PRINCIPIOS

3.1. ACCESO

El principio de puerto seguro no incluye el derecho a recibir datos "de forma fácilmente inteligible", como es el caso de las directrices de la OCDE ("principio de participación individual"). El Grupo de trabajo toma nota de las garantías dadas por el Departamento de Comercio (en su respuesta al dictamen 7/99) de que ello va implícito en el principio.

El principio de acceso prevé el derecho a suprimir la información únicamente si es inexacta y no cuando la información se recoja o se trate sin el consentimiento del interesado o de una manera incompatible con los principios. La obligación de suprimir los datos en este último caso, tal como recomendó el Grupo de Trabajo en su dictamen 7/99, es ahora una de las posibles sanciones en el apartado relativo a las "vías de recurso y sanciones" de la FAQ 11. El Grupo de Trabajo recomienda que, en lugar de dejarse a la discreción de los organismos responsables de la resolución de litigios (tal como se indica en la nota a pie de página correspondiente de la FAQ 11), la supresión se reconozco como un derecho individual o un deber de la organización del puerto seguro.

3.3. Opción

Respecto a los cambios en la utilización de los datos, actualmente se ofrece a los interesados la posibilidad de decidir la no divulgación *(opt-out*) si la información personal que les afecta se utiliza con fines incompatibles con los objetivos originalmente especificados. El principio debería ampliarse para incluir todos los usos diferentes de los datos personales.

Por otra parte, la posibilidad de *opt-out*) que ofrece el principio de opción debería ampliarse a aquellos casos de transferencia de datos a otros responsables del tratamiento, incluso si no se produce cambio de uso o de finalidad El Grupo de trabajo acoge favorablemente la norma actual relativa a la aceptación *(opt-i*n) en caso de información delicada, pero considera necesario que en los principios se defina claramente y sin reservas la categoría de datos que se consideran delicados.

La última frase del principio de opción debe aclararse: las palabras ® en cualquier caso ¯ deben sustituirse por ® además ¯. El Grupo de trabajo recomienda también que se aclare más el principio de finalidad y el concepto de opción.

3.3. Transferencia ulterior

La versión actual de los principios de puerto seguro permite las transferencias a terceros que no participen en el puerto seguro si éstos firman un acuerdo de protección de los datos. Este enfoque no es coherente con la normativa general destinada a garantizar la aplicación y la responsabilidad de las entidades dentro del sistema de puerto seguro. El Grupo de trabajo opina que, en estas condiciones, las transferencias ulteriores sólo pueden permitirse con el consentimiento del interesado.

4. APLICACIÓN

Como se recuerda en el artículo 1 de la Directiva y el Convenio Europeo para la Protección de los Derechos Humanos, el derecho a la vida privada constituye un derecho fundamental y toda persona tiene derecho a ser oída ante un organismo independiente. El puerto seguro permite la transferencia de datos personales tratados actualmente en la UE a un país en el que las garantías mencionadas pueden no existir. Por tanto, una cuestión clave es saber cómo se protegería el derecho fundamental a la vida privada en relación con los datos transferidos a los Estados Unidos si no se respetaran los principios de puerto seguro.

Según la última versión de los documentos estadounidenses, la aplicación de los principios se garantiza a dos niveles: 1. por un lado, la resolución alternativa de litigios (aunque los organismos existentes citados por los Estados Unidos parecen cubrir únicamente las actividades "en línea": BBB online, Webtrust y Trust-e); 2. por otro lado, la facultad de la *Federal Trade Commission* de tomar medidas provisionales, tal como ha explicado en tres cartas separadas el presidente de la FTC.

El "puente" entre estas dos alternativas es poco claro: según la FAQ 11, los organismos de resolución de litigios *deberían* notificar a la FTC los casos de incumplimiento de los principios, pero no tienen la obligación de hacerlo. Aunque las personas afectadas pueden presentar una queja directamente a la FTC, no existen garantías de que ésta examine su caso (tiene potestad discrecional). En concreto, los particulares no tienen derecho a ser oídos ante la FTC ni a hacer cumplir las decisiones de los organismos de resolución alternativa de litigios ni a recurrir dichas decisiones (o la no adopción de las mismas). En consecuencia, a las personas afectadas por una presunta violación de los principios se les garantizaría el derecho a recurrir a una instancia independiente 6 .

El proyecto de Memorando del Departamento de Comercio se refiere a la posibilidad de que los particulares accedan a los tribunales estadounidenses y reciban reparación por daños morales dentro de ciertas circunstancias, pues la experiencia muestra que este tipo de daño es el característico cuando se vulnera el derecho a la vida privada. Ambos aspectos habrán de revisarse a la luz de la experiencia, para dilucidar la eficacia de las vías de recurso que se indican en el mencionado Memorando.

En general, el Grupo de trabajo considera que este régimen adolece de insuficiencia en dos de las tres condiciones que indica en su documento de trabajo de 24 de julio de 1998: la necesidad de "ofrecer apoyo y asistencia a los interesados" (letra b) y de "ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas" (letra c).

Conclusiones

El Grupo de trabajo observa que la resolución propuesta sobre la adecuación se refiere a un sistema que todavía no es operativo. A este respecto, el Grupo de trabajo se congratula de la cláusula de revisión que aparece en la propuesta de Decisión de la Comisión, que permitirá revisar las resoluciones sobre adecuación a la luz de la experiencia; además el Grupo de trabajo considera necesario ratificar su dictamen de 7/99 en lo relativo al denominado "período de gracia" y confirma sus reservas sobre esta parte del proyecto de intercambio de cartas (el Grupo de trabajo observa que el borrador de carta de los servicios de la Comisión hace referencia a "extractos adjuntos del acta del Comité del artículo 31, a los que hasta ahora no se ha tenido acceso; el Grupo estaría interesado en recibirlos).

A tenor de lo anteriormente expuesto, y teniendo en cuenta el compromiso de los Estados Unidos con la protección de la vida privada a que hace referencia la respuesta del Departamento de Comercio al dictamen 7/99, el Grupo de Trabajo sigue preocupado por varios aspectos en los que piensa que habría sido posible conseguir un mayor nivel de protección de los datos. En particular, **al Grupo de Trabajo le preocupa que se introduzcan mejoraras para conseguir los siguientes objetivos:**

* claridad absoluta sobre el alcance del puerto seguro: por un lado, en términos de la legislación aplicable y, por otro, en términos de la jurisdicción de la FTC (apartado 1 del presente dictamen);
* limitación del número de excepciones según lo indicado en el punto 2 del presente dictamen;
* más mejoras de los principios tal como se indica en el punto 3;
* garantías adecuadas de recurso a título individual, tal como se indica en el punto 4.

Si se toma la decisión de seguir adelante, el Grupo de trabajo concederá particular relieve al valor de los mecanismos de revisión de la decisión y demás garantías.

Por último, e independientemente de la decisión que se adopte sobre el puerto seguro, el Grupo de trabajo insta a los servicios de la Comisión a finalizar sus trabajos y a presentar una decisión sobre las cláusulas de los contratos tipo (apartado 4 del artículo 26 de la Directiva), con el fin de crear un marco previsible, seguro y no discriminatorio para las transferencias de datos internacionales que no se limite a un único tercer país. Además, el Grupo de trabajo invita a la Comisión a considerar con urgencia la creación de un sistema de sello comunitario para los sitios Internet basado en criterios comunes de evaluación de la protección de los datos que pueda determinarse a escala comunitaria.

NOTAS:

1 Los documentos que se citan en el presente Dictamen pueden solicitarse en la Secretaría del Grupo de trabajo (véase cubierta).
2 Todos los documentos aprobados por el Grupo de trabajo están disponibles en: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm
3 Dictamen 7/99, página 6 de la versión española
4 Los principios aplicables a la información pública han sido desarrollados por el Grupo de trabajo del artículo 29 en su dictamen 3/99 sobre la información del sector público y la protección de datos personales, aprobado el 3 de mayo de 1999.
5 "Las excepciones al suministro de acceso son demasiado amplias y limitan indebidamente el acceso de los particulares en favor de los intereses comerciales. Si bien los derechos de acceso deberían sopesarse teniendo en cuenta al mismo tiempo otras consideraciones, los actuales principios de acceso permiten a las entidades menos propensas a considerar los derechos del interesado -el recopilador de datos- adoptar tales decisiones"(...).
6 De acuerdo con la presentación ya mencionada por el Diálogo Transatlántico de los Consumidores, a pesar de los casos anteriores en los que la privacidad individual se había visto comprometida, ningún grupo autorregulado ha sometido a investigación a una empresa: en sus conclusiones, el DTAC recomienda que los negociadores del puerto seguro consideren una prioridad el derecho individual de reparación.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS -ARTÍCULO 29

MEMORIA DE 2000 - ANEXO XIII - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS -ARTÍCULO 29 DICTAMEN 5/2000 SOBRE EL USO DE LAS GUÍAS TELEFÓNICAS PÚBLICAS PARA SERVICIOS DE BÚSQUEDA INVERSA O MULTICRITERIO (GUÍAS INVERSAS) ADOPTADO EL 13 DE JULIO DE 2000 DICTAMEN SOBRE EL USO DE LAS GUÍAS TELEFÓNICAS PÚBLICAS PARA SERVICIOS DE BÚSQUEDA INVERSA O MULTICRITERIO (GUÍAS INVERSAS)

1. INTRODUCCIÓN

En el marco del proceso de liberalización del sector europeo de las telecomunicaciones, nuevas empresas están ofreciendo servicios que anteriormente sólo suministraban los operadores tradicionales de telecomunicaciones. Por lo tanto, cada vez con mayor frecuencia, se ofrecen nuevos productos, entre ellos las guías telefónicas en formato electrónico. Estas guías contienen los nombres, direcciones y números de teléfono de millones de ciudadanos europeos de diversos Estados miembros.

Disponibles en el mercado en diversos países europeos, las guías incluyen información sobre los ciudadanos del país en que está establecido el servicio o la empresa y sobre los de otros países de la UE. Los formatos más utilizados para entregar estos productos son los sitios Internet y el CD-ROM.

Una de las principales innovaciones que ofrece la publicación electrónica es la posibilidad de proporcionar, de forma práctica y a coste reducido, capacidades ampliadas para el tratamiento de la información que figura en las guías telefónicas. Estas capacidades se refieren, básicamente, a la posibilidad de utilizar criterios más amplios de búsqueda para revelar información que contiene la guía.

De hecho, estos productos generalmente ofrecen **servicios de búsqueda inversa o multicriterio,** es decir: aparte de los métodos tradicionales de búsqueda en una guía telefónica para averiguar el número de teléfono de un abonado específico a partir de su apellido, ejecutan otros nuevos servicios que van más allá de los métodos tradicionales de búsqueda, proporcionando métodos múltiples para acceder a los datos personales de una persona determinada o incluso de un grupo de personas cuyos datos personales respondan a los criterios de búsqueda.

Como ejemplo de las capacidades de estos nuevos tipos de búsqueda, cabe citar la posibilidad de obtener el nombre y la dirección de un abonado indicando su número de teléfono o de realizar búsquedas basadas en la dirección, que permiten encontrar el nombre y el número de teléfono de abonados introduciendo información sobre su dirección. Efectivamente, puede ser técnicamente posible obtener los nombres y los números de teléfono de todas las personas que viven en una zona determinada (por ejemplo, una calle).

Esta nueva funcionalidad podría implicar un cambio significativo en las expectativas de intimidad de los ciudadanos en relación con los datos personales que figuran en las guías telefónicas públicas. En realidad, antes de la existencia de estos nuevos productos, el hecho de que una persona comunicara su número de teléfono a un tercero no implicaba, en circunstancias normales, la posibilidad de obtener cualquier otra información adicional a partir de esos datos; en cambio ahora, al existir estos productos en el mercado, la situación ha cambiado radicalmente: la simple revelación, intencionada o casual, de un número de teléfono podría ser la clave de acceso a información como la que generalmente figura en una tarjeta de visita, incluidos el nombre y la dirección y, en algunos casos, la profesión y el empleo.

Por otra parte, el mero conocimiento de la factura telefónica detallada de un ciudadano, en la que aparecen los números de teléfono a los que ha llamado, permitiría obtener una lista de los nombres y direcciones de todas las personas a las que ha telefoneado durante un período específico de tiempo.

Además, debería tenerse en cuenta la existencia de otra categoría de productos que contienen información geográfica, como mapas de ciudades y bases de datos con fotografías de todas las viviendas de una ciudad. Esta información puede asociarse fácilmente a la dirección que aparece en una guía telefónica, lo que permite la búsqueda multicriterio. Tampoco hay que olvidar las enormes posibilidades que se derivan de la combinación de esta información con la procedente de otras fuentes, como los registros públicos. Así pues, la cantidad de información que se puede obtener a partir de un simple número de teléfono podría ir mucho más allá de lo que un ciudadano medio puede esperar

1.2. ANÁLISIS JURÍDICO

La Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones 2 establece en el considerando 21 lo siguiente: *"Considerando que las guías son ampliamente divulgadas y accesibles alpúblico; que el derecho a la intimidad de las personas físicas y el interés legítimo de laspersonas jurídicas exigen que los abonados puedan decidir en qué medida se publican sus datos personales en dichas guías; que los Estados miembros podrán reservar esta posibilidad a los abonados que son personas físicas".*

Además, el artículo 11 establece el principio de que los datos personales recogidos en las guías telefónicas deberán limitarse *"(...) a lo estrictamente necesario para identificar a un abonado concreto, a menos que el abonado haya dado su consentimiento inequívoco para que se publiquen otros datos personales".*

El artículo 11 también estipula que el abonado *"tendrá derecho, de forma gratuita, a quese le excluya de una guía*

impresa o electrónica a petición propia, a indicar que sus datos personales no se utilicen para fines de venta directa, a que se omita parcialmente su dirección y a que no exista referencia que revele su sexo, cuando ello sea aplicable lingüísticamente".

Por otro lado, la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos 3 , dispone en la letra b) del apartado 1 de su artículo 6 que los datos personales sean *"recogidos con fines determinados, explícitos y legítimos, y no sean tratadosposteriormente de manera incompatible con dichos fines".*

En este sentido, el fin de las guías telefónicas convencionales es revelar el número de teléfono de un abonado a partir del conocimiento del nombre de un abonado (la dirección es solamente necesaria en caso de homónimos). Y el uso de estos datos personales se limita a ese fin específico. Por lo tanto, utilizar las guías para averiguar datos personales relativos a la persona física a partir de un número de teléfono cuyo abonado es desconocido o los nombres y números de teléfono de las personas que viven en una zona determinada, constituye un uso totalmente diferente del que el consumidor puede esperar cuando se le incluye en la guía. Por lo tanto, se trata de una nueva finalidad que no es compatible con la inicial (véase la letra b) del artículo 6 de la Directiva 95/46/CE)4 .

Sin embargo, las búsquedas inversas pueden resultar útiles y no deberían prohibirse como tales. Para que este procedimiento sea leal y lícito, tienen que cumplirse las condiciones de las Directivas: Puesto que el uso de datos personales en las guías telefónicas públicas para los servicios de búsqueda inversa o multicriterio constituye un nuevo fin, los responsables del tratamiento deberán informar de ello a los interesados (artículos 10 y 11 de la Directiva 95/46/CE).

Además, para que sea legítimo, este proceso deberá cumplir uno de los criterios fijados en el artículo 7 de la Directiva 95/46/CE. Según la letra f) del artículo 7, el tratamiento de datos estará legitimado si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por terceros, siempre que no prevalezca sobre el interés del individuo de proteger sus derechos fundamentales.

Para conseguir el equilibrio de intereses, deben identificarse y evaluarse los intereses en juego y los riesgos para la vida privada. A este respecto, la Directiva 97/66/CE ofrece indicaciones útiles: siempre y cuando se trate de la información mínima necesaria para identificar a un abonado, esta información podrá incluirse en las guías telefónicas convencionales a menos que el abonado se oponga. Sin embargo, en cuanto intervienen informaciones adicionales o funciones complementarias de la guía telefónica pública, se requiere el consentimiento del interesado. En lo que respecta al uso de guías telefónicas públicas para búsquedas inversas o multicriterio, la situación es comparable y, además, tal procedimiento puede constituir una intrusión no esperada en la intimidad. Hay que considerar que el interés del individuo por ser protegido prevalece sobre el interés del responsable del tratamiento o de terceros. Por lo tanto, tal procedimiento es legítimo solamente si el interesado da su consentimiento informado antes de cualquier inclusión de sus datos personales en las guías telefónicas públicas para las búsquedas inversas o multicriterio (letra a) del artículo 7 y letra h) del artículo 2 de la Directiva 95/46/CE).

Esto significa en la práctica que

* deberá obtenerse un *consentimiento específico e informado* del abonado antes de la inclusión de sus datos personales en cualquier clase de guía telefónica pública (telefonía tradicional, telefonía móvil, correo electrónico, firma electrónica, etc.) utilizada para las búsquedas inversas o multicriterio.

* El responsable del tratamiento deberá informar al abonado *en especial sobre* <UL> <LI>el uso de los datos personales en las guías alfabéticas, </UL> - si prevé utilizar sus datos personales en servicios de búsquedas inversas o multicriterio y en qué medida (qué tipo de búsqueda multicriterio se autoriza), - su derecho a modificar, en cualquier momento y gratuitamente, su decisión de autorizar cada tratamiento de datos.

* El responsable del tratamiento deberá aplicar también las *medidas técnicas y de*

organización apropiadas en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse (véase el artículo 17 de la Directiva 95/46/CE). Esto significa, por ejemplo, que la base de datos debería diseñarse de manera que evite en la medida de lo posible usos fraudulentos, como modificaciones ilícitas de los criterios de búsqueda o la posibilidad de copiar o acceder a toda la base de datos para un tratamiento posterior (por ejemplo, los criterios de búsqueda deben ser lo suficientemente precisos para permitir únicamente la presentación de un número limitado de resultados por página). El resultado debería ser que el fin para el que el abonado dio su consentimiento se garantice también por medios técnicos.

Estas condiciones no se aplican solamente a los operadores de telecomunicaciones, sino también a otros actores, por ejemplo los editores, es decir, a *todos* los que desean utilizar datos personales para ofrecer guías o servicios de búsqueda multicriterio 5 .

CONCLUSIONES

A tenor de lo expuesto anteriormente y teniendo en cuenta el marco jurídico concebido por la Directiva 97/66/CE y la Directiva 95/46/CE, el Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales considera que el tratamiento de datos personales en las guías inversas o en los servicios de búsqueda

inversa o multicriterio sin el consentimiento inequívoco e informado del abonado es desleal e ilícito. Deberán cumplirse las condiciones expuestas anteriormente para que tal procedimiento sea lícito.

El Grupo de Trabajo acoge con satisfacción y apoya plenamente la propuesta de la Comisión Europea para un proyecto de Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas 6 , que tiene en cuenta en particular los diferentes usos posibles de las guías públicas electrónicas (como las funciones de búsqueda inversa). El proyecto de Directiva establece que el abonado deberá dar su consentimiento informado sobre si sus datos personales pueden incluirse en una guía pública, con qué fin específico y en qué medida.

De este modo, la propuesta de la Comisión adapta las normas a la realidad, puesto que en los nuevos servicios de comunicaciones electrónicas, como GSM y correo electrónico, la mayoría de los abonados no desean hacer públicos sus números de teléfono móvil ni sus direcciones electrónicas y la mayoría de los proveedores de servicios han respetado en la práctica los deseos de sus abonados por motivos económicos.

El Grupo de Trabajo seguirá contribuyendo al debate sobre todas las cuestiones relacionadas con este proyecto de Directiva 7 .

NOTAS:

1 Los representantes de las autoridades austríacas, danesas y portuguesas de protección de datos manifestaron que en sus países respectivos la práctica de las búsquedas inversas no ha planteado problemas específicos hasta la fecha. El representante danés se abstuvo en la votación.
2 Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. DO L 24 de 30 de enero de 1998, p. 1. Disponible en: http://158.169.50.95:10080/legal/en/dataprot/protection.html
3 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DO L 281 de 23 de noviembre de 1995, p. 31. Disponible en: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm
4 En la misma lógica, el Grupo Internacional de Trabajo sobre protección de datos en las telecomunicaciones (grupo de Berlín) adoptó en su reunión n§ 23 una posición común sobre las guías telefónicas inversas en la que declara que la existencia de guías telefónicas inversas, sin normas específicas de protección, puede constituir una grave amenaza para la intimidad. Además, la posición común señala que el fin de una guía inversa "(...) no es el mismo que el de una guía telefónica; una guía telefónica permite obtener el número de teléfono de una persona conocida, a partir de su nombre y de un criterio geográfico, mientras que el propósito de una guía inversa es la búsqueda de la identidad y la dirección de abonados de los que sólo se conoce su número de teléfono". Igualmente, el grupo de Berlín afirma que llevar a cabo la búsqueda inversa en una guía telefónica sin el consentimiento del interesado constituye una recogida desleal de información. Un dictamen similar más detallado fue adoptado por la Comisión belga de protección de datos en junio de 1999 *(Commission de la protection de la vie privé*e, recomendación n§ 01/1999, de 23 de junio de 1999, disponible en : http://www.privacy.fgov.be
5 Véase la definición de responsable del tratamiento en la letra d) del artículo 2 de la Directiva 95/46/CE.
6 Véase COM(2000) 385 final (adoptada el 12 de julio de 2000).

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

MEMORIA DE 2000 - ANEXO XIV - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 DICTAMEN 6/2000 SOBRE LA CUESTIÓN DEL GENOMA APROBADO EL 13 DE JULIO DE 2000

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado en virtud del artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 1 , vistos el artículo 29 y los apartados 1, letra a), y 3 del artículo 30 de dicha Directiva, visto su Reglamento interno y, en particular, sus artículos 12 y 14, **ha aprobado el presente Dictamen: Dictamen 6/2000 sobre el genoma humano y la vida privada** El establecimiento de un primer mapa de la secuencia del ADN acaba de ser anunciado públicamente por los participantes en el proyecto sobre el genoma humano *(Human Genome Project*).

El Grupo de Trabajo reconoce que este logro fundamental debería permitir diagnosticar y tratar las enfermedades de forma antes inimaginable.

En la presentación pública del 26 de junio se reconoció que los riesgos de uso abusivo del conocimiento genético suscitan una preocupación legítima sobre la protección de la vida privada. El Grupo de Trabajo comparte esta preocupación.

El desciframiento de la secuencia del ADN abre la vía a nuevos descubrimientos y usos en el ámbito de la experimentación genética. Por otro lado, la información puede permitir identificar las personas, relacionarlas entre sí, y revelar datos complejos sobre la salud y evolución futuras de estas personas y de otras con las que estén genéticamente relacionadas.

El Grupo de Trabajo desearía destacar la importancia del derecho fundamental a la protección de la vida privada y a la consiguiente necesidad de adecuar a ese derecho el desarrollo de las nuevas técnicas genéticas, mediante las medidas de protección más apropiadas.

Hecho en Bruselas el 13 de julio de 2000 Por el Grupo de Trabajo *El Presidente* Stefano RODOTA

NOTAS:

1 Diario Oficial L 281 de 23.11.1995, p. 31, disponible en inglés en la siguiente dirección: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm

GRUPO DE PROTECCIÓN DE DATOS PERSONALES DEL ARTÍCULO 29

MEMORIA DE 2000 - ANEXO XV - DICTAMEN 7/2000 SOBRE LA PROPUESTA DE LA COMISIÓN EUROPEA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVA AL TRATAMIENTO DE LOS DATOS PERSONALES Y A LA PROTECCIÓN DE LA INTIMIDAD EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS DE 12 DE JULIO DE 2000 COM (2000) 385 ADOPTADO EL 2 DE NOVIEMBRE DE 2000

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 1 , Vistos el artículo 29 y la letra a) del apartado 1 y el apartado 3 del artículo 30 de dicha Directiva, Visto su reglamento interno y, en particular, sus artículos 12, 13 y 14, **Ha adoptado el presente dictamen 7/2000: 1. Introducción** En el contexto de la revisión del marco regulador de las telecomunicaciones en la Comunidad llevada a cabo en 1999 2 , la Comisión adoptó, el pasado 12 de julio, diversas propuestas de nuevas Directivas sobre las comunicaciones electrónicas con las que se proyecta sustituir las disposiciones legislativas vigentes en la materia. Una de las cinco propuestas presentadas constituye una revisión de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Tras su dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones 3 , el Grupo de trabajo desea ahora contribuir a los debates del Parlamento y el Consejo sobre el proyecto de Directiva.

2. Análisis del proyecto de Directiva

Las principales preocupaciones del Grupo de trabajo giran en torno al tratamiento de los datos personales que se realizan en Internet o utilizando Internet como medio, cuestión que deberá abordarse de forma más específica, así como a los nuevos problemas creados por la liberalización del mercado de las telecomunicaciones.

Artículo 1 - Objetivo y ámbito de aplicación - Artículo 3 - Servicios afectados

El Grupo de trabajo entiende que no se propone ningún cambio en cuanto al ámbito de aplicación ni a los servicios afectados. Por lo tanto, las disposiciones específicas de la Directiva vendrían a aplicarse a la provisión de los servicios de comunicaciones electrónicas *públicamente* disponibles en las redes de comunicación *públicas* de la Comunidad. El tratamiento de datos personales para el uso de las redes cerradas o privadas recaería por lo tanto exclusivamente en el ámbito de aplicación de la Directiva general 95/46/CE. Esta solución no parece muy afortunada si se tiene en cuenta que las redes privadas están adquiriendo una importancia cada vez mayor en la vida cotidiana y las comunicaciones de los ciudadanos -en el contexto, por ejemplo, de su trabajo-, y los riesgos que esas redes plantean para la protección de la intimidad están aumentando y materializándose consiguientemente (por ejemplo, control del comportamiento de los empleados a través del tráfico de datos o falta de confidencialidad de las comunicaciones).

La nueva Directiva propuesta tampoco regula el tratamiento de los datos personales en relación con la prestación de *servicios* a través de las redes y los servicios públicos de comunicaciones 4 , como la radiodifusión y los servicios de la sociedad de la información.

Ello significa que, en el último de los casos citados, el tratamiento de datos sólo debe ajustarse a lo dispuesto en la Directiva 95/46/CE, al igual que todas las cuestiones no reguladas por la directiva específica sobre la protección de intimidad (véase el considerando n§ 9, idéntico al considerando correspondiente de la Directiva 97/66/EC).

No obstante, los servicios interactivos de televisión sí quedarían regulados por la nueva Directiva.5 Resultaría sumamente útil que estos puntos se aclarasen bien en el texto de los artículos correspondientes de las distintas Directivas, bien en los considerandos.

Artículo 2 - Definiciones

El Grupo de trabajo agradece todos los esfuerzos dirigidos a aclarar la terminología y observa que la Directiva propuesta incorpora la opinión por él expresada en el documento de trabajo "Tratamiento de los datos personales en Internet", según la cual ambas Directivas sobre protección de datos son plenamente aplicables al tratamiento de datos en Internet 6 .

Los "datos sobre tráfico" se definen como *"cualquier dato tratado en el curso de o a efectos de la transmisión de una comunicación a través de una red de comunicaciones electrónicas* ". Esta definición no contiene una cláusula de necesidad. En opinión del Grupo de trabajo, se trata de una solución muy positiva, pues implica que todos los datos sobre tráfico generados durante una comunicación, sean o no necesarios para establecer esa comunicación, deben destruirse una vez finalizada la misma (apartado 1 del artículo 6). La definición incluye asimismo los datos sobre localización generados durante la transmisión de una comunicación y los datos de navegación (como los URL o localizadores unificados de recursos), que pueden revelar intereses personales de los particulares (por ejemplo, sitios web que pueden ofrecer indicaciones sobre las creencias religiosas, las ideas políticas, la salud o la vida sexual de quienes los frecuentan). Al indicar exactamente las páginas de un sitio web que han sido visitadas, revelan el contenido exacto al que ha podido acceder el particular.

Puesto que los datos sobre tráfico pueden incluir este tipo de información personal, deberían estar revestidos de la

confidencialidad prevista para las comunicaciones (artículo 5 y siguientes).7 El Grupo de trabajo interpreta que la definición propuesta de "llamada" no incluye la telefonía vocal por Internet, sino únicamente la telefonía tradicional por conmutación de circuitos.

Aunque el Grupo de trabajo ha acogido favorablemente la definición de "llamada" que se ofrece en la Directiva propuesta, persiste en su opinión de que, en la Directiva 97/66/CE vigente, el concepto de "llamada" incluye la utilización de Internet. Según se desprende de la exposición de motivos del proyecto de Directiva, la Comisión Europea parece compartir esta opinión.

El Grupo de trabajo observa que ya no figura una definición del término "abonado", a pesar de que el término se emplea a lo largo del proyecto de Directiva. En su lugar, se define el término "usuario", que excluye a las personas jurídicas. El Grupo de trabajo desearía conocer las razones de estos cambios.

El proyecto de Directiva ha dejado de referirse a los "servicios de telecomunicaciones", optando en su lugar por la expresión "servicios de comunicaciones electrónicas". La exposición de motivos de la propuesta explica que este cambio era necesario para armonizar la terminología con la de la propuesta de Directiva relativa a un marco regulador de las redes y los servicios de comunicaciones electrónicas 8 .

El término "servicios de comunicaciones electrónicas" no se define en la propuesta de Directiva sobre protección de la intimidad, sino en la letra b) del artículo 2 de la propuesta de Directiva relativa a un marco regulador de las redes y los servicios de comunicaciones electrónicas.

La nueva definición reza como sigue: *"se entenderá por servicio de comunicaciones electrónicas el prestado contra remuneración que consiste, en su totalidad o principalmente, en la transmisión y encaminamiento de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante el uso de redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos"* .

De hecho, la nueva definición parte del mismo concepto básico que la anterior (transmisión y encaminamiento de señales a través de servicios de comunicaciones electrónicas), pero la lista de ejemplos de servicios incluidos y excluidos de la definición resulta sumamente útil al despejar en cierta medida las dudas planteadas en las secciones anteriores.

La lista incluida en la nueva definición permite concluir que los servicios que transmitan contenidos mediante el uso de redes y servicios de comunicaciones electrónicas quedan excluidos del ámbito de aplicación del proyecto de Directiva sobre protección de la intimidad. Semejante conclusión se confirma en el preámbulo de la propuesta de Directiva relativa a un marco regulador de las redes y los servicios de comunicaciones electrónicas, cuyo considerando n§ 7 afirma que *"es necesario separar la regulación de la transmisión de la regulación de los contenidos"* , precisando, no obstante, que esa separación no es óbice para que se tengan en cuenta los vínculos existentes entre ambas.

La principal consecuencia de tal separación es que los servicios adicionales como DoubleClick o los que suministran el contenido de un *portal* o un sitio web (pero no los albergan) no están cubiertos por esta Directiva, sino solamente por la Directiva general sobre protección de datos. También significa que los *proveedores de servicios de Internet* (PSI) sólo están regulados por la Directiva específica en la medida en que actúen como proveedores de acceso y conexión a Internet, quedando regulados por la Directiva general cuando actúen como proveedores de contenidos.

La ventaja de esta nítida separación entre la regulación de los contenidos y de la transmisión es la claridad que aporta. No obstante, no está claro que su aplicación práctica vaya a resultar tan fácil (por ejemplo en el caso de un *proveedor de servicios de Internet* que también suministre contenidos al albergar su propio *portal*. Semejante *PSI* debería en tal caso aplicar la Directiva general a todas sus actividades y la Directiva específica (que impone obligaciones especiales) a aquellas actividades para las que desempeñe el papel de proveedor de acceso.

Otro aspecto interesante de la nueva definición de "servicios de comunicaciones electrónicas" es la referencia al dato de que los servicios deben prestarse contra remuneración. Ni el preámbulo ni la exposición de motivos hacen alusión alguna a la inclusión de este término ni proporcionan directrices sobre cómo interpretarlo. Una de las interpretaciones posibles implicaría que los proveedores de acceso gratuito deben quedar fuera del ámbito de aplicación de la Directiva sobre telecomunicaciones y protección de la intimidad revisada ya que no reciben remuneración alguna (al menos no financiera) por parte de los usuarios de Internet.

Sin embargo, esta interpretación es incorrecta, ya que la jurisprudencia del Tribunal de Justicia acerca de los servicios en el sentido del artículo 50 (antiguo artículo 60) del Tratado CE 9 , sostiene que la remuneración no tiene por qué ser necesariamente pagada por los beneficiarios de los servicios, pudiendo correr, por ejemplo, a cuenta de los anunciantes.

En el caso de los proveedores de acceso gratuito, la remuneración procede de hecho de quienes colocan anuncios o carteles en las páginas de Internet.

Está por lo tanto claro que estos servicios quedan incluidos en la definición de servicios de comunicaciones electrónicas y, por lo tanto, en el ámbito de aplicación de la Directiva.

A pesar de todo, resultaría muy conveniente aclarar este punto en el texto de la Directiva, pues no todos los lectores del

texto conocen la interpretación de este término ofrecida por el Tribunal de Justicia de las Comunidades Europeas 10 .

Artículo 4 - Seguridad

El Grupo de trabajo ha acogido favorablemente la explicación ofrecida en el considerando n§ 13 acerca de las medidas de seguridad, como la técnica de cifrado.

Propone que se considere la necesidad de imponer obligaciones más específicas a los operadores de las redes y los prestadores de servicios partiendo de la base de un análisis de las disposiciones legales nacionales de aplicación de las normas de seguridad con el fin de facilitar la libre circulación de datos y equipo (software y hardware). Sería también útil especificar los riesgos existentes, no sólo en relación con Internet, sino también en otros entornos de comunicación, ya que las obligaciones en materia de seguridad incumben a todos los prestadores de redes y servicios.

Artículo 5 - Confidencialidad de las comunicaciones

El Grupo de trabajo desea recordar la opinión generalizada de que la confidencialidad de las comunicaciones constituye uno de los principales elementos de la salvaguardia del derecho fundamental a la protección de la intimidad y los datos personales y del secreto de las comunicaciones. En una sociedad democrática, toda excepción a este derecho-obligación debería limitarse a lo estrictamente necesario y definirse claramente en las leyes con arreglo a las condiciones fijadas en los artículos 15 y 13 de la Directiva 95/46/CE.

Dado que la formulación propuesta del apartado 2 del artículo 5 es excesivamente imprecisa y, por lo tanto, permite excepciones al principio de confidencialidad sin respetar las condiciones básicas, dicho apartado debería suprimirse.

A este respecto, el Grupo de trabajo desea recordar su Recomendación 2/99, en la que subrayaba lo siguiente: "los operadores de telecomunicaciones y los proveedores de servicios de telecomunicaciones deben adoptar las medidas necesarias con el fin de hacer técnicamente difíciles o imposibles, según el estado actual de la técnica, la intercepta- ción de las telecomunicaciones por instancias no autorizadas por la ley. El grupo destaca a este respecto que la aplicación de medios eficaces de interceptación de las comunicaciones con fines legítimos, utilizando precisamente las técnicas más avanzadas, no debe tener por consecuencia reducir el nivel general de confidencialidad de las comunicaciones y de protección de la intimidad de las personas.

Estas obligaciones toman un sentido particular cuando las telecomunicaciones entre personas situadas en el territorio de los Estados miembros transiten o puedan transitar por el exterior del territorio europeo, en particular en la utilización de satélites o de Internet." La confidencialidad de las comunicaciones (incluido el comportamiento en Internet) debe ser la regla, no la excepción.

Artículo 6 - Datos sobre tráfico y facturación

El Grupo de trabajo opina que debe aprovecharse la oportunidad de revisar más minuciosamente las disposiciones referentes a los datos sobre tráfico. Dada la amplitud de la definición de los datos sobre tráfico, es preciso dejar claro que no resulta necesariamente aceptable dispensar un trato idéntico a todos los elementos constitutivos de los datos sobre tráfico. Debería especificarse sin dejar lugar a dudas con qué objetivos y en qué medida los distintos tipos de datos sobre tráfico (correspondientes a la nueva definición ampliada) pueden generarse, recabarse y almacenarse y para qué fines pueden utilizarse posteriormente. El Grupo de trabajo desearía subrayar que, incluso en caso de que se autorice el tratamiento de los datos con un fin específico y con el consentimiento del abonado, éste no renuncia definitivamente por ello a sus derechos a la protección de la intimidad y de los datos. El Grupo de trabajo recuerda asimismo que, en todo caso, el nivel de protección dispensado por la Directiva 97/66/CE debe mantenerse, cuando no reforzarse.

Apartado 2 del artículo 6: tras examinar el texto actualmente propuesto, que permite el tratamiento de los datos sobre tráfico necesarios para la facturación de los abonados, el Grupo de trabajo observa que el proyecto de Directiva no propone ningún tipo de armonización del plazo de impugnación legal de la factura. El Grupo de trabajo desea saber cómo proyecta la Comisión ajustarse a la Recomendación 3/99 en la que, con el propósito de reforzar el derecho fundamental a la intimidad de los ciudadanos, se proponía a la Comisión Europea la armonización de este plazo para fijar un límite al almacenamiento de datos sobre tráfico con estos fines precisos de facturación. El Grupo de trabajo sugiere al Parlamento Europeo y al Consejo que establezcan un plazo concreto que debería ser lo más breve posible. Todo tratamiento de los datos sobre tráfico con otros fines crea nuevos riesgos para el derecho fundamental de los ciudadanos a la intimidad, y sólo puede considerarse si se dispone previamente de las salvaguardias necesarias. El Grupo de trabajo recomienda por lo tanto la inclusión en el apartado 3 del artículo 6 de una prueba de "necesidad" en lo que respecta a la posibilidad de tratar los datos sobre tráfico para la promoción comercial del propio prestador del servicio.

En cuanto a la propuesta de autorizar el tratamiento de los datos sobre tráfico para la prestación de "servicios de valor añadido", el Grupo de trabajo considera que esta expresión no resulta lo suficientemente clara para garantizar la limitación de ese propósito. Los considerandos tampoco ofrecen ninguna definición ni indicación acerca de la gama completa de esos servicios. Dado que se trata de un contexto diferente al de la promoción comercial de los servicios de comunicaciones del propio prestador, es posible que requiera salvaguardias diferentes.

El Grupo de trabajo está plenamente de acuerdo con la nueva disposición del apartado 4 del artículo 6 referente a la información que debe facilitarse al abonado. Además, propone que se añada en el considerando correspondiente que los interesados también deben ser informados de su derecho de oposición al tratamiento (artículo 14 de la Directiva

95/46/CE).

Artículo 7 - Facturación detallada

El Grupo de trabajo considera muy favorable la referencia explícita en el artículo a las modalidades alternativas de comunicación o de pago que potencien la intimidad. Al mismo tiempo, lamenta que una de esas modalidades (supresión de algunas cifras, considerando 18 de la Directiva 97/66/CE) haya dejado de mencionarse en el considerando correspondiente de la propuesta. El Grupo de trabajo desearía se le confirmase que sigue tratándose de una modalidad legal y recomienda su integración en el considerando.

Artículo 9 - Datos sobre localización

Dado que es necesario aportar una mayor claridad a todo lo relacionado con los servicios de valor añadido (véase lo indicado más arriba), la posibilidad de utilizar los datos sobre localización (datos sobre tráfico) con esos fines debería examinarse en relación con la revisión radical de las normas aplicables a los datos sobre tráfico propuesta anteriormente. En principio, los datos sobre localización no deben tratarse para la prestación de servicios de valor añadido; excepcionalmente, pueden tratarse con fines claramente especificados que requieran por motivos técnicos la utilización de los datos sobre localización y siempre que se ofrezcan salvaguardias proporcionales a los riesgos existentes para la intimidad.

Sin adelantar la opinión de fondo definitiva del Grupo de trabajo acerca del tratamiento de los datos sobre localización para los servicios de valor añadido 11 , cabe indicar que, desde su punto de vista, la posibilidad técnica de rehusar el tratamiento de los datos propuesta en el apartado 2 del artículo 9 no es satisfactoria.

Habida cuenta de la sensibilidad de los datos sobre localización en relación con la libertad de circulación y del hecho de que los datos sobre localización que aquí se regulan no son necesarios para establecer la comunicación, el usuario o abonado debe tener pleno control sobre su tratamiento. La norma debería pues plantearse a la inversa: el abonado debe tener la posibilidad, mediante un procedimiento sencillo, de autorizar libremente el tratamiento de los datos sobre localización para cada prestación de un servicio de valor añadido (incluida, en caso necesario, la conexión a la red o la transmisión de una comunicación).

Los aspectos técnicos del ejercicio de este derecho deben estar incorporados al equipo del usuario o abonado y no a la red (contrariamente a lo que sucede con la identificación de la línea llamante).

Artículo 10 - Excepciones

El Grupo de trabajo considera que este artículo puede necesitar salvaguardias adicionales para evitar la elusión de las normas más estrictas recogidas en los artículos 15 y 13 de la Directiva 95/46/CE combinados. Dado que se mantiene el "antiguo" termino de "llamada", el Grupo de trabajo interpreta que este artículo sólo cubre la telefonía vocal por redes fijas y móviles, quedando excluida la telefonía vocal por Internet, las direcciones IP y el correo electrónico.

(a) En cuanto a la posibilidad propuesta de anular, a petición de un abonado, la opción de no ser identificado 12 con el fin de rastrear las llamadas maliciosas o molestas, convendría establecer una salvaguardia procedimental que garantice que se comprueba si una llamada determinada es efectivamente maliciosa o molesta.

(b) La anulación de la eliminación de la identificación de la línea llamante y la utilización de los datos sobre localización contra los deseos del abonado o usuario sin que éste lo sepa carece de la especificidad suficiente: en primer lugar, debería aclararse a qué tipo de datos sobre localización (datos sobre tráfico) se refiere la medida. En segundo lugar, para evitar la elusión del artículo 15, debería especificarse qué cuerpos y fuerzas de seguridad están autorizados para responder a las llamadas de urgencia e imponer la obligación de borrar los datos una vez conseguido el objetivo de la ayuda.

En este contexto, el Grupo de trabajo observa que el *apartado 3 del artículo 22 del proyecto de Directiva relativa al servicio universal y los derechos de los usuarios 13* obliga a los Estados miembros a velar por que "las empresas operadoras de redes telefónicas públicas pongan a disposición de las autoridades receptoras de llamadas de urgencia información relativa a la ubicación de las personas que efectúan llamadas al número europeo de urgencia "112", siempre que sea técnicamente viable". Aunque no cabe duda de que los servicios de auxilio a personas en situaciones de emergencia deberán disponer de toda la información necesaria para identificar al autor de la llamada, el Grupo de trabajo desea poner de manifiesto a la Comisión la necesidad de garantizar la coherencia con los principios de la protección de datos.

El concepto y la definición de las autoridades de los servicios de urgencia deben por lo tanto coincidir en ambos textos, y la obligación de facilitar datos sobre localización a esas autoridades limitarse a lo estrictamente necesario para identificar a la persona en peligro.

No obstante, habida cuenta de la sensibilidad de los datos sobre localización (véanse los comentarios a los artículos 2 y 9), puede merecer la pena considerar hasta cierto punto la posibilidad de que el número de urgencia "112" se clasifique como servicio, con la consecuencia de que sólo se le proporcionen los datos necesarios sobre localización de aquéllos abonados que lo hayan requerido.

Artículo 12-Guías de abonados

El Grupo de trabajo es favorable a la propuesta de que sean los abonados quienes decidan si desean figurar o no en las guías, ya sean impresas o electrónicas. Además, habida cuenta de la dimensión adquirida por las guías electrónicas en la actual sociedad de la información, los abonados deberían recibir información acerca de los posibles usos de las guías; además, los datos que éstas pueden incluir deberían limitarse a los necesarios para identificar a los abonados sin revelar otra información personal.

Este requisito está vinculado a otra cuestión que aún no se ha abordado en el proyecto de Directiva: actualmente, diversas autoridades competentes en materia de protección de datos están dirimiendo casos de búsquedas inversas en las guías. Éstas constituyen nuevos servicios en el mercado liberalizado de las telecomunicaciones, consistentes en la oferta, con un bajo nivel de dificultad y de costes, de nuevas capacidades de tratamiento de toda la información contenida en las guías telefónicas.

Por ejemplo, es posible encontrar el nombre y la dirección de una persona determinada a partir de su número de teléfono, o los nombres y números de teléfono de todos los vecinos de una calle a partir del nombre de la misma. Es posible descubrir mucha más información acerca de una persona de lo que ésta se imagina cuando da permiso para que su nombre figure en la guía de teléfonos (tanta información como la que suele aparecer en una tarjeta de visita: nombre y apellidos, dirección, profesión y lugar de trabajo). Es más, el simple conocimiento de los datos que aparecen en la factura detallada de un abonado en la que sólo figuren los números de teléfono a los que éste haya llamado permite obtener una lista de los nombres y las direcciones de todas las personas que hayan recibido llamadas de este abonado durante un periodo concreto. Otros productos de búsqueda contienen información geográfica ("datos sobre localización", véanse los comentarios a los artículos 2 y 9) como mapas de ciudades y bases de datos con fotografías de todos las viviendas de una ciudad. Esta información podría vincularse fácilmente a la dirección que aparece en la guía de teléfonos y permite la búsqueda con arreglo a criterios múltiples.

Se trata aquí de una nueva función de las guías difícilmente compatible con su propósito inicial. Además, es ilegal en tanto en cuanto el sujeto a quien se refieran los datos no haya prestado su consentimiento para que esa información personal sea tratada con esos nuevos fines. El Grupo de trabajo ha adoptado una posición común a este respecto y considera importante que el proyecto de Directiva aborde explícitamente esta cuestión, exigiendo el consentimiento fundamentado del interesado para la inclusión de sus datos en las guías públicas con facilidad de búsqueda inversa.

Otro aspecto importante es el hecho de que estas guías pueden ser "editadas" por cualquiera. Es por lo tanto esencial asegurar que las transmisiones de datos efectuadas por un prestador de servicios u operador con vistas a la compilación de guías u otra utilización de los datos respeten las opciones expresadas (de forma gratuita) por los usuarios o abonados al prestador u operador inicial. Éste debe informar al usuario o abonado acerca de estas utilizaciones (uso comercial, guías inversas, etc.) antes de que sea efectivo el abono.

La cesión de datos en forma de CD ROM plantea en algunos casos un problema adicional relacionado con la duración de la licencia: ésta deberá determinarse de una forma que impida la utilización de datos anticuados respecto de las opciones escogidas por los interesados.

Artículo 13 - Comunicaciones no solicitadas

El envío de correo-basura (spam) es, como su nombre indica, la práctica de bombardear con mensajes electrónicos no solicitados, por lo general de carácter comercial, a personas con las que el remitente no ha mantenido contacto previo alguno.

Se trata de una modalidad muy concreta de violación de la intimidad: el usuario carece de interfaz humano, corre con el coste de la comunicación y, habitualmente, recibe este tipo de correo en la intimidad de su propio hogar.

No es de extrañar que los consumidores prefieran las comunicaciones comerciales solicitadas, personalizadas y diferenciadas al correo-basura, el cual resulta irritante, hace perder el tiempo (el necesario para leer los mensajes y borrarlos) y cuesta dinero. Las molestias causadas por los remitentes de correo-basura mina la confianza de los consumidores en el comercio electrónico.

El sector exige, además, cierta seguridad jurídica: los mensajes electrónicos no solicitados colocan a los proveedores de servicios de Internet en la inaceptable posición de verse forzados a proveer el ancho de banda y el equipo necesarios para el envío de unos mensajes basura que la abrumadora mayoría de sus clientes no desean. La eliminación de este tipo de correo de los servidores y la atención a los consumidores airados acarrean también considerables costes. En algunas ocasiones, los sistemas se bloquean por la mera carga de mensajes electrónicos comerciales no solicitados, lo que paraliza y retrasa el tráfico legítimo. La mayor parte de los PSI tratan de filtrar el correo basura e incluyen en sus contratos con los abonados cláusulas que prohiben a éstos el envío o la transmisión de estos mensajes. Existen registros de servidores sospechosos conocidos como fuentes de correo-basura. Pero los filtros que utilizan no son precisos al 100% y a veces bloquean los mensajes legítimos si éstos proceden de un servidor incluido en la lista negra. No obstante, la inexistencia de una prohibición legal de enviar correo basura coloca a los PSI en una situación delicada; la existencia de semejante prohibición facilitaría la adopción de medidas más directas contra los remitentes de correo basura.

Las últimas tendencias del mercado parecen indicar que las empresas de mercadotecnia directa en línea que lideran el mercado de los EE.UU. operan sobre la base de sistemas de autorización previa ("opt-in"), ya que los datos suministrados con arreglo a los mismos son de mejor calidad y el nivel de respuestas positivas que facilitan es considera-

blemente superior. Algunos incluso practican un "opt-in" doble: aunque el individuo haya accedido a recibir comunicaciones comerciales (por ejemplo, manifestando su acuerdo a tal efecto en una página web), en el primer mensaje electrónico de contacto (solicitado) se le vuelve a pedir que confirme sus deseos a la empresa.

La Internet ofrece grandes posibilidades de compilar direcciones electrónicas de los usuarios interesados en recibir comunicaciones comerciales sobre temas específicos por correo electrónico y dispuestos a dar su consentimiento con tal fin. Los envíos basados en el consentimiento tienen muchas más probabilidades de llegar a clientes potenciales que el correo basura.

En cinco Estados miembros (Alemania, Austria, Italia, Finlandia y Dinamarca), la ley prohibe el envío de comunicaciones comerciales no solicitadas.

En los demás Estados miembros, bien se dispone de un sistema de rechazo expreso ("opt-out"), bien la situación no está totalmente clara. Las empresas de los países que han optado por el sistema de rechazo expreso pueden recurrir a utilizar, además de las direcciones de correo electrónico de su propio país, las de los consumidores de los Estados miembros donde impera el sistema de autorización previa. Además, dado que las direcciones de correo electrónico carecen a menudo de indicaciones sobre el país de residencia de los destinatarios, la existencia de un sistema de regímenes divergentes dentro del mercado interior no ofrece una solución común para la protección de la intimidad de los consumidores.

Las cláusulas de autorización previa suponen una solución equilibrada y eficaz para eliminar los obstáculos que se oponen a la provisión de comunicaciones comerciales con una protección paralela del derecho fundamental de intimidad de los consumidores.

El Grupo de trabajo acoge favorablemente y apoya la propuesta de dispensar al problema del correo electrónico no solicitado un tratamiento idéntico al de los sistemas de llamada automática sin intervención humana y los aparatos de fax. En todas estas situaciones, el abonado carece de interfaz humano y sufraga parte de los costes de la comunicación. El grado de violación de la intimidad y la carga económica son comparables en los tres casos (véase el dictamen 1/2000).

Artículo 14 - Características técnicas y normalización (y considerando n§ 22)

El Grupo de trabajo celebra y apoya la propuesta de adoptar medidas específicas a escala comunitaria en caso necesario para garantizar la aplicación armonizada de las normas de protección de datos.

Habida cuenta de que el desarrollo de la tecnología sigue una dinámica ascendente ("bottom-up"), podría ser útil recordar a la industria el interés que reviste para ella la integración de factores de respeto e incluso de protección activa de la intimidad ya en las primeras fases del desarrollo del equipo lógico y físico.

El Grupo de trabajo opina que la tecnología debe ajustarse a las prescripciones legales y facilitar su aplicación, especialmente el principio de minimización de los datos que se deriva de los artículos 6 y 7 de la Directiva 95/46/CE y el ejercicio de los derechos de la persona sobre sus propios datos. Teniendo en cuenta la experiencia de varios Estados miembros, la Recomendación 3/97 sobre el anonimato en Internet y la Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, se propone añadir un párrafo en los términos siguientes: *El diseño y la selección de las tecnologías de tratamiento de datos, incluido el software y el hardware, se ajustará al objetivo de no tratar datos personales, o de tratar los menos posibles, y facilitará el ejercicio de los derechos de la persona sobre sus propios datos.*

Siempre que resulte posible y no desproporcionado con los fines de protección previstos, deberán utilizarse datos anónimos y seudónimos.

Transparencia

El Grupo de trabajo opina que, aunque no cabe duda acerca de la aplicabilidad de las obligaciones de informar a los interesados recogidas en la Directiva general sobre protección de datos,14 se obtendría cierto valor añadido si se obligase explícitamente a los prestadores de servicios a informar a los abonados o usuarios de sus derechos antes y después del abono o la utilización, brindándoles de esa forma la oportunidad de ejercer en cualquier momento las opciones o derechos que les otorgan las Directivas sobre protección de datos. Esta información se refiere a los fines del tratamiento propuesto de los datos, la identidad de los controladores, los destinatarios, en caso de que existan terceros, los derechos individuales, etc.. Se propone que los prestadores/operadores publiquen esta información para permitir al abonado/usuario escoger en todo momento entre las opciones disponibles para ejercer sus derechos. Por ejemplo, esto podría llevarse a la práctica mediante la publicación de la política de protección de la intimidad en una página web.

3. Conclusiones

El Grupo de trabajo acoge favorablemente la revisión dirigida a garantizar que los mismos servicios sean objeto de una regulación equivalente con independencia de los medios por los que se presten. Ello significa asimismo que los consumidores y usuarios deberían disfrutar del mismo nivel de protección de su intimidad y datos personales con independencia de la tecnología empleada para prestar un servicio determinado. El Grupo de trabajo comparte y apoya

plenamente la opinión de la Comisión según la cual el mantenimiento de un alto nivel de protección de los datos y la intimidad de los ciudadanos constituye uno de los objetivos declarados. Además, el Grupo de trabajo reconoce que se ha propuesto un considerable número de adaptaciones para aumentar el nivel de protección de los datos en todas las comunicaciones electrónicas.

El Grupo de trabajo recomienda que la Comisión, el Parlamento Europeo y el Consejo tengan en cuenta sus observaciones. Además, invita a la Comisión a que resuelva los asuntos pendientes de aclaración y permita de esa forma que el Grupo de trabajo contribuya al proceso en curso.

El Grupo de trabajo sugiere además que el presente proyecto de Directiva sea discutido por el Grupo de trabajo "cuestiones económicas - protección de datos" del Consejo. Esa medida permitiría acelerar el proceso de adopción de todas las Directivas propuestas en relación con la revisión del sector de las telecomunicaciones y facilitaría el acceso de los expertos competentes a este texto.

El Grupo de trabajo se reserva la posibilidad de hacer nuevas observaciones sobre este proyecto de Directiva a medida que vaya evolucionando.

NOTAS:

1 Diario Oficial L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm
2 La revisión de 1999 comenzó con una Comunicación de la Comisión en noviembre de 1999, seguida de un amplio proceso de consultas cuyos resultados se resumieron en una segunda Comunicación aprobada por la Comisión el pasado 26 de abril. Todos los documentos referentes a la revisión y los proyectos de Directivas están disponibles en http://www.ispo.cec.be/infosoc/telecompolicy/review99/Welcome.html
3 Todos los documentos adoptados por el Grupo están disponibles en : http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm
4 Esto se deduce del *artículo 3* de la presente propuesta de Directiva y del *artículo 2* del proyecto de Directiva general. El Grupo de trabajo señala que en ninguno de los dos documentos se definen los "servicios públicos de comunicaciones" y que la definición de los "servicios de comunicaciones electrónicas" del proyecto de Directiva sobre la protección de la intimidad resulta incompleta en comparación con la del texto general.
5 Sería útil saber si está cubierto el envío de mensajes textuales a teléfonos móviles.
6 Véanse el artículo 2 (definiciones), el proyecto de considerando n§ 5, el artículo 3 (servicios afectados) y la definición de las "redes de comunicaciones electrónicas" en el documento sobre el marco regulador, en los que las "redes IP" podrían añadirse a los ejemplos citados.
7 Otro aspecto merecedor de un debate más profundo es la posibilidad de que algunos de estos datos se consideren datos sensibles, cuyo tratamiento está en principio prohibido, en el sentido del artículo 8 de la Directiva general sobre protección de datos 95/46/ CE.
8 COM (2000) 393.
9 Asunto C-109/92 Wirth [1993] ECR I-6447 , 15.
10 Para ello, podría por ejemplo añadirse la palabra *"habitualmente*" al lado de las palabras "contra remuneración" en el texto de la definición y explicar en el considerando respectivo el significado de estos términos con arreglo a la jurisprudencia anteriormente citada.
11 O, de forma más general, acerca de la divulgación de los datos sobre localización a los usuarios de las redes.
12 La eliminación de la identificación de la línea llamante significa que el abonado puede optar por conservar su anonimato respecto del receptor de la llamada. La anulación de este derecho implica que la línea llamante puede ser identificada incluso contra los deseos de su autor. Por lo que respecta a las llamadas de urgencia, se propone que esto se aplique también a los datos sobre localización incluso en el supuesto de que el abonado no haya otorgado su consentimiento para el tratamiento de esos datos. 11 O, de forma más general, acerca de la divulgación de los datos sobre localización a los usuarios de las redes. 12 La eliminación de la identificación de la línea llamante significa que el abonado puede optar por conservar su anonimato respecto del receptor de la llamada. La anulación de este derecho implica que la línea llamante puede ser identificada incluso contra los deseos de su autor. Por lo que respecta a las llamadas de urgencia, se propone que esto se aplique también a los datos sobre localización incluso en el supuesto de que el abonado no haya otorgado su consentimiento para el tratamiento de esos datos.
13 Disponible en el sitio web indicado en la nota a pie de página n§ 2.
14 Véanse los artículos 10, 11, 12, 14, etc. de la Directiva 95/46/CE mencionados en el considerando n§ 9 del proyecto de Directiva, así como el apartado 2 del artículo 4, el apartado 4 del artículo 6 y los artículos 7, 8, 9, 11, 12 y 13 del proyecto de Directiva.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

MEMORIA DE 2000 - ANEXO XVI - DOCUMENTO DE TRABAJO PRIVACIDAD EN INTERNET: ENFOQUE COMUNITARIO INTEGRADO DE LA PROTECCIÓN DE DATOS EN LÍNEA -ADOPTADO EL 21 DE NOVIEMBRE DE 2000.

Este documento pretende ofrecer un enfoque comunitario integrado de la cuestión de la protección de datos en línea. La palabra "integrado" subraya que el análisis se basa principalmente en los textos de la Directiva general sobre protección de datos (Directiva 95/46/CE) y de la Directiva relativa a las telecomunicaciones y a la intimidad (Directiva 97/66/CE), aunque también se tienen en cuenta y se recogen todos los dictámenes y documentos que el Grupo de Trabajo ha adoptado hasta el momento sobre determinadas cuestiones importantes relacionadas con este tema 1 .

Al debatir las prioridades del trabajo futuro, el Grupo de Trabajo ha defendido en varias ocasiones la necesidad de tratar las cuestiones sobre protección de datos relacionadas con el uso de Internet. En 1999, con el fin de abordar estos asuntos de una forma eficaz y sistemática, se creó el Grupo operativo sobre Internet, cuyo objetivo primordial es reunir los recursos y las experiencias técnicas de las distintas autoridades nacionales en materia de protección de datos y contribuir así a la interpretación y la aplicación uniformes de la normativa vigente en este campo.

El Grupo operativo sobre Internet ha redactado varios documentos que a lo largo de los dos últimos años ha adoptado el Grupo de Trabajo.

Desde principios de 2000, el Grupo operativo sobre Internet se ha reunido con mayor frecuencia con vistas a alcanzar un documento de síntesis que pueda servir como referencia a la hora de tratar las cuestiones actuales, y en la medida de lo posible también las futuras, relacionadas con la intimidad en Internet.

El objetivo principal de este documento es ofrecer un primer enfoque de la cuestión de la privacidad en línea que pueda contribuir a aumentar la sensibilización respecto a los riesgos que el uso de Internet supone para la intimidad y que, al mismo tiempo, sirva de guía para interpretar las dos Directivas existentes en este campo. El Grupo de Trabajo es consciente de que la protección de la privacidad es una de las mayores preocupaciones de los usuarios de la Red 2 Por lo tanto, concede una especial atención al tratamiento de este 7 asunto, aunque reconoce que determinadas cuestiones polémicas, que suscitan un debate especial, pueden requerir un mayor trabajo en el futuro.

- Este documento no pretende ser exhaustivo en sí mismo, pero intenta cubrir las situaciones más habituales a las que pueden enfrentarse los usuarios de Internet cuando utilizan alguno de los servicios disponibles en la Red, tales como el correo electrónico, los navegadores, los buscadores, los foros de debate, etc. Debido a su carácter general, tampoco aborda cuestiones específicas que pueden requerir un estudio más detallado del Grupo de Trabajo en el futuro, como el control del correo electrónico en el puesto de trabajo. Este documento de trabajo se basa en el estado actual de Internet, que es, por naturaleza, un fenómeno enormemente dinámico y cambiante.

Para facilitar la lectura del documento, en primer lugar se abordan la descripción técnica básica y las cuestiones jurídicas generales. Posteriormente se trata por separado cada uno de los distintos servicios de Internet, analizando en cada capítulo las cuestiones técnicas y jurídicas pertinentes. Otro capítulo se dedica a las medidas y tecnologías en favor de la privacidad que pueden utilizarse para incrementar la privacidad de los usuarios de Internet. El último capítulo presenta las conclusiones.

Al final del documento se incluye un glosario de términos técnicos para facilitar a los lectores la comprensión de los conceptos técnicos utilizados en el texto. Las palabras contenidas en el glosario aparecen en el texto destacadas en cursiva.

El Grupo operativo sobre Internet ha decidido deliberadamente mantener cierto grado de superposición en el documento, lo que permitirá a los lectores con especial interés en un tema específico realizar una lectura selectiva. Para ello se han mantenido en el texto algunas descripciones adicionales, repetitivas en ocasiones, destinadas a simplificar la consulta de los distintos capítulos.

La coordinación del trabajo del Grupo operativo sobre Internet ha sido responsabilidad de Peter HUSTINX, presidente de la autoridad holandesa responsable de la protección de datos. Un grupo de redacción nombrado en el seno del Grupo operativo sobre Internet y formado por Diana ALONSO BLAS (de la autoridad holandesa de protección de datos) y Anne-Christine LACOSTE (de la autoridad belga de protección de datos) ha preparado la versión consolidada del documento de trabajo. Entre las tareas que ha realizado este grupo de redacción cabe destacar la estructuración y el control de la coherencia de todo el documento, la integración y el posterior desarrollo de las cuestiones jurídicas adicionales y de la información técnica y los comentarios recibidos de otras delegaciones, la elaboración del glosario de términos técnicos y la redacción de las conclusiones del documento.

Delegados de las autoridades responsables de la protección de datos de seis países han participado en diferentes fases del trabajo del Grupo operativo sobre Internet, redactando textos que han servido de base para varios capítulos, comentando las aportaciones de otros miembros del Grupo operativo sobre Internet e interviniendo en los debates que tuvieron lugar durante las cinco reuniones que el Grupo operativo celebró en 2000.

Cabe mencionar en especial a Anne-Christine Lacoste y Jean-Marc Dinant (Bélgica), Ib Alfred Larsen (Dinamarca), Marie Georges (Francia), Angelika Jennen y Sven Moers (Alemania), Emilio Acedo Félez (España) y Diana Alonso Blas, Ronald Hes y Bernard Hulsman (Países Bajos). El Grupo operativo sobre Internet desearía expresar su agradecimiento a Christine Sottong-Micas (Secretaría del Grupo de Trabajo sobre protección de datos del artículo 29 de la Comisión

Europea) y Karola Wolprecht (prácticas 1999/2000 en la Comisión Europea) por su ayuda y su asistencia.

CAPÍTULO 2: DESCRIPCIÓN TÉCNICA DE INTERNET

I. Nociones básicas

Internet es una red de ordenadores que se comunican entre sí utilizando el *protocolo* de control de transporte/*protocolo* de Internet (TCP/IP)3 . Se trata de una red internacional de ordenadores interconectados que permite a millones de personas comunicarse unas con otras en el "ciberespacio" y acceder a inmensas cantidades de información procedente de todo el mundo 4 .

El predecesor histórico de Internet fue la red militar ARPAnet (1969). La idea básica era construir una red estadounidense digitalizada que permitiese a los ordenadores del ejército, de los contratistas que trabajaban para el ejército y de las universidades participantes en investigaciones relacionadas con la defensa comunicarse entre sí a través de canales redundantes, incluso en caso de que algunas partes de la red resultasen dañadas en una guerra 5 .

Los primeros programas de correo electrónico aparecieron en 1972. En 1985, la Fundación nacional de la ciencia de EE.UU. construyó la red NSFNET con el fin de enlazar seis grandes centros informáticos del país.

En los años ochenta dicha red se transfirió a un grupo de universidades llamado MERIT y se fue abriendo paulatinamente a instituciones no académicas y organizaciones no estadounidenses.

En 1990, Tim Berners Lee, que trabajaba en el Centro Europeo para la Investigación Nuclear de Ginebra, diseñó el primer navegador y aplicó el concepto de *hipervínculo*, tras lo cual se han ido añadiendo continuamente gran variedad de nuevos servicios y funciones.

Sin embargo, conviene tener en cuenta que el TCP/IP sigue siendo el *protocolo* básico de transmisión de datos en Internet y que todos los servicios dependen de él. Este *protocolo*, cuyo diseño permite una instalación muy sencilla, no depende de ningún sistema operativo ni informático específico.

En Internet, cada ordenador se identifica con una dirección IP numérica única de la forma A.B.C.D, en la que A, B, C y D son números del 0 al 255 (por ejemplo, 194.178.86.66).

Las *redes TCP/IP* se basan en la transmisión de paquetes pequeños de información, cada uno de los cuales contiene la dirección IP del emisor y del destinatario. Estas redes funcionan sin conexiones, lo que significa que, al contrario de lo que sucede con la red telefónica, por ejemplo, no es necesaria una conexión previa entre dos dispositivos para iniciar la comunicación. Esto permite igualmente realizar diversas comunicaciones con interlocutores distintos de forma simultánea.

El *DNS (sistema de nombres de dominio)* es un mecanismo de asignación de nombres a ordenadores identificados con una dirección IP. Dichos nombres presentan la forma <nombre>.dominio de nivel superior, donde <nombre> es una cadena formada por una o varias subcadenas separadas por un punto. El dominio de nivel superior puede ser un dominio genérico (por ejemplo, "com" para páginas web comerciales u "org" para organizaciones sin ánimo de lucro) o bien un dominio geográfico, como "be" para Bélgica. El *DNS* no es un servicio gratuito y las empresas o las personas que deseen un nombre de dominio deben identificarse. Ciertas herramientas públicas existentes en la Red permiten encontrar el enlace entre el nombre de dominio y la empresa, así como entre la dirección IP y el nombre de dominio. No es necesario un nombre de dominio para conectar un ordenador a Internet. Los nombres de dominio son dinámicos. Un único ordenador conectado a Internet puede tener uno o varios nombres de dominio, o también no tener ninguno, pero un nombre de dominio específico se refiere siempre a una dirección IP determinada.

Actualmente existe una cantidad limitada de direcciones IP. Este número depende de la extensión del campo asignado a la dirección IP en el *protocolo* 6 . En Europa, las direcciones IP se asignan mediante un procedimiento internacional 7 a proveedores de acceso a Internet que las reasignan a sus clientes, ya sean organizaciones o particulares.

Gracias a una herramienta de búsqueda de acceso público,como http://www.ripe.net/cgi-bin/ whois, se puede identificar al responsable de una determinada reserva de dirección IP. En general, éste será:

* El administrador de una red local con acceso a Internet (por ejemplo, una PYME o un organismo público), que seguramente usará un esquema fijo de direccionamiento IP y mantendrá una lista con la correspondencia entre los ordenadores y las direcciones IP.

Si esta persona está utilizando el *protocolo de configuración dinámica del host* (DHCP 8), el programa *DHCP* dispondrá normalmente de un fichero registro con el número de la tarjeta Ethernet. Este número único en el mundo identifica un ordenador determinado en la red local.

* Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet. En este caso, normalmente el proveedor mantendrá un fichero histórico con la dirección IP asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. Es más, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado,

junto con la fecha, la hora y la duración, para la posterior facturación.

* El titular del nombre de dominio, que podrá ser un nombre de empresa, el nombre de un empleado de una empresa o un particular.

En estos casos, ello significa que, con la asistencia de las terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre, dirección, número de teléfono, etc.) por medios razonables.

Un *encaminador* es un dispositivo que proporciona rutas a las *redes TCP/I*P. Esto significa que la ruta TCP/IP es dinámica, pues depende de los fallos o las sobrecargas de algunos *encaminadores* o enlaces. También puede servir como *cortafuegos* entre una organización e Internet. En particular, puede garantizar que todas las direcciones que proceden de determinado *proveedor de servicios de Internet* están autorizadas.

Cabe señalar que la velocidad de transmisión es el criterio fundamental de encaminamiento en *redes TCP/I*P. Con información circulando casi a la velocidad de la luz, si en París hay un atasco de la Red puede resultar más eficaz que un paquete TCP/IP enviado de Londres a Madrid pase por Nueva York. Algunas herramientas permiten al usuario de Internet conocer el camino entre dos puntos, aunque en teoría puede cambiar cada segundo e incluso durante la transferencia de una misma página web.

Protocolos más sofisticados que emplean el TCP/IP

A partir del TCP/IP, existen otros *protocolos* capaces de ofrecer determinados servicios.

Básicamente, los *protocolos* más utilizados son:

* el HTTP *(protocolo* de transporte de hipertexto), utilizado para navegar,

* el FTP *(protocolo* de transferencia de ficheros), utilizado para transferir ficheros,

* el NNTP *(protocolo* de transferencia de noticias a través de la Red), utilizado para acceder a foros de debate,

* el SMTP *(protocolo* simple de transferencia de correo) y los POP3 *(protocolo* de oficina de correo), utilizados para enviar y recibir correo electrónico.

Jerarquía de niveles y *protocolos* en un proceso de comunicación por Internet

M30.BMP;

* Estos *protocolos* son necesarios porque el *protocolo* TCP/IP sólo permite transmitir información en masa de un ordenador a otro. El ordenador que ofrece un servicio se denomina SERVIDOR, mientras que el ordenador que utiliza un servicio recibe el nombre de CLIENTE. Para prestar un servicio técnico, tanto el cliente como el servidor han de emplear el mismo *protocol*o, es decir, las mismas normas de comunicación. A menudo se habla de Internet como una red cliente-servidor. Cabe destacar que sea cual sea el servicio utilizado, el *protocolo* TCP/IP se utiliza siempre en todos los servicios anteriormente mencionados. Esto significa que las amenazas a la privacidad relacionadas con el *protocolo* TCP/IP estarán presentes al utilizar cualquier servicio de la Red.

* Con objeto de evitar malentendidos en relación con el significado general de la palabra "servicio", en este texto se empleará el término *protocolo* para designar los *protocolos* HTTP, FTP, NNTP y otros servicios disponibles en Internet.

Un *servidor proxy* es un servidor que actúa como intermediario entre el usuario de Internet y la Red. Funciona como una *caché web* y mejora de forma espectacular la velocidad de visualización de la información (por ejemplo, en la visualización de páginas web). Muchas organizaciones o proveedores importantes de acceso a Internet ya han aplicado esta solución. Cada página, imagen o logotipo descargado desde el exterior por un miembro de una organización se almacena en una caché en el *servidor proxy* y queda automáticamente disponible para los demás miembros de la misma organización.

II. AGENTES PARTICIPANTES EN INTERNET

Cabe señalar que una empresa o un individuo pueden desempeñar distintos papeles en Internet y, por lo tanto, ejecutar simultáneamente distintas operaciones de tratamiento de datos (por ejemplo, registro de conexiones en calidad de operador de telecomunicaciones o almacenamiento de sitios web visitados en calidad de *proveedor de servicios de Internet*), con todo lo que esto implica en la aplicación de principios sobre privacidad.

Operador de telecomunicaciones

En Europa, la infraestructura de telecomunicaciones ha sido, de hecho, monopolio de los operadores tradicionales de telecomunicación. Sin embargo, esta situación está cambiando. Además, a menudo este monopolio se reduce a los cables o las fibras ópticas, mientras que en el caso de las comunicaciones inalámbricas y las nuevas tecnologías, como *WA*P, *UMT*S, etc., está surgiendo la competencia entre los agentes nacionales.

No obstante, el operador tradicional de telecomunicaciones sigue siendo un agente importante, pues es quien se encarga de la comunicación de datos entre el usuario de la Red y el proveedor de acceso a Internet.

Con fines relacionados con la facturación, el operador de telecomunicaciones procesa datos sobre tráfico tales como el número que realiza la llamada y su situación (en el caso de los teléfonos móviles), el número llamado y la fecha, la hora y la duración de la comunicación 9 .

Proveedor de acceso a Internet

El proveedor de acceso a Internet proporciona, generalmente sobre la base de un contrato, una conexión TCP/IP a: - Personas que utilicen un *módem* o un adaptador de terminal (RDSI). En este caso, el abonado recibirá una dirección IP válida durante la conexión que probablemente cambiará la próxima vez que se conecte y se denomina dirección IP dinámica.

Si se trata de una línea *ADSL* (conexión a través de una línea de suscripción asimétrica digital) o de cable de vídeo, la dirección IP será normalmente estática, pues dichas conexiones son permanentes.

Para obtener una conexión, una persona 10 ha de firmar un contrato, (la suscripción es gratuita), y dar su nombre, dirección y otros datos personales.

Por regla general, el usuario recibirá un nombre de identificación de usuario, que puede ser un seudónimo, y una contraseña, con lo que nadie más podrá utilizar su abono. Aunque sólo sea por motivos de seguridad, los proveedores de acceso a Internet parecen registrar siempre en un fichero, de forma sistemática, la fecha, la hora, la duración y la dirección IP dinámica que se ha dado a un usuario de Internet. En la medida en que es posible vincular el fichero registro a la dirección IP del usuario, esta dirección se ha de considerar un dato de carácter personal.

- Organismos que utilicen una conexión por línea conmutada o, de forma más habitual, una línea arrendada a las oficinas de la empresa. Normalmente, el operador tradicional de telecomunicaciones será quien proporcione la línea.

La conexión también se puede establecer vía satélite o mediante un sistema de radio terrestre. El proveedor de acceso a Internet asignará a la empresa direcciones IP y utilizará un *encaminador* para garantizar que éstas se respetan.

Los proveedores de acceso a Internet poseen una o más líneas arrendadas (par trenzado, fibra óptica, enlace vía satélite) conectadas a otros proveedores mayores.

Proveedor de servicios de Internet

El *proveedor de servicios de Internet* ofrece servicios de la Red a empresas y particulares. Es propietario o arrendatario de una conexión TCP/IP permanente y utiliza servidores conectados continuamente a Internet. Por lo general, el proveedor desempeñará el papel de sistema anfitrión (almacenando páginas web en su servidor web) y ofrecerá acceso a foros de debate y a servidores FTP, así como servicios de correo electrónico. Esto implica la utilización por parte de uno o varios servidores de los *protocolos* POP3, SMTP, FTP, NNTP y HTTP.

Las empresas que actúan como proveedores de acceso a Internet a menudo ofrecen también servicios como *proveedores de servicios de Interne* t.

Por este motivo, el término genérico *proveedor de servicios de Internet* se utiliza en ocasiones para designar tanto a los proveedores de acceso como a los *proveedores de servicio* s.

No obstante, desde un punto de vista conceptual, los papeles que desempeñan son diferentes. Concretamente, el proveedor de acceso a Internet encaminará, en su calidad de vía de entrada a la Red, todo el tráfico que genere el abonado, mientras que el *proveedor de servicios de Internet* sólo tendrá conocimiento de lo que suceda en sus servidores 11 . En este informe, cuando se utilice el término *proveedor de servicios de Internet* se incluirá normalmente a los proveedores de acceso. El término proveedor de acceso a Internet sólo se empleará cuando sea evidente que se hace referencia exclusivamente al acceso a la Red; en caso contrario se empleará el término genérico *proveedor de servicios de Interne*t.

Desde un punto de vista técnico, la presencia de servidores equipados con *protocolos* resultará decisiva en la recopilación de datos personales.

En el caso de los servidores HTTP, generalmente se crea sistemáticamente por defecto un fichero registro o un fichero histórico que puede contener todos o algunos de los datos que aparecen en la cabecera de la petición HTTP (charloteo del navegador), además de la dirección IP. El fichero registro es una práctica estándar y todos los servidores lo crean.

Usuario

El usuario de Internet puede ser un particular que accede a la Red desde su casa, normalmente con una conexión TCP/IP temporal y, por tanto, con una dirección IP dinámica, a través de un *módem* o de un adaptador de terminal (RDSI) o bien con una conexión permanente y una dirección IP estática mediante una línea *ADS*L, televisión por cable, etc. La conexión también se puede realizar a través de un teléfono móvil, aunque suele ser más cara.

Si un abonado proporciona una identidad falsa o utiliza la identidad de otro usuario, dando el nombre de usuario y la contraseña de otra persona, es posible localizar al propietario de la línea a la que se ha asignado una determinada dirección IP comparando esta información con los datos recogidos en el fichero registro del proveedor de acceso a Internet. De hecho, esto es lo que hace la policía para localizar intromisiones delictivas en ordenadores conectados a Internet.

Lo mismo sucede si una persona está utilizando una red local o una intranet.

El usuario puede ser también una organización, una administración pública o una empresa que utiliza Internet no sólo para proporcionar o hallar información, sino también para recoger datos que le sirvan en su trabajo o sus actividades, como procedimientos administrativos, venta de mercancías o prestación de servicios, publicación de guías, anuncios por palabras, envío de cuestionarios, etc.

III. SERVICIOS DISPONIBLES EN INTERNET 12

Cualquier persona con acceso a Internet puede utilizar gran variedad de métodos de comunicación y de recuperación de la información.

Los más habituales son el correo electrónico (capítulo 4), los foros de debate y la charla electrónica (capítulo 6) y la World Wide Web (capítulo 5).

Todos estos métodos se pueden utilizar para transmitir texto y la mayoría de ellos pueden transportar también sonidos, imágenes fijas e imágenes de vídeo animadas. En conjunto, estas herramientas constituyen un medio único, conocido por los usuarios como "ciberespacio", que todas las personas pueden utilizar en cualquier parte del mundo siempre que dispongan de acceso a Internet.

Correo electrónico

El correo electrónico permite a un usuario enviar un mensaje electrónico a otra persona o a un grupo de direcciones. En general, el mensaje se almacena electrónicamente en un servidor hasta que el destinatario comprueba su buzón.

A veces avisa de su llegada mediante algún tipo de indicador.

Foros de debate

Los foros de debate se utilizan para compartir información o expresar opiniones sobre temas concretos. Los grupos suelen componerse siempre de los mismos participantes, cuyas aportaciones pueden también ser leídas por otras personas. Existen miles de grupos de este tipo, cada uno de los cuales fomenta el intercambio de información o de opiniones sobre un tema determinado. Cada día se envían alrededor de 100 000 mensajes nuevos.

Salas de charla electrónica ("chat rooms")

Dos o más personas que deseen comunicarse directamente pueden entrar en una sala de charla para iniciar un diálogo en tiempo real escribiendo mensajes que aparecen casi de forma inmediata en las pantallas de los demás.

World Wide Web

El tipo de comunicación más conocido en Internet es la World Wide Web, que permite a los usuarios buscar y recuperar información almacenada en ordenadores remotos. Para expresarlo de una forma sencilla, la Web consiste en una inmensa cantidad de documentos almacenados en distintos ordenadores de todo el mundo.

Navegar por Internet resulta relativamente sencillo. Un usuario puede escribir la dirección de una página que ya conoce o introducir una o más palabras clave en un buscador comercial para encontrar sitios relacionados con un tema que le interese.

Normalmente, los usuarios exploran una determinada página web o se trasladan a otra pulsando con el ratón del ordenador en uno de los iconos o enlaces de la página. Desde el punto de vista del lector, la Web se podría comparar a una enorme biblioteca con millones de publicaciones indizadas y fácil acceso o a un centro comercial que se expande de forma irregular para ofrecer bienes y servicios (véase el capítulo 7).

Cualquier persona u organización que disponga de un ordenador conectado a Internet puede "publicar" o recopilar información (véanse los capítulos 6, 7 y 8). Entre quienes publican o recaban datos se encuentran organismos gubernamentales, instituciones educativas, entidades comerciales, grupos de interés y particulares. Pueden ofrecer su información al conjunto de los usuarios de Internet o restringir el acceso a la misma a un grupo seleccionado.

IV. Riesgos para la privacidad 13

Riesgos para la privacidad inherentes a la utilización del *protocolo* TCP/IP Dado que Internet se ha considerado

desde el principio una red abierta, existen muchas características de los *protocolos* de comunicación que pueden llevar, más por accidente que de forma intencionada, a una invasión de la intimidad de los usuarios de Internet.

En lo que respecta al *protocolo* TCP/IP, hay tres características que parecen constituir una posible invasión de la intimidad.

* La **ruta** que siguen los paquetes TCP/IP es dinámica y se guía por la lógica de conseguir el mejor resultado. En teoría, puede variar durante la descarga de una página web o la transmisión de un correo electrónico, pero en la práctica suele permanecer estática. En telecomunicaciones, los resultados dependen más de la congestión de la Red que de la distancia física existente entre los nodos *(encaminadores*).

Esto significa que el camino "más corto" entre dos poblaciones situadas en un mismo país de la UE puede pasar por un país ajeno a la Unión en el que quizá no exista una protección de datos adecuada 14 . El usuario medio de Internet no dispone de medios razonables para modificar este camino, aun en el caso de que conozca la ruta seguida en un determinado momento.

* La traducción entre el nombre de dominio y la dirección IP numérica se realiza a través de un **servidor DNS** que recibe y puede rastrear todos los nombres de los servidores de Internet con los que el usuario haya intentado contactar. En la práctica, quienes mantienen esos servidores de nombres de dominio suelen ser los proveedores de acceso a Internet, que disponen de capacidad técnica para conocer mucho más que eso, como se verá en los próximos capítulos.

* La orden **"pin**g", disponible en todos los sistemas operativos, permite a cualquier persona conectada a Internet saber si un determinado ordenador está encendido y conectado a la Red. Esta orden consiste en escribir las letras PING seguidas de la dirección IP (o el nombre correspondiente) del ordenador. Normalmente, el usuario de éste no sabrá que alguien ha intentado averiguar si estaba conectado a Internet en un determinado momento ni conocerá los motivos por los que lo ha hecho.

Cabría señalar que las conexiones permanentes a Internet realizadas por cable y *ADSL* presentan los mismos riesgos.

Aunque estas operaciones de tratamiento de datos son legítimas y en ocasiones ineludibles para el correcto funcionamiento de Internet, el usuario debería tener conocimiento de ellas y de las medidas de seguridad que puede aplicar.

Riesgos para la privacidad inherentes a la utilización de protocolos de alto nivel

Este apartado se centra en tres características que casi siempre están presentes a la hora de emplear el *protocolo* HTTP en los navegadores más utilizados. Conviene subrayar que la combinación de estas características puede acarrear graves consecuencias para la privacidad de los usuarios de Internet.

El *protocolo* HTTP presenta una importancia estratégica en la medida en que es el más utilizado en la Web y puede ofrecer servicios como el correo electrónico y los foros de debate, que hasta ahora se prestaban a través de *protocolos* especializados de alto nivel, como POP3, SMTP o NNTP 15 .

El charloteo del navegador

Es un hecho conocido que escribir "http://www.website.org/index.htm" significa "muéstrame la página llamada 'index.htm' en el servidor www.website.org utilizando el *protocolo* HTTP".

Se podría creer que sólo la dirección IP de la persona que navega por Internet y el fichero que quiere ver se transmiten al sitio web. Sin embargo, no es así.

La siguiente tabla recoge algunos de los datos que se transmiten de forma sistemática en la cabecera HTTP al realizar una petición HTTP (charloteo del navegador automático) y a los que, por tanto, puede acceder el servidor: La definición técnica de estos campos se encuentra en el RFC 1945 para HTTP 1.0 o en el RFC 2068 para HTTP 1.1. Se pueden formular las siguientes observaciones al respecto:

* La primera línea es la única indispensable.

* En la línea "Accept", cada navegador menciona que el usuario de Internet está utilizando Windows 95. Cabría preguntarse por qué.

Netscape añade que la versión del navegador es francesa. Cada navegador da la identificación de su nombre, versión y subversión.

* Mientras se describen los formatos aceptados, Microsoft informa a cada sitio de que el ordenador del usuario de Internet tiene instalados Powerpoint, Excel y Word.

* Opera no revela la página remitente.

* Opera no revela el idioma del usuario de Internet, mientras que Netscape dice que es francófono y Microsoft, además, revela que es belga francófono.

Hipervínculos invisibles

Los *hipervínculos* constituyen el valor añadido de Internet. Gracias a ellos se puede navegar de un continente a otro con hacer un simple clic con el ratón. Lo que el usuario corriente no ve es que los programas clásicos de navegación permiten incluir en el código HTML de la página una petición HTTP de descargar imágenes. No es necesario que esas imágenes se encuentren en el mismo servidor que ha recibido la petición de presentar una determinada página web.

En este caso, la variable HTTP_REFERER contiene la referencia de la página remitente, es decir, la página principal en la que se localizarán las imágenes. En otras palabras: si un sitio web incluye en su página en HTML un vínculo invisible con una imagen situada en el sitio web de una empresa de cibermarketing, ésta conocerá la página remitente antes de enviar la *pancarta* publicitaria. Cuando se realiza una búsqueda con un motor de búsqueda, el nombre de la página web incluye las palabras clave que se han introducido.

Cookies

Las *cookies* son datos que se pueden almacenar en ficheros de texto en el disco duro del usuario y de los que el sitio web puede conservar una copia. Forman parte del tráfico HTTP, por lo que se pueden transportar sin problemas con el tráfico IP.

Las *cookies* residen en el disco duro del usuario y recogen información sobre él que el sitio web que las depositó puede recuperar, o que alguien que conozca el formato de los datos de la página web puede leer. Una *cookie* puede contener todo tipo de información que el sitio web quiera incluir en ella: páginas visitadas, anuncios consultados, número de identificación del usuario, etc.16 .

En algunas ocasiones, pueden resultar útiles para ofrecer un determinado servicio a través de Internet o para simplificar la navegación del usuario. Por ejemplo, algunos sitios web utilizan *cookies* para identificar a sus usuarios cada vez que éstos los vuelven a visitar, de modo que no necesitan registrarse cada vez que quieren consultar las novedades.

La SET-COOKIE se instala en la cabecera de la respuesta HTTP 17 , concretamente en *hipervínculos* invisibles. Para una duración determinada 18 , la *cookie* se almacena en el disco duro del usuario de Internet y se vuelve a enviar al sitio web que la originó o a otros sitios pertenecientes al mismo subdominio. Este reenvío se efectuará a través de un campo COOKIE que formará parte del charloteo del navegador ya descrito.

Utilizando conjuntamente el charloteo del navegador e *hipervínculos* invisibles, una empresa de cibermarketing puede, por defecto, conocer todas las palabras clave introducidas por un usuario de Internet en el motor de búsqueda en el que se anuncia la empresa, así como el ordenador, el sistema operativo, la marca de navegador del usuario de Internet, su dirección IP y la hora y la duración de las sesiones HTTP. La combinación de estos datos sin procesar con otros que ya posea la empresa permite la deducción de nueva información, tal como 19 :

1. El país donde vive el usuario de Internet.
2. El dominio de Internet al que pertenece.
3. El sector de actividad de la empresa donde trabaja.
4. La facturación y el volumen de la empresa donde trabaja.
5. La función y el puesto del usuario de Internet dentro de dicha empresa.
6. El proveedor de acceso a Internet.
7. El tipo de sitios web que actualmente visita.

La *cookie* permite el envío sistemático de un identificador permanente y único con cada petición de información, mientras que la dirección IP resulta ser un identificador relativamente débil, pues puede quedar oculto por proxies, y poco fiable, debido a su carácter dinámico en el caso de los usuarios que acceden a Internet con un *módem*.

Muchas empresas de cibermarketing han adoptado este proceso invisible de elaboración de perfiles 20 .

Riesgos para la privacidad relacionados con la aplicación del *protocolo* HTTP en los **navegadores habituales**

La combinación de charloteo del navegador, *hipervínculos* invisibles y *cookies* proporciona los medios necesarios para elaborar un perfil invisible de cada usuario de Internet que utiliza un navegador instalado por defecto. Este perfil no está "en sí mismo" vinculado al *protocolo* HTTP, como ha definido el *W3C* 21 . Además, la definición del *protocolo* HTTP 1.1 ha llamado explícitamente la atención de la industria sobre posibles cuestiones relacionadas con la privacidad inherentes a la utilización del *protocolo* HTTP 22 : - *"La descripción de las capacidades del agente usuario en cada petición puede resultar muy ineficaz (dado que sólo un pequeño porcentaje de respuestas tienen representaciones múltiples) y una posible violación de su intimidad"* [página 68].

- *"El envío de una cabecera Accept-Language con las preferencias lingüísticas completas del usuario en cada petición puede ir en contra de sus expectativas de protección de la privacidad"* [página 98].

- *"El cliente NO DEBERÍA enviar el campo de cabecera From 23 sin el consentimiento del usuario, pues ello puede ser contrario a los intereses de intimidad del mismo o a la política de seguridad del sitio web. Es muy recomendable que el usuario pueda prohibir, autorizar y modificar el valor de este campo en todo momento antes de una petición"* [página 118].

- *"A menudo, los clientes HTTP tienen acceso a grandes cantidades de datos personales, como el nombre del usuario, su situación y dirección postal, su contraseña, sus claves de* encriptación*, etc., y DEBERÍAN ser extremadamente prudentes para evitar cualquier fuga involuntaria de esta información a otras fuentes a través del* protocolo *HTTP. Se recomienda encarecidamente que se establezca un interfaz para que el usuario pueda controlar la divulgación de esta información y que los diseñadores y desarrolladores presten una atención especial a esta cuestión. La historia demuestra que errores de este tipo provocan a menudo graves problemas de seguridad o de intimidad y que suelen constituir una publicidad extremadamente perjudicial para la empresa responsable"* [página 143]24 .

V. Cuestiones económicas

El crecimiento de Internet en los últimos años ha sido espectacular. Entre 1981 y 1996, el número de ordenadores que almacenan la información y proporcionan las comunicaciones ("host") aumentó de unos 300 a cerca de 9 400 000. En torno al 60 % de ellos se encuentran en los Estados Unidos. En 1996 unos 40 millones de personas eran usuarios de Internet; se espera llegar a unos 200 millones 25 para 2000 y se prevé que en 2005 la mitad de la población europea esté conectada a la Red 26 .

En muchos países europeos la suscripción de los particulares a Internet es gratuita, pero el abonado tiene que pagar al operador de telecomunicaciones por la línea. El proveedor de acceso o el *proveedor de servicios de Internet* obtendrá una remuneración del operador de telecomunicaciones en forma de una prima de retroconexión que dependerá de la duración de la llamada local realizada por el abonado a Internet. Esto significa que, aunque no deba pagar por la suscripción a Internet, el usuario ha de hacer frente a los gastos de las líneas telefónicas utilizadas, lo que beneficiará tanto a los proveedores de acceso y de servicios de Internet como a los operadores de telecomunicación.

Los fabricantes de software también se beneficiarán de la utilización de Internet, pues aunque ofrezcan sus productos al consumidor de forma gratuita (software gratuito, navegadores, etc.), perciben una remuneración por el uso que los servidores de sitios web hacen de sus programas.

La venta directa es una de las actividades más lucrativas de la Red. Las empresas de cibermarketing instalan *pancartas* publicitarias en páginas web, a menudo de tal forma que la recopilación de datos personales resulta invisible para el titular de los datos. El uso de enlaces invisibles, junto con el charloteo del navegador y las *cookie*s, permite que empresas de venta desconocidas elaboren perfiles individualizados de los usuarios de Internet. Una sola empresa de cibermarketing podría vender aproximadamente medio millardo de *pancartas* publicitarias al día. Las empresas de venta directa financian muchos motores de búsqueda.

Instalando *hipervínculos* invisibles a empresas de cibermarketing en sus propias páginas web, los sitios web más visitados (especialmente los motores de búsqueda) enviarán una orden a navegadores como Netscape e Internet Explorer para que abran una conexión independiente HTTP con el servidor HTTP de la empresa de cibermarketing.

Como ya se ha explicado, mientras gestiona la petición HTTP, el navegador comunicará automáticamente varios datos, a saber: la dirección IP, la página remitente (en el caso de un motor de búsqueda, esta variable contiene las palabras clave introducidas por el usuario), la marca, la versión y el idioma del navegador (por ejemplo, Internet Explorer 4.02, neerlandés) y el tipo y el sistema operativo utilizados (Windows 2000, Linux 2.2.5, Mac OS 8.6, etc.), así como la *cookie* de identificación (como UserId=342ER432), que tal vez la empresa de cibermarketing ya haya incorporado con *hipervínculos* invisibles previos.

Normalmente, el usuario medio de Internet ignora que muchas de las *pancartas* que ve tras introducir un URL (localizador de recursos uniforme) no proceden del sitio web que está visitando. Tampoco sabe que al descargar una *pancarta* publicitaria su navegador transmitirá sistemáticamente una serie de datos únicos, como la identidad, la dirección IP y el URL completo de la página web en la que se encuentra, incluidas también las palabras clave tecleadas en motores de búsqueda y el nombre de los artículos de prensa que está leyendo en línea. Todos esos datos pueden combinarse para determinar el perfil general de un ciudadano que navega de una página a otra, gracias a la identidad única almacenada en la *cooki*e.

Se considera que la recopilación de información relativa al usuario en entornos en línea es una práctica de importancia económica y estratégica.

Las siguientes líneas, extraídas de una famosa publicación americana 27 , ilustran esta idea: *Son demasiadas las empresas, incluidas muchas compañías punteras que están surgiendo en Internet, que no se han centrado lo suficiente en el valor de los perfiles de los clientes.*

Quien posea los derechos *sobre los perfiles de los clientes en línea será quien determine los ganadores y los perdedores de esta nueva era.* Conviene mencionar que la recopilación de datos de usuarios de Internet suele ser gratuita para la empresa, pues a menudo son los propios consumidores quienes los proporcionan a través, por ejemplo, de formularios. Los sitios web recurren habitualmente a programas de fidelidad, como juegos, cuestionarios o boletines informativos, que obligan al visitante de la página a comunicar datos personales.

Algunos casos recientes confirman el valor creciente que las empresas otorgan a los perfiles de los consumidores. Las listas de clientes se venden o comparten, principalmente a través de la fusión de compañías de tecnología de la información que de este modo aumentan la cantidad de datos y perfiles a su disposición.

Finalmente, se darán adquisiciones basadas en datos del consumidor en las que éstos sean los activos primarios objeto de la compra. (...) Actualmente, los datos del consumidor constituyen, de muchas formas, la moneda de cambio del comercio electrónico. Dichos consumidores son clientes valiosos, pues han demostrado que compran y han comprado a la competencia. (...) Los nombres existentes en una base de datos permiten a las empresas importantes ahorros situados en torno a 100 USD por cliente 28 en publicidad destinada a conseguir nuevos clientes.

Los datos de los clientes también se ponen a la venta cuando quiebran las empresas de Internet. Recientemente, una empresa de juguetes ha incluido en su liquidación la venta de los perfiles de sus clientes. Estos perfiles se recopilaron de acuerdo con una política de privacidad consistente en no comunicar nunca dicha información a terceros sin el consentimiento expreso del cliente. Los perfiles contenían el nombre, la dirección, datos de facturación, información sobre el comportamiento de compra y el perfil familiar, con los nombres y las fechas de nacimiento de los hijos.

El 8 de agosto de 2000, TRUSTe, que había aprobado la política de privacidad de la empresa, anunció que había presentado una reclamación ante el Tribunal de quiebras de los Estados Unidos en contra del consentimiento de la Comisión federal de comercio a las condiciones de liquidación de los activos de la empresa 29 .

Una política completa de protección de la privacidad debe tener en cuenta el equilibrio entre los intereses económicos y los derechos humanos.

Quedan por resolver dos grandes cuestiones:

* Se ha recabado en Internet gran cantidad de datos personales sobre usuarios de la Red sin el conocimiento y/o el consentimiento previo de sus titulares, debido principalmente a los efectos secundarios invisibles de la tecnología Internet. Es probable que en los próximos años aumente el intercambio de datos personales con fines lucrativos 30 , pero ¨hasta dónde llegará el usuario de Internet en esta práctica? ¨Qué tipo de información personal puede compartir el propio titular, por cuánto tiempo y en qué circunstancias?

* Si la financiación de determinados sitios web, como los motores de búsqueda, se realiza principalmente con cargo a la industria del cibermarketing, puede existir la tentación de recurrir a elaborar perfiles personalizados para garantizar que servicios hasta entonces gratuitos excluyan a quienes no dispongan de un nivel suficiente de ingresos, no hayan respondido a cientos de *pancartas* publicitarias o deseen proteger su privacidad.

VI. Conclusiones

* Internet se concibió como una red mundial abierta (www) a través de la cual se podría compartir información. Sin embargo, es necesario encontrar un equilibrio entre el "carácter abierto" de Internet y la protección de los datos personales de los usuarios de la Red.

* Con frecuencia se recaba en Internet gran cantidad de información sobre los usuarios de la Red sin que ellos lo sepan. Es necesario tratar esta falta de transparencia con los usuarios de Internet, con el fin de alcanzar un grado aceptable de protección del consumidor y de sus datos personales.

* Los *protocolos* son medios técnicos que determinan la forma en que se recogen y se tratan los datos. Los navegadores y el software desempeñan también un papel importante. En algunos casos están dotados de un identificador que permite relacionar al usuario de Internet con sus actividades en la Red.

Por lo tanto, corresponde a los agentes que intervienen en su diseño y su desarrollo ofrecer al usuario productos que respeten la privacidad. En ese sentido, conviene señalar que el artículo 14 del proyecto de Directiva sobre telecomunicaciones de 12 de julio de 2000 afirma que, cuando sea preciso, la Comisión deberá adoptar medidas destinadas a asegurar que los equipos técnicos incorporan las garantías necesarias para proteger la información de carácter personal y la privacidad de los usuarios y abonados.

CAPÍTULO 3: APLICACIÓN DE LA LEGISLACIÓN RELATIVA A LA PROTECCIÓN DE DATOS

I. Cuestiones jurídicas generales

El análisis jurídico de los distintos fenómenos existentes que se presenta en los próximos capítulos se basa en que las dos Directivas sobre protección de datos (Directiva 95/46/CE y Directiva 97/66/CE) se aplican en principio a los datos de carácter personal tratados en Internet 31 .

Todas las consideraciones jurídicas que aparecen en este documento se basan en la interpretación de estas Directivas, así como en los documentos adoptados por el Grupo de Trabajo y, cuando así se indica, en la jurisprudencia del Tribunal Europeo de Derechos Humanos.

Datos personales en Internet

Como ya se ha mencionado en este documento, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP,

pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los *proveedores de servicios de Internet* que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva 32 .

En otros casos, un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo.

Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones IP estáticas.

Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como *cookies* con un identificador único o sistemas modernos de *minería de datos* unidos a bases de datos con información sobre usuarios de Internet que permite su identificación.

Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, este documento parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, en Internet se tratan grandes cantidades de información personal para la cual son de aplicación las Directivas sobre protección de datos.

Aplicación de las Directivas

Como ya ha afirmado con anterioridad el Grupo de Trabajo, la Directiva general 95/46/CE sobre protección de datos se aplica a todo tratamiento de datos de carácter personal que entre en su ámbito de aplicación, independientemente de los medios técnicos utilizados. Por consiguiente, el tratamiento de datos personales en Internet ha de considerarse a la luz de esta Directiva 33 .

Así pues, la Directiva general resulta aplicable en todos los casos y a todos los agentes mencionados en la primera parte de este capítulo (descripción técnica).

La Directiva específica 97/66/CE relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones detalla y completa la Directiva general 95/46/CE, pues fija disposiciones técnicas y jurídicas específicas. La Directiva 97/66/CE se aplica al tratamiento de datos de carácter personal en relación con la prestación de servicios públicos de telecomunicación en redes públicas de telecomunicaciones dentro de la Comunidad. Los servicios de Internet son servicios de telecomunicaciones, por lo que Internet queda incluido en el sector de las telecomunicaciones.

La Directiva 95/46/CE se aplica a todas las cuestiones que no quedan específicamente cubiertas por la Directiva 97/66/CE, tales como las obligaciones relativas al responsable y los derechos individuales, o los servicios de telecomunicaciones no públicos 34 . Los datos personales que el usuario de Internet proporciona de forma voluntaria durante su conexión a la Red corresponderán siempre al ámbito de aplicación de esta Directiva.

La tabla siguiente intenta definir los casos en que la Directiva específica 97/66/CE es de aplicación y aquéllos en que lo es la Directiva 95/46/CE, así como establecer los principios más pertinentes. Sin embargo, se ha de tener en cuenta que cuando los agentes desempeñan varios papeles al mismo tiempo se producirá cierta superposición.

M31.BMP;

Es evidente que la clave para decidir si las dos Directivas son o no aplicables radica en determinar si el servicio prestado puede considerarse un "servicio de telecomunicación" conforme a la definición recogida en la letra d) del artículo 2 de la Directiva 97/66/CE: *la transmisión y el envío de señales a través de redes de telecomunicación.*

Si la Directiva específica sobre telecomunicaciones es de aplicación, se han de adoptar las normas específicas de ésta.

Proveedor de telecomunicaciones

No cabe duda de que la conexión de un usuario de Internet a un *proveedor de servicios de Internet* que preste servicios de Internet y encamine las solicitudes y las respuestas de los usuarios a los servidores de sitios web y viceversa constituye un servicio de telecomunicaciones. Por lo tanto, la Directiva 97/66/CE es aplicable a los proveedores de telecomunicaciones, a los *proveedores de servicios de Internet* y a los proveedores de líneas y de *encaminadores* destinados al tráfico de Internet.

Proveedores de servicios de Internet (incluidos los proveedores de acceso a Internet) Lo mismo puede decirse de los *proveedores de servicios de Internet* : no cabe duda de que la Directiva específica sobre telecomunicaciones es también aplicable a sus actividades.

Un caso interesante es el de las instituciones o personas que tienen acceso directo a Internet sin necesidad de recurrir a un *proveedor de servicios de Internet*. Estas instituciones actúan en realidad como *proveedores de servicios de Internet* que conectan su propia red privada a Internet.

El artículo 3 de la Directiva 97/66/CE define su ámbito de aplicación especificando que afecta a los servicios públicos de telecomunicación en las redes públicas de telecomunicación en la Comunidad. En el caso mencionado no se trata de una red pública, sino de una red privada para un grupo determinado de usuarios. Así pues, se puede concluir que, pese a responder a la definición de servicios de telecomunicación, esos servicios no se pueden considerar públicos y, por lo tanto, no corresponden al ámbito de aplicación de la Directiva 97/66/CE.

Es importante señalar que, en tales casos, lo dispuesto en la Directiva específica podría aplicarse de nuevo si la información se enviase fuera de la red privada.

Obviamente, la Directiva general sobre protección de datos resulta plenamente aplicable en estos casos.

Sitios web muy visitados

En general, un sitio web está alojado en un *proveedor de servicios de Internet* (por ejemplo, el sitio web del Consejo de Europa), lo que significa que su responsable arrienda a un *proveedor de servicios de Internet* cierta capacidad de almacenamiento para instalar su sitio web y ponerlo a disposición del público.

Asimismo, implica que el *proveedor de servicios de Internet* responde a las peticiones de páginas web de los usuarios de Internet en nombre del Consejo de Europa.

En consecuencia, la persona que "administra" el sitio web (en este caso, el Consejo de Europa) sólo decide sobre la información que se publicará en el sitio web, pero no realiza ningún tipo de operación *que conlleve la transmisión o el encaminamiento de señales en las redes de telecomunicació* n.

En el caso de los sitios web en los que pueden solicitarse bienes o servicios, quien los suministre será el responsable del sitio. Sin embargo, cuando se trate de servicios de telecomunicación como tales, normalmente los suministrará el *proveedor de servicios de Interne*t, y no el responsable del sitio web.

Por lo tanto se puede afirmar que los sitios web contratan servicios de telecomunicación (transmisión) del *proveedor de servicios de Interne*t, pero que no realizan ningún servicio ellos mismos. La Directiva 97/66/CE es aplicable al *proveedor de servicios de Internet* como tal, pero no a los sitios web, que corresponden al ámbito de aplicación de la Directiva general.

Servicios de portal

Un *portal* ofrece una presentación ordenada de enlaces. El usuario de Internet puede visitar fácilmente determinados sitios web de otros proveedores de contenidos a través del *portal* visitado.

Los *portales* están alojados en *proveedores de servicios de Interne*t. En algunos casos, el *portal* pertenece al *proveedor de servicio*s, como sucede con Worldonline.nl; en otros, el *proveedor de servicios de Internet* aloja el *portal* para un tercero que proporciona los contenidos.

En ambos casos, quien presta el servicio de telecomunicación es el *proveedor de servicios de Internet,* tal como se define en el artículo 2 de la Directiva 97/66/CE, y es a él a quien se aplica dicha Directiva, y no al proveedor de contenidos.

Servicios adicionales

El proveedor de servicios adicionales no siempre queda dentro del ámbito de aplicación de la Directiva sobre protección de la intimidad y telecomunicaciones.

Algunos de estos proveedores de servicios, como Nedstat, tratan datos recabados de sitios web y los vuelven a vender a los propietarios de los sitios.

Los datos que tratan proceden de Internet, pero en principio su actividad no implica *la transmisión o el encaminamiento de señales en redes de telecomunicació* n.

Por lo tanto, no desempeñan un papel fundamental en el proceso de telecomunicación entre el usuario de Internet y el sitio web. Si los datos que procesan sólo consisten en datos agregados no identificables, se podría incluso decir que no corresponden al ámbito de aplicación de la Directiva general, pues no entra en juego ningún dato de carácter personal.

Agentes como Doubleclick, Engage o Globaltrash colocan anuncios en páginas solicitadas. Normalmente existe un contrato entre estos anunciantes y el *proveedor de servicios de Internet* que aloja las páginas web en las que se muestra la publicidad.

Técnicamente, cada vez que se accede a un sitio web éste contacta mediante un *hipervínculo* automático con el anunciante para que coloque *pancartas* en las páginas solicitadas.

Por otra parte, el anunciante puede colocar ficheros *cookie* en el disco duro del ordenador del usuario de Internet con objeto de elaborar perfiles de los visitantes del sitio y personalizar así las *pancartas* que aparecen en la página web 36 .

No está claro si las actividades básicas de Doubleclick, Engage y otros anunciantes pueden considerarse servicios de telecomunicación o no.

Parece ser que no transmiten ni encaminan señales de acuerdo con la definición del artículo 2 de la Directiva de telecomunicaciones, sino que ofrecen contenidos informativos que se colocan en las páginas web solicitadas utilizando las redes y las infraestructuras de telecomunicación existentes.

En cualquier caso, éste es un buen ejemplo de una situación en la que resulta difícil aplicar la definición vigente de servicios de telecomunicación a servicios relacionados con Internet.

II. Revisión de la Directiva de telecomunicaciones: definición de "servicios de comunicación electrónica"

La Comisión Europea anunció en una Comunicación de 1999 37 su intención de llevar a cabo una revisión general del marco jurídico vigente aplicable a las telecomunicaciones en Europa. En el transcurso de esta revisión general se examinará y actualizará también la Directiva vigente sobre tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones.

El Grupo de Trabajo del artículo 29 ya publicó algunas reflexiones relacionadas con esta revisión en su dictamen 2/2000, presentado por el Grupo operativo sobre Internet y aprobado el 3 de febrero de 2000 38 .

El texto de la Comunicación de la Comisión Europea destacaba que la revisión prevista prestaría especial atención a la terminología utilizada en la Directiva 97/66/CE, con el fin de aclarar que los nuevos servicios y tecnologías quedan cubiertos por esta Directiva, con lo que se evitarán posibles ambigüedades y se facilitará la aplicación coherente de los principios sobre protección de datos. En su dictamen 2/2000, el Grupo de Trabajo juzgó favorablemente la revisión de la terminología con este fin.

La Comisión publicó la propuesta de Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas 39 . En su comunicado de prensa 40 , la institución subraya que uno de los objetivos del nuevo paquete es garantizar la protección del derecho a la privacidad en Internet.

Esta propuesta ya no habla de "servicios de telecomunicación", sino de "servicios de comunicaciones electrónicas". La exposición de motivos de la propuesta afirma que este cambio era necesario para adaptar la terminología a la propuesta de Directiva y establecer un marco común de las redes y los servicios de comunicaciones electrónicas 41 .

La expresión "servicios de comunicaciones electrónicas" no se define en la propuesta de Directiva de intimidad y telecomunicaciones, sino en la letra b) del artículo 2 de la propuesta de Directiva, que establece un marco común de las redes y los servicios de comunicaciones electrónicas.

La nueva definición reza: *(Se entenderá por) "servicio de comunicaciones electrónicas", el prestado contra remuneración que consiste, en su totalidad o principalmente, en la transmisión y encaminamiento de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante el uso de redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos."*

De hecho, la nueva definición se basa en la misma idea que la anterior (la transmisión y el encaminamiento de señales en servicios de comunicación electrónica), pero contiene una lista de servicios incluidos en la definición y excluidos de ella que resulta muy útil, pues aclara los debates esbozados en el apartado anterior.

De esta lista incorporada a la nueva definición se puede concluir que los servidores de contenidos transmitidos a través de redes y servicios de comunicación electrónica no pertenecerán al ámbito de aplicación de la Directiva revisada sobre intimidad y telecomunicaciones. Así se confirma en el preámbulo de la propuesta de Directiva, que establece un marco común para las redes y los servicios de comunicación electrónica (séptimo considerando) en el que se afirma que *es necesario separar la regulación de la transmisión de la regulación de los contenidos.* Sin embargo, se acepta que esta separación no debe pasar por alto las relaciones existentes entre ellas.

La consecuencia más importante de esta separación es que servicios adicionales, tales como DoubleClick o los que suministran contenidos a un *portal* o a un sitio web (sin alojarlos), no quedan cubiertos por esta Directiva, sino simplemente por la Directiva general. También significa que los *proveedores de servicios de Internet* quedan dentro del ámbito de aplicación de la Directiva específica siempre que actúen como proveedores de acceso y ofrezcan conexión a Internet, pero que cuando actúen como proveedores de contenidos sólo se les aplicará la Directiva general 42 .

La ventaja que ofrece una división clara entre las normas referentes a los contenidos y las relativas a la transmisión es la claridad. Sin embargo, en la práctica resultará más difícil aplicar dicha separación. Pensemos, por ejemplo, en el caso de un *proveedor de servicios de Internet* que ofrezca también contenidos alojando su propio *portal*. Este *proveedor* deberá aplicar la Directiva general a todas sus actividades y la Directiva específica (que impone obligaciones específicas) a las actividades en las que actúa como proveedor de acceso.

Otro aspecto interesante de la nueva definición de "servicios de comunicaciones electrónicas" es la referencia a la remuneración por el servicio. Ni en el preámbulo ni en la exposición de motivos se menciona la inclusión de este término y tampoco se orienta sobre cómo interpretarlo. Una posible interpretación sería que los proveedores de acceso

gratuito a Internet quedarían fuera del ámbito de aplicación de la Directiva revisada sobre intimidad y telecomunicaciones, ya que no perciben remuneración alguna, o al menos no financiera, de los usuarios de Internet.

Sin embargo, esta interpretación no es correcta, pues en la jurisprudencia del Tribunal Europeo de Justicia se menciona claramente que, en relación con los servicios en el sentido del artículo 50 (antiguo artículo 60) del Tratado CE 43 , no es necesario que la remuneración vaya a cargo del beneficiario del servicio, pues también puede corresponder, por ejemplo, a los anunciantes.

En el caso de los proveedores de acceso gratuito a Internet, de hecho quienes ofrecen una remuneración a los proveedores son quienes colocan anuncios o *pancartas* en páginas de Internet. Así pues, queda claro que estos servicios quedan cubiertos por la definición de servicios de comunicación electrónica y, por lo tanto, corresponden al ámbito de aplicación de la Directiva.

No obstante, sería aconsejable aclarar esta cuestión en el texto de la Directiva, pues no todos los lectores están al corriente de la interpretación que el Tribunal Europeo de Justicia ha dado de este término. Esto se podría hacer, por ejemplo, en el preámbulo de la Directiva.

III. Otras disposiciones jurídicas aplicables

Existen otros reglamentos comunitarios que tratan algunos aspectos relacionados con Internet. Cabe mencionar los siguientes instrumentos: la Directiva 1999/93/CE por la que se establece un marco comunitario para la *firma electrónica* 44 , la Directiva 97/7/CE relativa a la protección de los consumidores en materia de contratos a distancia 45 y la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información (Directiva sobre el comercio electrónico)46 .

Sin embargo, la mayoría de estos reglamentos no establecen normas completas y específicas sobre protección de datos y en la mayor parte de los casos dejan la regulación de esta cuestión en manos de las Directivas específicas.

Por ejemplo, en su considerando 14, la Directiva sobre el comercio electrónico dice que *"la protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva 95/46/CE y la Directiva 97/66/CE, que son enteramente aplicables a los servicios de la sociedad de la información (...) y, por tanto, no es necesario abordar este aspecto en la presente Directiva*", y, en la letra b) del punto 5 del artículo 1, que *"la presente Directiva no se aplicará a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE y 97/66/CE* ".

El considerando 14 de la Directiva sobre comercio electrónico subraya que *"la aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso anónimo de redes abiertas como Internet".*

No obstante, la Directiva sobre la *firma electrónica* establece, en su artículo 8, algunas normas específicas sobre protección de datos aplicables a los proveedores de servicios de certificación y a los organismos nacionales competentes en materia de acreditación o supervisión. Este artículo obliga a los Estados miembros a velar por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan los requisitos establecidos en la Directiva general sobre protección de datos. Además, esta disposición establece que los proveedores de servicios de certificación que expidan al público certificados únicamente puedan recabar datos personales directamente del titular de los datos o previo consentimiento explícito de éste, y sólo en la medida necesaria para la expedición y el mantenimiento del certificado. Los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento explícito de su titular.

De especial importancia es el apartado 3 del artículo 8 de esta Directiva, que estipula que, sin perjuicio de los efectos jurídicos concedidos a los seudónimos con arreglo al Derecho nacional, los Estados miembros no impedirán al proveedor de servicios de certificación que consigne en el certificado un seudónimo del firmante en lugar de su verdadero nombre.

El considerando 24 del preámbulo de esta Directiva destaca la importancia de que los proveedores de servicios de certificación observen la normativa sobre protección de datos y el respeto a la intimidad con objeto de aumentar la confianza del usuario en la comunicación y en el comercio electrónicos.

IV. Aplicación de las normativas nacionales sobre protección de datos y sus efectos internacionales

Las letras a) y b) del apartado 1 del artículo 4 de la Directiva regulan la aplicación de disposiciones nacionales de un Estado miembro cuando: - "el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable; - el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público".

La Directiva especifica que la noción de establecimiento implica el ejercicio efectivo y real de una actividad mediante una instalación estable, y que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto.

De acuerdo con lo establecido en la letra c) del apartado 1 del artículo 4 de la Directiva, los datos recogidos utilizando medios, automatizados o no, localizados en el territorio de la UE/EEE están sujetos a lo dispuesto en la normativa comunitaria sobre protección de datos.

El considerando 20 de esta Directiva amplía la explicación: "El hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; (considerando) que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva".

Aunque la interpretación de la noción de "equipos" o "medios" ha suscitado un debate sobre su alcance, determinados ejemplos quedan indudablemente dentro del ámbito de aplicación del artículo 4. Éste será el caso, por ejemplo, de un fichero de texto instalado en el disco duro de un ordenador que recibirá, almacenará y devolverá información a un servidor ubicado en otro país. Dichos ficheros de texto, conocidos como *cookie*s, se utilizan para recabar datos para un tercero. Si el ordenador se encuentra en un país de la UE y el tercero está fuera de la Comunidad, éste último aplicará los principios del Derecho nacional de ese Estado miembro a la recopilación de datos a través de la *cooki*e.

En tal caso, de conformidad con el apartado 1 del artículo 4, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

V. Conclusiones

- En Internet se procesan grandes cantidades de datos personales a los que se aplican las Directivas sobre protección de datos.

- La Directiva general es aplicable en todos los casos, mientras que la Directiva específica lo es a los servicios de telecomunicación.

Debido a la terminología utilizada en la Directiva 97/66/CE, a veces resulta difícil determinar si un servicio concreto se puede considerar de telecomunicación.

- La revisión del marco jurídico relativo a las telecomunicaciones ha ayudado a aclarar el ámbito de aplicación de la Directiva sobre intimidad y telecomunicaciones. Sin embargo, algunos aspectos pueden requerir aclaraciones adicionales, y especialmente la referencia a la necesidad de incluir la remuneración en la definición de servicios de comunicación electrónica. Para evitar posibles malentendidos en relación con el ámbito de aplicación de la Directiva, convendría recoger en su preámbulo la interpretación que el Tribunal Europeo de Justicia ha dado a este texto.

- La legislación europea sobre protección de datos debe aplicarse a los datos recabados con equipos, automatizados o no, situados en el territorio de la UE/EEE.

CAPÍTULO 4: CORREO ELECTRÓNICO

I. Introducción

No resulta fácil describir en pocas palabras la base técnica del correo electrónico, debido, principalmente, a los siguientes factores:

* Existen algunos *protocolos* oficiales pero, al igual que sucede con el *protocolo* HTTP, el grado de riesgo para la privacidad dependerá de cómo se ejecuten en la práctica.

Existen miles de programas de servidores o clientes de correo electrónico diferentes y parece sumamente difícil sacar conclusiones generales, pues no se dispone de datos fiables sobre su utilización.

* Las operaciones invisibles de tratamiento que realizan esos programas son, como ya indica la palabra "invisible", difíciles de detectar.

Además, los programas se están ampliando y complicando tanto que resulta casi imposible tener la certeza de que se han registrado todas las funciones, incluso las más ocultas.

En consecuencia, la descripción siguiente no puede considerarse exhaustiva y no siempre será representativa de lo que sucede diariamente en decenas de millones de ordenadores personales conectados a Internet en todo el mundo.

II. Agentes

Son varios los agentes que intervienen en el proceso de tratamiento de un mensaje de correo electrónico. Cada uno de ellos deberá tener en cuenta las cuestiones relativas a la protección de datos en cada fase del proceso. Estos agentes son 47 :

* El remitente del mensaje
* El destinatario del mensaje (titular de una dirección de correo electrónico)
* El proveedor del servicio de correo electrónico (servidor de correo que almacena el mensaje enviado a un usuario hasta que éste desea recibirlo)
* El proveedor de software que suministra al remitente el programa cliente de correo electrónico
* El proveedor de software que suministra al destinatario el programa cliente de correo electrónico
* El proveedor de software que suministra el programa servidor de correo.

III. Descripción técnica

Básicamente, un usuario que quiera utilizar el correo electrónico necesita:

* Un "programa cliente de correo electrónico", que es un programa instalado en el ordenador personal del usuario

* Una dirección de correo electrónico (una cuenta de correo electrónico)

* Una conexión a Internet.

Proceso de envío de un mensaje de correo electrónico

Existe una gran variedad de "programas clientes de correo electrónico", pero todos han de ceñirse a los estándares de Internet. El envío de un mensaje consta, básicamente, de los siguientes pasos:

* El usuario compone un mensaje en su "programa cliente de correo electrónico" y escribe en el campo del destinatario la dirección correspondiente.

* Al pulsar el botón "enviar" en el programa cliente de correo electrónico, un *proveedor de servicios de Internet* transferirá el mensaje al servidor de correo del destinatario, normalmente una organización, o al buzón de la cuenta de correo electrónico del usuario.

* Si el mensaje se envía al servidor de correo de una organización, éste lo transmitirá directamente al destinatario o, en su defecto, a un servidor de retransmisión ("retransmisión de salida").

* El mensaje puede pasar por distintos servidores de retransmisión hasta llegar al servidor de correo del destinatario.

* El destinatario estará directamente conectado al servidor de correo (por ejemplo, en una red de área local) o habrá de establecer una conexión para recibir el mensaje.

Direcciones de correo electrónico

Las direcciones de correo electrónico constan de dos partes separadas por el símbolo "&"; por ejemplo: john.smith&nowhere.com o subs34219&nowhere.org

* La parte derecha identifica el dominio en que el destinatario tiene la cuenta. Se trata en realidad de un nombre DNS referido a la dirección IP del servidor de correo.

* La parte izquierda describe la identificación única del destinatario. Es el nombre con el que el servidor de correo electrónico lo identifica. No existe ninguna obligación técnica de que sea el verdadero nombre del destinatario: puede consistir en un seudónimo escogido por el titular o un código arbitrario asignado por el servidor de correo en el proceso de registro.

Desde el punto de vista técnico, para enviar un mensaje de correo electrónico no es necesario identificarse. De hecho, sucede lo mismo que en el mundo real, donde una persona puede enviar una carta sin tener que dar su nombre. En el caso de la *buzonfia* ("spam"), en general el emisor no utilizará una cuenta de correo electrónico, sino que accederá directamente al *protocolo* SMTP, lo que le permitirá suprimir o modificar su dirección de correo electrónico.

Protocolos de correo electrónico

Además del *protocolo* TCP/IP, en el correo electrónico se utilizan otros dos *protocolo*s:

1. El primero es el *protocolo* simple de transferencia de correo (SMTP) y se utiliza para ENVIAR un correo de un cliente al servidor de correo del destinatario. El mensaje no se envía directamente al ordenador del destinatario, que puede no estar encendido o conectado a Internet cuando el emisor decida enviarlo. Esto significa que, para recibir un correo, el usuario de Internet debe disponer de un buzón de correo (una cuenta) en un servidor. El proveedor de servicios de

correo almacena el mensaje y espera a que el destinatario vaya a buscarlo.

2. El segundo es el *protocolo* POP y lo utiliza el destinatario para establecer una conexión con el servidor de correo y comprobar si tiene algún mensaje. Para ello, el destinatario tiene que introducir su nombre de buzón y su contraseña, de modo que nadie más pueda acceder a su correspondencia.

En general, los programas cliente de correo electrónico incluyen ambos *protocolo*s, pues es probable que un usuario de Internet que quiera enviar un mensaje desee igualmente recibir una respuesta.

IV. Riesgos para la privacidad

Determinadas cuestiones conllevan riesgos específicos para la privacidad.

Recopilación de direcciones de correo electrónico

Como ya se ha mencionado, la dirección de correo electrónico es un elemento indispensable para establecer una conexión. Pero por otra parte, es también una valiosa fuente de información que contiene datos personales del usuario. Por lo tanto, es útil conocer los distintos métodos de recogida de direcciones de correo electrónico.

Existen distintas formas de recopilar direcciones de correo electrónico:

* El proveedor del "programa cliente de correo electrónico", que se compra o se obtiene de forma gratuita, solicita al usuario que se registre.

* También es posible introducir en los programas un código que transmitirá al proveedor de software la dirección de correo electrónico del cliente sin que éste se entere (tratamiento invisible).

* En algunos navegadores se han detectado fallos en la seguridad que permiten a un sitio web conocer las direcciones de correo electrónico de sus visitantes. Ello se puede hacer a través de contenidos activos malignos que utilicen, por ejemplo, un *JavaScript.*

* También es posible configurar algunos navegadores para que envíen la dirección de correo electrónico como una contraseña anónima cuando se establecen conexiones FTP (sin embargo, ésta no es una configuración por defecto).

* Algunos sitios web pueden solicitar la dirección de correo electrónico en distintas situaciones (por ejemplo, los sitios comerciales a la hora de realizar un pedido, un registro previo para acceder a una sala de charla, etc.).

* Hay otros modos de recabar direcciones de correo electrónico en espacios públicos en Internet 48 .

* Existe la posibilidad de interceptar el correo electrónico durante la transmisión de un mensaje.

Datos sobre tráfico

Resulta esencial establecer una distinción entre el contenido de un correo electrónico y los datos sobre tráfico, que son los datos que los *protocolos* necesitan para realizar correctamente la transmisión del emisor al destinatario.

Los datos sobre tráfico constan, por una parte, de la información que proporciona el emisor (por ejemplo, la dirección de correo electrónico del destinatario), y por otra de información técnica generada de forma automática durante el procesamiento del mensaje (como la fecha y la hora de envío o el tipo y la versión del "programa cliente de correo electrónico").

Todos los datos sobre tráfico o parte de ellos se colocan en una cabecera que se transmite al destinatario junto con el mensaje. El servidor de correo del receptor y el "cliente de correo" utilizan las partes transferidas de los datos sobre tráfico para tratar correctamente el mensaje entrante. El destinatario podría usar los datos sobre tráfico (propiedades del correo electrónico) con fines analíticos, como comprobar el camino seguido por el mensaje en Internet.

Se considera que los siguientes datos quedan incluidos en la definición de "datos sobre tráfico":

* dirección de correo electrónico y dirección IP del emisor
* tipo, versión e idioma del programa cliente
* dirección de correo electrónico del receptor
* fecha y hora de envío del correo electrónico
* tamaño del correo electrónico
* conjunto de caracteres utilizado
* tema del mensaje (esto ofrece también información sobre el contenido de la comunicación)
* nombre, tamaño y tipo de los documentos adjuntos
* lista de retransmisores SMTP utilizados.

En la práctica, normalmente los servidores de correo electrónico del emisor y del receptor almacenan los datos sobre tráfico. Esto también podrían hacerlo los servidores de retransmisión en el camino de comunicación a través de Internet.

Dado que la Directiva 97/66/CE no define formalmente los datos sobre tráfico, conviene señalar que algunos agentes de Internet podrían considerar erróneamente que los datos personales que no son necesarios para la comunicación ni para la facturación pero se generan durante la transmisión son datos sobre tráfico que pueden almacenar.

En su Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación 49 , el Grupo de Trabajo del artículo 29 abordó algunos de los problemas de privacidad relacionados con datos sobre tráfico. El Grupo de Trabajo considera que los medios más eficaces para reducir riesgos inaceptables para la privacidad a la vez que se reconoce la necesidad de un cumplimiento efectivo de la legislación se basan en que los datos sobre tráfico no deberían, en principio, conservarse sólo con fines de cumplimiento de la ley, y en que las normativas nacionales no deberían obligar a los operadores de telecomunicaciones, a los servicios de telecomunicaciones y a los *proveedores de servicios de Internet* a guardar los datos sobre tráfico durante un tiempo superior al necesario para efectuar la facturación.

En la declaración oficial de la Conferencia de autoridades europeas de protección de datos, celebrada en Estocolmo en la primavera de 2000, se señaló que en los casos específicos en que se han de conservar datos sobre tráfico deberá existir una necesidad demostrable, el período de conservación deberá ser lo más breve posible y la práctica deberá estar claramente regulada por la ley.

Contenido del correo electrónico

La confidencialidad de las comunicaciones está protegida por el artículo 5 de la Directiva 97/66/CE. En virtud del mismo, ninguna persona distinta de los usuarios podrá leer el contenido de un correo electrónico entre dos partes. Si durante la transmisión el contenido del mensaje se almacena en servidores de retransmisión, debería borrarse tan pronto como haya sido enviado.

Si un servidor de retransmisión no puede enviar un correo electrónico, podrá almacenarlo durante un período de tiempo breve y limitado hasta que se devuelva al emisor junto con un mensaje de error que le informe de que el correo electrónico no se pudo hacer llegar al destinatario.

El contenido de un correo electrónico se almacena en el servidor de correo hasta que el programa cliente de correo electrónico del usuario solicita su entrega. En algunos casos, el usuario puede optar por dejar el mensaje almacenado en el servidor de correo a pesar de tener una copia propia. Si el usuario no se decide por esta posibilidad, el servidor deberá borrar el mensaje lo antes posible una vez que tenga la certeza de que el destinatario lo ha recibido.

Si se realiza un control antivirus en forma de análisis de contenidos, éste deberá llevarse a cabo de forma automática y sólo con ese fin. Los datos no deberán analizarse con ningún otro propósito ni comunicarse a nadie, ni siquiera si se detecta algún virus.

Otro riesgo para la privacidad asociado al correo electrónico está relacionado con la incapacidad del usuario de eliminar de un modo fácil y eficaz un mensaje que ha enviado o recibido, pues la función de borrar no suprimirá necesariamente un correo del sistema.

En ese caso puede resultar relativamente fácil para otro usuario del mismo ordenador o para un administrador del sistema, si se trata de un ordenador en red, recuperar un mensaje que el usuario original quería borrar y cree que ha desaparecido del sistema.

Aunque el problema no es exclusivo del correo electrónico, resulta especialmente significativo en este contexto. Para solucionarlo, los sistemas deberían diseñarse de manera que la función de borrar eliminase realmente la información del sistema.

Para controlar el tráfico de una red se puede utilizar tanto el hardware como el software.

Esto se conoce como *husmeo*. Los programas de *husmeo* pueden leer todos los paquetes de datos de una red y presentar en texto claro toda la comunicación no encriptada. La forma más sencilla de *husmeo* se puede realizar utilizando un ordenador personal normal conectado a una red, con programas que se pueden encontrar fácilmente.

Si el *husmeo* se realiza en nudos o empalmes centrales de Internet, esto permitiría interceptar y controlar a gran escala el contenido de mensajes de correo electrónico y los datos sobre tráfico de acuerdo con determinadas características, principalmente la presencia de palabras clave. Como actividad de control general y exploratoria, el *husmeo* sólo puede permitirse si se respetan las condiciones establecidas en el artículo 8 del Convenio Europeo de Derechos Humanos, aun cuando lo lleven a cabo organismos gubernamentales.

En este contexto, resulta interesante señalar las preocupaciones actuales existentes en todo el mundo sobre un posible control de las comunicaciones internacionales y, en particular, sobre el sistema de interceptación de satélites "Echelon". La supervisión internacional es actualmente una cuestión candente en el programa de trabajo del Parlamento Europeo 50 . En un informe dirigido al Director General de Estudios del Parlamento Europeo 51 sobre el desarrollo de las tecnologías de supervisión y el riesgo de abuso de la información económica, se menciona que el sistema "Echelon" ha existido durante más de veinte años. De acuerdo con este informe, Echelon utiliza intensamente las redes mundiales de comunicación de la NSA 52 y el GCHQ 53 similares a Internet para permitir que centros remotos de información interroguen a ordenadores en cada sitio dedicado a la recopilación y reciban los resultados de forma

automática.

Otro sistema de control polémico es Carnivore que, de acuerdo con la información publicada por el EPIC (Centro de Información sobre la Intimidad Electrónica)54 , controla el tráfico en las instalaciones de los *proveedores de servicios de Internet* con objeto de interceptar información de criminales sospechosos en el correo electrónico. El EPIC afirma que Carnivore podría analizar millones de mensajes de correo electrónico por segundo y permitir a los agentes encargados de velar por el cumplimiento de la ley interceptar todas las comunicaciones digitales de un cliente de un *proveedor de servicios de Interne*t. El Congreso de Estados Unidos, los medios de comunicación y la comunidad de defensa de la privacidad han planteado preguntas muy serias sobre la legalidad de Carnivore y los abusos que puede conllevar su uso. En respuesta a las protestas públicas relacionadas con Carnivore, el 27 de julio de 2000 la Fiscal General Janet Reno anunció que se permitiría el acceso de un "grupo de expertos" a las especificaciones técnicas del sistema, con objeto de aliviar la preocupación pública.

El debate sobre la vigilancia mundial de las comunicaciones también forma parte del programa de trabajo del Consejo de Europa. El 27 de abril de 2000, el Comité de expertos en delitos del ciberespacio publicó su "proyecto de Convenio sobre delincuencia en el ciberespacio"55 . Este Convenio obligaría a las empresas que ofrecen servicios de Internet a recoger y almacenar datos destinados a los organismos públicos encargados de velar por el cumplimiento de la ley, con lo que facilitaría la recopilación de información.

Sería necesario un intercambio de tales datos entre autoridades gubernamentales de distintos países, incluso los que no son parte en el Convenio Europeo de Derechos Humanos u otros instrumentos del Consejo de Europa o de la UE en materia de protección de datos. Hasta la fecha, no se ha previsto ningún requisito sustancial para proteger el derecho fundamental a la intimidad y la protección de los datos personales en terceros países que reciben datos de carácter personal sobre ciudadanos de la UE, y tampoco se han establecido los principios básicos para respetar las normas relativas a derechos humanos fundamentales como la necesidad y la proporcionalidad.

Aunque su intención no es comentar el texto del proyecto de Convenio, el Grupo de Trabajo desearía recordar el punto de vista presentado por las autoridades europeas de protección de datos en una declaración realizada en abril de 2000 durante la Conferencia de Estocolmo, en la que señalaron con preocupación que, según las propuestas presentadas, los *proveedores de servicios de Internet* deberían almacenar habitualmente los datos sobre tráfico no sólo con fines de facturación, con objeto de permitir un posible acceso de los organismos encargados de velar por el cumplimiento de la ley.

La Conferencia señaló que esta retención constituiría una invasión ilegal de los derechos fundamentales que garantiza el artículo 8 del Convenio Europeo de Derechos Humanos y declaró que en los casos específicos en que se hayan de conservar datos sobre tráfico, debería existir una necesidad demostrable, el período de conservación debería ser lo más breve posible y la práctica debería estar claramente regulada por la ley. En su Recomendación 2/99 56 , el Grupo de Trabajo del artículo 29 ha tratado los aspectos que afectan a la privacidad en la interceptación de las comunicaciones. En esta Recomendación, el Grupo de Trabajo señala que cualquier interceptación de las telecomunicaciones, definida como el conocimiento por un tercero de los datos sobre el contenido y el tráfico de las telecomunicaciones privadas entre dos o más corresponsales y, en especial, de los datos sobre tráfico relacionados con la utilización de servicios de telecomunicación, constituye una violación del derecho individual a la privacidad y a la confidencialidad de la correspondencia. De esto se desprende que las interceptaciones son inaceptables, a menos que cumplan tres criterios fundamentales, de conformidad con lo dispuesto en el apartado 2 del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales del 4 de noviembre de 1950 57 y de la interpretación que el Tribunal Europeo de Derechos Humanos ha hecho de esta disposición: un fundamento jurídico, la necesidad de la medida en una sociedad democrática y la conformidad con alguno de los objetivos legítimos enumerados del Convenio 58 .

V. Análisis de cuestiones especiales

Correo web

Los sistemas de correo electrónico que utilizan páginas web como interfaz se conocen como *"correo we*b" (por ejemplo, Yahoo, Hotmail, etc.). Se puede acceder al *correo web* desde cualquier lugar y el usuario no necesita conectarse a un determinado *proveedor de servicios de Interne*t, como cuando utiliza una cuenta normal de correo electrónico.

El *correo web* suele ser gratuito, pero para obtener su cuenta a menudo los usuarios se ven obligados a comunicar al proveedor datos personales. De acuerdo con las investigaciones realizadas por las autoridades responsables de la protección de datos, parece ser que muchos proveedores de *correo web* venden o comparten datos de carácter personal con fines comerciales.

El *correo web* utiliza el *protocolo* HTML, en lugar del POP, para leer y controlar el correo electrónico. De hecho, los mensajes se muestran en una página HTML clásica.

Esta característica permite al proveedor de servicios de correo incorporar anuncios personalizados en la página HTML en la que éste se presenta (gráficamente, fuera del propio mensaje). El *correo web* depende en gran medida de patrocinadores y visualiza gran cantidad de *pancartas* publicitarias.

Dado que los sistemas de *correo web* se basan en el *protocolo* HTTP, pueden ser vulnerables a los "Web bugs", que

permiten descubrir la identidad de correo electrónico de una persona mediante *cookies* y etiquetas HTML incrustadas.

Los proveedores de *correo web* no deben incorporar *hipervínculos* invisibles en páginas web en las que la cuenta de correo electrónico forma parte del URL. Si lo hacen, ayudan a transmitir la dirección de correo electrónico del titular de los datos a la empresa de publicidad. Ésta es otra forma de invasión de la privacidad del usuario con un tratamiento invisible.

Guías

Existen distintos servicios en Internet que ofrecen guías de direcciones de correo electrónico. Estas guías públicas están sujetas a las mismas normas que las telefónicas y otros datos a disposición del público, como se explicará en el capítulo 6. En el marco jurídico vigente, el usuario debe disponer al menos del derecho a oponerse al tratamiento de sus datos, de acuerdo con el artículo 14 de la Directiva 95/46/CE y con el artículo 11 de la Directiva 97/66/CE.

Cabe señalar que el borrador de la directiva revisada sobre el tratamiento de datos de carácter personal y la protección de la privacidad en el sector de las telecomunicaciones armoniza las obligaciones de los responsables de los datos a este respecto y ofrece a los titulares de dichos datos el derecho de aprobar su incorporación en guías. El Grupo de Trabajo considera que éste es un avance importante.

Buzonfia

La *buzonfia* se puede definir como el envío de correos electrónicos no solicitados, de naturaleza generalmente comercial, en grandes cantidades y de forma repetida a personas con las que el emisor no ha tenido ningún contacto previo 59 . El Grupo de Trabajo del artículo 29 ya abordó esta cuestión en su Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico 60 .

Desde el punto de vista de los ciudadanos, el problema presenta tres aspectos: en primer lugar, la recopilación de la dirección de correo electrónico de una persona sin su consentimiento o conocimiento; en segundo lugar, la recepción de grandes cantidades de publicidad no deseada, y por último, el coste del tiempo de conexión.

Las direcciones de correo electrónico pueden recabarse en guías públicas o empleando distintas técnicas. Por ejemplo, el propio usuario puede dar su dirección de correo electrónico al comprar bienes o servicios en Internet.

En otros casos, un proveedor puede vender a terceros la dirección que el usuario le ha proporcionado.

De acuerdo con el Grupo de Trabajo, las normas de la Directiva sobre protección de datos ofrecen una respuesta clara a las cuestiones sobre privacidad que plantea la *buzonfia* y establecen una imagen nítida de los derechos y obligaciones de los participantes. Conviene distinguir dos situaciones:

* Si una empresa obtiene una dirección de correo electrónico directamente de una persona con vistas a realizar un envío de correo electrónico comercial o a que lo realice un tercero al que ha revelado los datos, la empresa original debe informar a la persona de esos propósitos al recopilar la dirección 61 . Además, desde el momento en que comunica su dirección, el titular de los datos debe contar con el derecho mínimo de oponerse al uso de sus datos con medios electrónicos sencillos, como marcar una casilla prevista para este fin por la empresa original, en primer lugar, y por las empresas que han recibido datos de la empresa original, posteriormente 62 . Determinadas legislaciones nacionales de aplicación de las directivas pertinentes incluso obligan a la empresa a solicitar el consentimiento del titular de los datos. Los requisitos recogidos en el artículo de la Directiva sobre comercio electrónico referentes a las comunicaciones comerciales no solicitadas completan estas normas a escala técnica imponiendo la obligación de consultar un registro sobre el proveedor de servicios, sin perjuicio alguno de las obligaciones generales aplicables a los responsables de los datos.

* Si una dirección de correo electrónico se recaba en un espacio público en Internet, su uso para envío de correo electrónico comercial no solicitado podría incumplir la legislación comunitaria pertinente por tres motivos: en primer lugar, podría considerarse un tratamiento desleal de datos de carácter personal en virtud de la letra (a) del apartado 1 del artículo 6 de la Directiva general; en segundo lugar, iría en contra del "principio de finalidad" recogido en la letra (b) del apartado 1 del artículo 6 de dicha Directiva, pues el titular de los datos publicó su dirección de correo electrónico para un fin diferente, como la participación en un foro de debate; por último, teniendo en cuenta el desequilibrio de costes y las molestias que sufre el destinatario, el envío de dichos mensajes no podría considerarse satisfactorio de acuerdo con el equilibrio de intereses estipulado en la letra (f) del artículo 7 63 .

Una característica específica del envío de mensajes comerciales de correo electrónico es que, mientras que el coste para el emisor es muy reducido comparado con los métodos tradicionales de venta directa, implica un gasto para el receptor en términos de tiempo de conexión. Esta situación constituye un claro incentivo para utilizar esta herramienta de comercialización a gran escala sin prestar atención a las cuestiones relativas a la protección de datos y los problemas provocados por el correo electrónico comercial.

El coste del correo electrónico no solicitado recae tanto en el receptor como en el proveedor de correo Internet del receptor, que puede ser el servidor de *correo web* o el *proveedor de servicios de Internet* del destinatario.

El servidor de correo tiene que almacenar durante cierto tiempo los mensajes de correo electrónico no solicitados. Por su parte, el receptor ha de pagar 64 para descargar un mensaje que no desea leer y pierde tiempo clasificando los

mensajes recibidos y eliminando los no solicitados, sobre todo cuando los mensajes de *buzonfia* no aparecen identificados como tales en la casilla destinada al tema, lo que se suele hacer mediante un

código "ADV:" de anuncio en los primeros caracteres de dicha casilla. Se estima que la *buzonfia,* también conocida como correo basura, constituye actualmente el diez por ciento del total del correo electrónico mundial 65 .

VI. Aspectos de seguridad y confidencialidad

El correo electrónico ofrece las mismas posibilidades de comunicación que el tradicional, por lo que se le aplican las mismas normas que a la inviolabilidad de la correspondencia.

Todo el mundo tiene derecho a enviar un mensaje por correo electrónico a otra persona sin que un tercero lo lea. El artículo 5 de la Directiva 97/66/CE, que cubre las comunicaciones y los correspondientes datos sobre tráfico enviados, por ejemplo, por correo electrónico, establece las obligaciones aplicables a la confidencialidad de las comunicaciones. Junto con estas obligaciones, el artículo 4 de esa misma Directiva obliga a los proveedores de servicios públicos de telecomunicación a adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y a informar a los usuarios sobre un riesgo concreto de violación de la seguridad y sobre las posibles soluciones, incluidos los costes necesarios.

En el mundo no electrónico, cualquier persona puede enviar cartas anónimas o firmadas con un seudónimo. Para poder enviar un mensaje anónimo de correo electrónico, varios proveedores de este servicio ofrecen al abonado la posibilidad de obtener direcciones anónimas de correo electrónico.

Desde el punto de vista del usuario, son varias las cuestiones pertinentes según el tipo de correo electrónico:

* La confidencialidad, que es la protección de los datos transmitidos contra la curiosidad de terceros. Una posible forma de garantizar la confidencialidad consiste en *encriptar* el mensaje que se va a enviar.

La *encriptación* y la desencriptación se basan en software complementario de los programas habituales de correo electrónico (programas accesorios) o en programas de correo electrónico y navegadores que ofrecen estos servicios.

La resistencia de la *encriptación* depende de los algoritmos y la longitud de las claves utilizadas.

* La *integridad,* que es una garantía de que la información no sufrirá alteraciones de forma accidental o intencionada. La *integridad* puede obtenerse calculando un código especial basado en el texto que se transferirá encriptado junto con el propio texto. El receptor podrá entonces descifrar el código y, volviéndolo a calcular, comprobar si el mensaje ha sido modificado.

* La *autentificación,* que garantiza que un usuario es realmente quien afirma ser.

La *autentificación* se puede verificar mediante el intercambio de *firmas digitales* basadas en *certificados electrónico*s. No es necesario que dichos certificados mencionen el verdadero nombre del abonado, que, en virtud de lo establecido en el artículo 8 de la Directiva relativa a la *firma electrónica* 66 , puede sustituirse por un seudónimo.

VII. Medidas en favor de la privacidad67

Dos tipos de herramientas merecen una mención especial en este capítulo: los filtros de correo electrónico y el correo electrónico anónimo 68 .

1) Los filtros de correo electrónico analizan todo el correo electrónico entrante de un usuario y sólo dejan pasar los mensajes que éste ha indicado que desearía recibir. Está muy extendido el uso de estos sistemas para eliminar la *buzonfi*a.

Actualmente varias empresas ofrecen herramientas que los usuarios de Internet pueden instalar en sus ordenadores para descartar el correo electrónico no deseado. Además, varios paquetes de correo electrónico permiten a los abonados filtrar los mensajes conforme aparecen en el escritorio.

Los filtros más eficaces son los que permiten la entrada exclusiva de determinados mensajes de correo electrónico. Sin embargo, aunque este sistema es útil para las personas que disponen de una red permanente de corresponsales de correo electrónico, resultaría incómodo para la mayoría de la población, pues requeriría la aprobación de cada nuevo corresponsal.

Las tecnologías de filtrado más habituales permiten la entrada de todos los mensajes excepto los que proceden de determinados nombres de dominio o direcciones o los que contienen determinadas palabras clave en la línea destinada al tema. Sin embargo, los emisores pertinaces modifican a menudo su nombre de dominio o su dirección para poder atravesar los filtros, pues normalmente las cuentas de correo electrónico basadas en la Web son gratuitas y resulta sencillo incorporarse a ellas o dejarlas en cualquier momento. Por último, debido a las elevadas posibilidades de error, resulta difícil realizar un filtrado eficaz utilizando palabras clave.

2) El correo electrónico anónimo permite a los usuarios comunicar en línea su dirección de correo electrónico sin tener que revelar su identidad 69 . Actualmente se puede disponer de este servicio de forma gratuita en Internet gracias a varias empresas que realizan servicios de "reenvío".

Con estos servicios, el responsable del reenvío elimina la identidad del usuario de los mensajes que éste ha enviado. Las respuestas al correo electrónico anónimo van al responsable del reenvío, quien vincula la dirección anónima a la verdadera y entrega la respuesta al cliente de un modo seguro.

VIII. Conclusiones

Desde el punto de vista de la protección de datos, se deben abordar las siguientes cuestiones relacionadas con el correo electrónico:

Tratamiento invisible realizado por "clientes de correo" y retransmisores SMTP

El titular de los datos debería disponer de la oportunidad de permanecer en el anonimato en la mayor medida posible, sobre todo cuando participa en un foro de debate. Parece ser que junto con el contenido del mensaje a menudo se envían las direcciones de correo electrónico de los participantes en estos foros 70 . Esto contraviene el artículo 6 de la Directiva 95/46/CE, que limita el tratamiento de la información a los casos en que sea necesario con fines legítimos 71 .

Conservación de datos sobre tráfico por intermediarios y proveedores de servicios de correo En virtud del artículo 6 de la Directiva 97/66/CE, los datos sobre tráfico deberán destruirse en cuanto termine la comunicación. La Directiva sólo establece determinadas excepciones a este principio, por ejemplo, cuando es necesario realizar un tratamiento mayor para efectuar la facturación 72 .

Interceptación

La interceptación del correo electrónico (la comunicación y los correspondientes datos sobre tráfico) es ilegal, a menos que así se haya dispuesto por ley en circunstancias concretas de acuerdo con el Convenio Europeo de Derechos Humanos y la Directiva 97/66/CE. En cualquier caso, debe prohibirse el *husmeo* a gran escala. El principio de especificidad, corolario de la prohibición de toda vigilancia general o exploratoria, implica que, en lo que respecta a los datos sobre tráfico, las autoridades públicas sólo pueden acceder a los datos sobre tráfico de forma individual y nunca de forma proactiva ni como norma general 73 .

Almacenamiento y análisis del contenido del correo electrónico

El contenido del correo electrónico debe mantenerse en secreto y se ha de impedir que los intermediarios y proveedores de servicios de correo puedan leerlo, incluso con "fines de seguridad en la red". Si se utiliza un programa antivirus para analizar documentos adjuntos, éste debe ofrecer suficientes garantías de confidencialidad. Si se detecta algún virus, el proveedor de servicios deberá tener la capacidad necesaria para avisar al emisor, pero ni siquiera en este caso deberá leer el contenido del mensaje ni de los documentos adjuntos.

El Grupo de Trabajo del artículo 29 recomienda encarecidamente la *encriptación* del contenido del correo electrónico, sobre todo cuando contiene información delicada de carácter personal. Los proveedores de servicios de correo electrónico deberían poner a disposición del público herramientas gratuitas de fácil utilización para encriptar el contenido de los mensajes. Además, los proveedores deberían ofrecer al abonado la oportunidad de descargar el correo desde el servidor del proveedor al ordenador cliente del usuario con una conexión segura. Debería tenerse igualmente en cuenta la necesidad de *integridad* y *autentificación*.

Correo electrónico no solicitado *(buzonfia)*

Si una empresa obtiene una dirección de correo electrónico directamente de una persona con vistas a realizar un envío de correo electrónico comercial no solicitado o a que lo realice un tercero al que ha revelado los datos, la empresa original debe informar a la persona de esos propósitos al recopilar la dirección.

Además, desde el momento en que comunica su dirección el titular de los datos debe contar con el derecho mínimo de oponerse al uso de éstos con medios electrónicos sencillos, como marcar una casilla prevista para este fin por la empresa original, en primer lugar, y por las empresas que han recibido datos de la empresa original, posteriormente Si una dirección de correo electrónico se recaba en un espacio público en Internet, su uso para envío de correo electrónico comercial no solicitado podría incumplir la legislación comunitaria pertinente.

Guías de correo electrónico

Al igual que sucede con las guías telefónicas, el titular de los datos debe tener la posibilidad de decidir su exclusión de las mismas en virtud de los principios anteriormente mencionados de limitación de finalidad (letra b del apartado 1 del artículo 6 de la Directiva 95/46/CE) y del derecho a solicitar que no se le incluya en una guía (artículo 11 de la Directiva 97/66/CE). Además, se debería ofrecer al titular de los datos la posibilidad de aparecer en una guía especial de direcciones de correo electrónico que no se pueda utilizar con fines de venta directa.

Es importante tener en cuenta que en la versión actual de la propuesta de Directiva relativa a la protección de la inti-

midad en el sector de las telecomunicaciones este derecho de exclusión se transformará en un derecho de consentimiento, lo que constituye un avance importante a favor de los titulares de los datos.

CAPÍTULO 5: NAVEGACIÓN Y BÚSQUEDA

I. Introducción

Tal vez la actividad más habitual de los usuarios de Internet consiste en visitar páginas web con el fin de obtener información, lo que conlleva la visualización pasiva de su contenido. También es posible interactuar con los sitios web de un modo más activo. A menudo, el usuario de Internet ha de pulsar en un *hipervínculo*, entrar en un anuncio de la pantalla *(pancarta)* o completar un formulario con más información. El conjunto de estas actividades se denominará "navegación por la Web". En la práctica, esto se realiza mediante un navegador que conecta al usuario de Internet con un servidor web en alguna parte de Internet.

Desde el punto de vista de la protección de datos, cabe plantear tres cuestiones:

* ¨Qué información se genera sobre las actividades del usuario de Internet mientras éste navega por la Web?

* ¨Dónde se almacena esta información?

* ¨Qué información es necesaria para la prestación de los servicios que ofrecen los sitios web? La última cuestión, que se refiere a los datos personales que un usuario de Internet comunica de forma voluntaria y a las condiciones en que los revela, no se tratará aquí, pues este capítulo se centra en las informaciones personales inherentes al proceso (técnico) de navegar por Internet y ofrece un esquema de las etapas posteriores en el proceso de navegación, así como una indicación de los datos de carácter personal que se generan.

II. Descripción técnica y agentes participantes

El proceso de navegación por la Web

* Proveedores de telecomunicaciones.

Para contactar con un sitio web, normalmente un usuario de Internet entra en la Red a través de una conexión telefónica con un *proveedor de servicios de Internet*. El proveedor de telecomunicaciones registra la llamada al *proveedor de servicios de Internet*.

* Proveedor de acceso a Internet.

El punto de entrada al *proveedor de servicios de Internet* es el servidor de acceso a la red. Por lo general, este servidor registra la *identificación de la línea de llamada* que solicita la conexión. La mayoría de los proveedores de acceso a Internet registran también el nombre de conexión, la hora de conexión y desconexión y la cantidad de datos transferidos en el transcurso de la sesión.

Conviene señalar que, en algunos casos, el proveedor de acceso a Internet es también el proveedor de telecomunicaciones.

* Asignación de la dirección IP.

Una vez establecido contacto con el proveedor de acceso a Internet, éste asigna una dirección IP dinámica para la sesión del usuario de Internet 74 .

Desde entonces, todas las comunicaciones de la sesión se realizan desde y hacia esa dirección IP. El número IP acompaña a todos los paquetes transmitidos en las etapas siguientes de comunicación. El número IP asignado pertenece siempre a un conjunto determinado de números asignado al proveedor de acceso a Internet. Así, terceras partes externas pueden identificar fácilmente al *proveedor de servicios de Internet* del que provienen los paquetes IP 75, 76 .

Posteriormente, el tráfico de Internet se clasifica en el *proveedor de servicios de Internet* por el número de puerto, que especifica el servicio y el *protocolo* correspondiente. En general, las solicitudes para visitar un sitio web se realizan mediante el *protocolo* HTTP.

En el *proveedor de servicios de Internet*, este tráfico se reconoce por un número de puerto determinado. También puede transferirse directamente a un *encaminador* que conecta al usuario de la Red con los sitios web externos solicitados.

A menudo, la solicitud se transmite a un *servidor proxy* dedicado que registra la solicitud de un determinado sitio web. El *servidor proxy* guarda una copia del contenido de los sitios web más visitados. Si el sitio solicitado por el usuario de Internet se encuentra en el *servidor proxy*, éste sólo tiene que pedir al sitio correspondiente una actualización con los cambios que se hayan producido desde el momento en que se almacenó la copia. Esta medida reduce enormemente

la cantidad de datos que han de intercambiar el *proveedor de servicios de Internet* y el sitio web, porque basta con que se comuniquen cambios y no páginas completas. El *servidor proxy* puede mantener una lista pormenorizada de visitas a sitios web conectados a una dirección IP en un momento determinado. Éstas pueden relacionarse con un usuario en particular mediante la dirección IP y el registro de las horas de la sesión.

* *Encaminadore*s. En su camino entre el *proveedor de servicios de Internet* y el sitio web visitado, por lo general el tráfico pasa por varios *encaminadores* que dirigen los datos entre la dirección IP del usuario de Internet y la dirección IP del sitio web. Respecto al almacenamiento de datos de carácter personal, estos *encaminadores* se consideran elementos neutrales, aunque se puedan aplicar en ellos recursos dedicados destinados a interceptar el tráfico de Internet.

* Sitios web muy visitados. Una vez establecida la conexión con el sitio web, éste recaba información sobre el usuario de Internet que lo visita.

Todas las solicitudes van acompañadas de la dirección IP de destino. El sitio web sabe igualmente desde qué página ha llegado el usuario, es decir, conoce la referencia de la página previa o URL. La información sobre las visitas al sitio web se almacena habitualmente en el "fichero histórico común". Todos los datos mencionados anteriormente pueden utilizarse con el fin de acumular, mediante un analizador de registros, información sobre el tráfico procedente de un sitio web o con destino a éste, así como sobre las actividades de los visitantes.

Tras conectar con un sitio web, en la comunicación entre los programas de navegación más utilizados por los usuarios de Internet y los sitios web visitados se recoge información adicional. Esto se conoce como "datos de charloteo", que suelen constar de los siguientes elementos 77 : - Sistema operativo - Tipo y versión del navegador - *Protocolos* utili - zados en la navegación - Página remitente

- Preferencias de idioma

- *Cookies*

La instalación de *cookies* 78 permite al sitio web disponer de mayor capacidad de recogida de información. Se trata de datos que pueden almacenarse en ficheros de texto en el disco duro del usuario y de los que el sitio web puede conservar una copia. Forman parte del tráfico HTTP, por lo que se pueden transportar sin problemas con el tráfico IP. Una *cookie* puede contener un número único (identificador global único) que permite realizar una mejor identificación que las direcciones IP dinámicas.

Estas *cookies* aumentan la capacidad de los sitios web de almacenar y "personalizar" la información sobre sus visi - tantes. El sitio puede releer la *cookie* de forma periódica con objeto de identificar a un usuario de Internet y reconocerlo cuando vuelva a visitar el sitio, comprobar posibles contraseñas, analizar el camino que ha seguido durante una sesión y dentro de un sitio, registrar transacciones (por ejemplo, adquisición de artículos), personalizar un sitio, etc.

Existen *cookies* de distinta naturaleza: las hay permanentes y de duración limitada, en cuyo caso se llaman *"cookies* de sesión".

Algunas pueden resultar útiles para ofrecer un determinado servicio en Internet o para simplificar la navegación.

Por ejemplo, algunos sitios web utilizan *cookies* para identificar a sus usuarios cada vez que éstos los vuelven a visitar, de modo que no es necesario que se registren cada vez que quieren consultar las novedades.

Sin embargo, no se deben subestimar las consecuencias del uso de *cookies* en la privacidad. Esta cuestión se abor - dará en el apartado de este capítulo dedicado al análisis jurídico.

* *Portales*

Debido a la complejidad creciente de Internet, sus usuarios se conectan a menudo a un sitio web a través de los llamados *portale*s, que ofrecen una presentación ordenada de vínculos web.

Los *portales* suelen contener vínculos con sitios comerciales y podrían compararse con un centro comercial electrónico que aloje gran cantidad de tiendas. Recopilan información de la misma forma que cualquier sitio web, pero también pueden almacenar información sobre las visitas a todos los sitios existentes "tras" el *porta*l.

Los *portales* siempre están alojados por un *proveedor de servicios de Interne*t, que en ocasiones puede incluso ser su propietario. En estos casos, el *proveedor de servicios de Internet* tiene la posibilidad de recabar datos sobre las visitas de un usuario a los sitios que se encuentran "tras" su *portal* y puede, por tanto, elaborar un perfil completo del usuario.

En un informe 79 sobre Internet y la privacidad basado en investigaciones realizadas sobre 60 *proveedores de servi - cios de Internet* de los Países Bajos, la autoridad holandesa en materia de protección de datos (*Registratiekame*r) llegó a la conclusión de que el proveedor de contenidos (en este caso, el *proveedor de servicios de Internet* propietario del *porta*l) puede llegar a saber cuántos anuncios se han colocado, con qué frecuencia ha visitado el usuario una tienda electrónica, qué productos ha comprado y cuánto ha pagado por ellos.

* *Proveedores de servicios adicionales*

En ocasiones, los datos recabados por los sitios web se transmiten (automáticamente) a un tercero que no forma parte de la comunicación original (por ejemplo, empresas especializadas en el análisis estadístico de la Web, como Nedstat). La finalidad de esta práctica puede ser almacenar datos estadísticos sobre las visitas al sitio web para venderlos posteriormente a los propietarios de dichos sitios. A menudo, las *pancartas* publicitarias recopilan mediante *cookies* información sobre los sitios web que una persona ha visitado. Algunos proveedores de servicios, como DoubleClick o Globaltrash, almacenan la información relativa a las visitas a los sitios web en los que han colocado anuncios. Con estos datos se puede elaborar un perfil de las preferencias de los usuarios de Internet que se utilizará posteriormente para personalizar páginas web.

La navegación desde el punto de vista del usuario de Internet

En muchos casos, un ordenador personal en el que se haya instalado un programa de navegación cargará automáticamente, una vez encendido, una página de inicio seleccionada en la Web. Esta página puede contener *hipervínculos* que pueden activarse para visitar otros sitios web o motores de búsqueda. Mientras navega, el programa de navegación del usuario de Internet envía una petición a un servidor situado en cualquier parte del mundo para que transmita una página web específica, identificada con su URL, alojada en dicho servidor web. Al hacer clic en un *hipervínculo*, en realidad el usuario de Internet está descargando en su ordenador la página web solicitada.

Tras conectarse a su *proveedor de servicios de Internet*, el usuario de Internet escoge uno de los siguientes métodos de navegación:

* Desplazarse directamente al sitio web solicitado introduciendo su URL; por ejemplo, www.amazon.com. El URL también contiene el *protocolo*.

* Llegar al sitio web mediante un sitio remitente *(portal)* que contiene *hipervínculos* a otros sitios. Estos *portales* están adquiriendo mayor popularidad a medida que aumenta el número de páginas web existentes y los usuarios de Internet necesitan orientación para encontrar la información que les interesa.

* Encontrar sitios interesantes introduciendo primero consultas en motores de búsqueda, que recurren a la indización por medio de palabras clave. El usuario introduce una o varias palabras clave e inicia la búsqueda.

El motor de búsqueda comienza entonces a buscar los títulos de los sitios correspondientes y sus direcciones URL en su base de datos de índices. Puede reunir perfiles personales a medida que acumula los términos de búsqueda introducidos por un usuario de Internet y los sitios web visitados posteriormente. La personalización se realiza a menudo por medio de *cookies*. Algunos motores de búsqueda ofrecen también servicios más personalizados para los cuales se pide al usuario de Internet que proporcione información sobre sus preferencias personales con el fin de obtener, por ejemplo, actualizaciones periódicas de sitios web sobre un tema determinado 80 .

III. Riesgos para la privacidad

Millones de usuarios de Internet de todo el mundo navegan con frecuencia por la World Wide Web o buscan información en Internet. Sin embargo, estas actividades no están exentas de riesgos desde el punto de vista de la privacidad.

En Internet se obtienen y tratan grandes cantidades de información de un modo que resulta invisible para el titular de los datos. En ocasiones, el usuario de Internet no es consciente de que sus datos personales se han recogido y procesado y se pueden utilizar con fines que ignora. El titular de los datos no está enterado del tratamiento y, por lo tanto, no es libre para decidir al respecto 81 .

Además, cuando los datos recopilados durante la navegación por Internet pueden relacionarse con otras informaciones sobre el usuario, surgen otros riesgos. El temor a tal cruce de datos personales sobre usuarios de Internet ha estado muy presente en el debate sobre la fusión entre la empresa publicitaria de Internet DoubleClick y la empresa de estudios de mercado Abacus Direct.

Se temía que, de producirse esta fusión, la base de datos de DoubleClick con información sobre los hábitos de uso de Internet pudiera cotejarse con la base de datos de Abacus Direct, que contenía nombres y direcciones reales, así como con información detallada sobre los hábitos de compra de los clientes 82 .

La fusión se produjo en noviembre de 1999. De acuerdo con la información ofrecida en el sitio web de Doubleclick 83 , los nombres y direcciones comunicados de forma voluntaria por un usuario en un sitio web perteneciente a Abacus Alliance serían cotejados por Abacus utilizando un código de correlación y la *cookie* de DoubleClick, con otras informaciones sobre el interesado.

La información contenida en la base de datos Abacus Online sobre cada usuario incluye: nombre, dirección, catálogo, historial de compras en línea y datos demográficos. Esta base de datos recoge igualmente información que no permite identificar a un usuario y que ha sido recabada por sitios web u otras empresas con las que DoubleClick mantiene relaciones comerciales.

Según DoubleClick, hasta la fecha no se ha establecido ninguna relación entre las bases de datos de DoubleClick y de Abacus.

Nuevo software de control

Los *proveedores de servicios de Internet* disponen actualmente de nuevas tecnologías de control que generarán una cantidad de información sobre modelos de tráfico y preferencias de contenido muy superior a la que ha existido en la red telefónica pública conmutada (PSTN). Estas tecnologías prometen ofrecer el equivalente en Internet de los registros de llamadas de la red telefónica pública conmutada, e incluso más.

El software de este tipo se conoce popularmente como aplicaciones E.T. *"porque, una vez que se han instalado en el ordenador del usuario y han aprendido lo que querían saber, hacen lo mismo que el extraterrestre de Steven Spielberg: llamar a casa"84* .

A título de ejemplo, Narus, una empresa privada de software de Palo Alto, California (EE.UU.), ofrece a los *proveedores de servicios de Internet* software que "controla el flujo de datos y analiza cada paquete con objeto de extraer de él la cabecera e información útil"85 . Narus afirma que trabaja en estrecha colaboración con socios clave, tales como Bull, Cisco y Sun Microsystems. Estos programas pueden utilizarse para identificar y medir la telefonía Internet y otras aplicaciones (como la Web, el correo electrónico o los faxes IP), pero también pueden controlar el contenido del tráfico IP que se puede facturar (por ejemplo, información protegida por derechos de autor que requiere el pago de un canon, el uso a medida de una aplicación o audioclips). Los programas de Narus informan en tiempo real al *proveedor de servicios de Internet* sobre los sitios web más visitados, así como sobre los contenidos visualizados y descargados 86 .

Alexa 87 es una herramienta que puede añadirse a un navegador para acompañar al usuario durante la navegación y ofrecerle información adicional sobre el sitio visitado (titular registrado, valoraciones y análisis del sitio), así como hacerle sugerencias sobre sitios relacionados. A cambio de ofrecer este servicio a los usuarios, Alexa ha recabado una de las mayores bases de datos sobre hábitos de utilización de la Web. Amazon pagó 250 millones de dólares en acciones por Alexa a principios de los noventa. En su política de privacidad, Alexa afirma que la información recogida sobre la utilización de la Web a través de sus ficheros de uso de la misma y de *cookies* permanece anónima.

Otro de los productos fabricados por Alexa es el programa zBubbles, una herramienta de compra en línea que recoge datos de navegación sobre el usuario con objeto de ofrecerle recomendaciones sobre determinados productos, asesoramiento comparativo para sus adquisiciones, etc. De acuerdo con la información publicada en la revista Time 88 zBubbles también envía información a Alexa cuando los usuarios no compran. Este producto se ha diseñado para que aparezca en pantalla durante toda la sesión de navegación, aunque la mayoría de los usuarios no están comprando continuamente.

Otro ejemplo interesante de software de control es Radiate, antes conocido como Aureate. Radiate es una empresa publicitaria que trabaja con fabricantes de *software compartid*o. Parece ser 89 que los anuncios de Radiate contenían software E.T. que se instaló en los ordenadores de 18 millones de personas, y utilizaron su conexión a Internet para obtener información sobre el tipo de anuncios que los usuarios visitaban en la Red.

La versión original de los programas de Radiate, que aún reside en numerosos ordenadores, se desarrolló para seguir llamando a casa incluso después de que se borrase el programa de *software compartido* que la instaló en ellos. Los usuarios necesitaban una herramienta especial para eliminar el fichero que más adelante la empresa proporcionó desde su sitio web.

En la actualidad existen cientos de aplicaciones E.T. Se cree que más de 22 millones de personas las han descargado 90 . El software de control E.T. constituye de nuevo un ejemplo de tecnología de tratamiento de los datos personales de los usuarios sin que éstos se enteren (tratamiento invisible): la mayoría de los usuarios ni siquiera se imagina que estos programas están instalados en su ordenador.

A menudo, los fabricantes de estas aplicaciones E.T. declaran que aunque tienen capacidad para recoger datos relativos a los usuarios de los ordenadores no establecen conexiones con individuos. Sin embargo, esto no es una garantía suficiente para el usuario, pues, dado el valor comercial de los datos individualizados, las empresas que los recaban podrían modificar sus políticas en cualquier momento. El riesgo potencial de abuso de los datos sigue existiendo 91 .

IV. Análisis jurídico

El punto de partida en el análisis jurídico de los fenómenos de navegación y búsqueda en Internet es que las dos Directivas sobre protección de datos (Directiva 95/46/CE y Directiva 97/66/CE) son, en principio, aplicables a Internet 92 .

Principales preceptos de la Directiva general 95/46/CE: principio de finalidad,

tratamiento leal e información al interesado

Tres de las cuestiones abordadas en la Directiva general merecen una atención especial en este capítulo: el principio de finalidad, el principio de tratamiento leal y la información al interesado.

Información al titular de los datos

En Internet los datos fluyen con gran rapidez y a menudo no se observan las normativas tradicionales referentes a la información que se proporciona al interesado sobre el tratamiento de sus datos y los fines del mismo. En algunos casos, los usuarios de Internet no tienen pleno conocimiento de la existencia ni de las capacidades del software o el hardware a través de los que se realiza el tratamiento, como las *cookies* o las aplicaciones informáticas E.T.

El Grupo de Trabajo trató estos casos en su Recomendación 1/99 93 , en la que destacó que el requisito de informar al titular a fin de que tenga conocimiento del tratamiento de sus datos constituye una condición para la legitimidad de éste.

Los productos de hardware y software de Internet deberían proporcionar a los usuarios información sobre los datos que pretenden recabar, almacenar o transmitir, así como sobre el fin con que se han pedido.

Los productos de hardware y software de Internet también deberían permitir al interesado acceder fácilmente a los datos recabados sobre él con posterioridad.

El incumplimiento de las obligaciones impuestas por la Directiva general no se puede imputar a la velocidad de los flujos de datos en Internet. De hecho, Internet es un medio que permite ofrecer información rápida y sencilla al titular de los datos. Siempre que se recopilen datos de carácter personal, se debería proporcionar al interesado información básica 94 de un modo que garantice la recogida leal de sus datos, que podría ser, dependiendo de la situación, directamente en la pantalla o en el formulario en el que se obtienen los datos o a través de una casilla de aviso en la pantalla (por ejemplo, cuando se envían *cookie*s). El interesado debería disponer de la posibilidad de oponerse al tratamiento u obtener más información haciendo clic en algún lugar.

Algunos sitios web siguen una política de privacidad que incluye la información sobre los datos que tratan, los fines de dicho tratamiento y la forma en que el interesado puede ejercer sus derechos. Sin embargo, ésta no es la regla general, y ni siquiera cuando existe tal política se ofrece toda la información necesaria.

Pese a estar a favor de las políticas de privacidad completas y precisas, el Grupo de Trabajo es claramente partidario de que se informe al interesado directamente en la pantalla o a través de la utilización de casillas de aviso en el momento en que se recopilan sus datos, sin que él tenga que realizar ninguna acción para acceder a la información, pues los usuarios de Internet no siempre leen las medidas de protección de la privacidad de todos los sitios web que visitan mientras navegan.

Para desempeñar un papel informativo serio, sería aconsejable que las descripciones de las medidas de protección de la privacidad no fuesen demasiado extensas, que presentasen una estructura clara y que ofreciesen información precisa sobre la política de protección de datos del sitio de forma sencilla y comprensible.

El trabajo de la OCDE en este campo (generador de políticas de protección de la privacidad o asistente en materia de privacidad), podría ayudar a alcanzar estos objetivos, aunque el uso de un generador no constituye por sí mismo una garantía de cumplimiento de las Directivas comunitarias.

En la práctica es improbable que las medidas de protección de la privacidad basten por sí mismas, pues no contienen información suficiente desde el punto de vista de la protección de datos. Un estudio reciente realizado por el EPIC 95 en Estados Unidos sobre las medidas de protección de la privacidad de los 100 sitios de comercio electrónico más visitados mostró que pocos de los sitios con tráfico intenso ofrecían una protección adecuada. De hecho, ninguno de ellos respetaba elementos importantes de las prácticas leales de información investigadas en el estudio 96 .

Principio de finalidad

La información que se ha de proporcionar al titular de los datos debería ser, en todos los casos, suficiente y sencilla en lo que respecta a los fines del tratamiento. El artículo 6 de la Directiva general prohíbe que los datos sean tratados posteriormente de manera incompatible con dichos fines.

Este principio resulta especialmente relevante para los sitios web que recaban información sobre el comportamiento de navegación de los usuarios de Internet, para los programas a los que el usuario ha autorizado a controlar su comportamiento en Internet con un fin específico pero no con otros fines (desconocidos) y para los *proveedores de*

Servicios de Internet.

En principio, sólo los *proveedores de servicios de Internet* deberían recopilar datos de navegación relativos a los usuarios de Internet, y en la medida en que los necesiten para prestar un servicio al abonado, en este caso la visita a los sitios web que éste desee. En ocasiones, los *proveedores de servicios de Internet* mencionan la necesidad de conservar estos datos con el fin de poder supervisar el funcionamiento de sus sistemas. Sin embargo, ello no requiere el almacenamiento de datos que permitan la identificación del usuario, pues se puede medir y controlar el funcionamiento de un sistema basándose en datos agregados.

Un informe reciente de la Registratiekamer 97 concluyó que cuando los *proveedores de servicios de Internet* conservan datos individuales sobre tráfico de los usuarios no lo hacen en calidad de proveedores de acceso. Esta información resulta especialmente interesante para sus actividades como proveedores de contenido.

Sin embargo, debería señalarse que éste es un fin completamente diferente. Resultaría útil que el principio de limita-

ción de los fines pudiera integrarse en medios técnicos. Esto podría considerarse también una forma de tecnología en favor de la protección de la privacidad 98 .

Tratamiento leal de datos

El artículo 6 de la Directiva general contiene varios principios destinados a garantizar el tratamiento leal de los datos de carácter personal. Uno de ellos es el principio de limitación de los fines mencionado en los párrafos anteriores.

Dicho artículo especifica igualmente que los datos de carácter personal deberían conservarse en una forma que permita la identificación de los interesados durante un período no superior al necesario a los fines para los que se han recogido. Esto significa que, una vez que los datos son anónimos para impedir que se puedan relacionar con el titular de los datos, pueden utilizarse con otros fines, como evaluar los resultados del servicio ofrecido por un *proveedor de servicios de Internet* o elaborar un estudio sobre el número de visitantes de un sitio web.

Los motores de búsqueda más utilizados mantienen registros de consultas en los que se recogen tanto las consultas como otros tipos de información, incluidos los términos utilizados 99 . Estos términos son interesantes para empresas que pretenden seleccionar *metaetiquetas* de páginas web y estimar la demanda en línea de contenidos relacionados con determinadas marcas, empresas o productos. Si no existe una relación entre el registro de la consulta y la identidad del usuario de Internet que introdujo la palabra clave, no existen obstáculos jurídicos que puedan impedir el mantenimiento de estos datos agregados.

Si los datos de navegación y búsqueda en Internet no se hacen anónimos, no deberían conservarse una vez finalizada la sesión de Internet. Esta cuestión se explicará con mayor detalle cuando se aborde la Directiva específica relativa a la intimidad y las telecomunicaciones en los datos sobre tráfico.

Al considerar la lealtad del fin del tratamiento de datos, también debería tenerse en cuenta el artículo 7 de la Directiva, que establece varias condiciones para que el tratamiento sea leal, incluidos el consentimiento del interesado y el equilibrio entre el interés legítimo del responsable de los datos y los derechos fundamentales del titular de los mismos. El responsable del tratamiento debería tener siempre en cuenta este equilibrio de intereses cuando recaba información personal de un usuario de Internet.

Principales preceptos de la Directiva específica sobre intimidad y telecomunicaciones

Como se puede observar en la tabla que aparece en el capítulo 3, algunas disposiciones de la Directiva de telecomunicaciones resultan especialmente pertinentes para la navegación y la búsqueda en Internet.

Aunque el título de la Directiva 97/66/CE se refiera al sector de las telecomunicaciones en general, es evidente que la terminología empleada en el texto se basa en la tecnología RDSI. La mayoría de los preceptos de esta Directiva utilizan términos como "llamadas", que aluden a la telefonía tradicional y RDSI y dificultan la aplicación a los servicios de Internet. No obstante, normalmente éstos se pueden incluir en el ámbito de aplicación de la Directiva, aunque, como se puede ver en los párrafos siguientes, se han de afrontar ciertas dificultades.

Sin embargo, muchos de estos problemas terminológicos quedan resueltos en el texto de la propuesta de revisión de la Directiva de 12 de julio de 2000 100 , en el que se han actualizado algunas de las definiciones para garantizar la cobertura de todos los tipos diferentes de servicios de transmisión para las comunicaciones electrónicas, independientemente de la tecnología empleada.

Las referencias al término "llamadas" se limitan actualmente a los casos en que el legislador se refiere específicamente a llamadas telefónicas, tal como se especifica con la inclusión de una definición de esta palabra en la letra e) del artículo 2 101 . En cualquier otro caso, el nuevo texto utiliza "comunicaciones" o "servicios de comunicaciones".

En los siguientes párrafos se comentarán las normas más pertinentes de la Directiva 97/66/CE. Siempre que resulte adecuado, este documento se referirá a los cambios introducidos por la nueva propuesta de revisión de la Directiva.

Artículo 4: Seguridad

Los proveedores de servicios de telecomunicación deberían ofrecer medidas adecuadas de seguridad que tomen en consideración las técnicas más avanzadas. Estas medidas deberían ser proporcionales a los riesgos de cada situación específica.

Este precepto resulta especialmente pertinente para los proveedores de *encaminadores* y líneas de conexión, ya que estos sistemas transportan grandes cantidades de información.

Este artículo no se ha modificado en la nueva propuesta, excepto en lo que respecta a la sustitución del término "servicios de telecomunicaciones" por "servicios de comunicaciones electrónicas".

Artículo 5: Confidencialidad

Las normas nacionales garantizarán la confidencialidad de las comunicaciones. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados 102 .

Son varios los agentes participantes en las actividades de búsqueda y navegación en Internet a los que afecta este artículo: proveedores de *encaminadores* y líneas de conexión, *proveedores de servicios de Internet* y proveedores de telecomunicaciones en general.

En principio, este artículo se refiere al contenido de la comunicación. Sin embargo, la distinción entre datos sobre tráfico y contenido no resulta fácil de aplicar en el contexto de Internet, sobre todo cuando se hace referencia a la navegación.

En un primer momento, los datos relativos a ésta podrían considerarse datos sobre tráfico. No obstante, el Grupo de Trabajo opina que navegar por distintos sitios podría considerarse una forma de comunicación y, como tal, debería quedar cubierta por el ámbito de aplicación del artículo 5.

Por sí mismo, el comportamiento de navegación de un usuario de Internet (datos de navegación) que visite distintos sitios web puede revelar mucho sobre la comunicación que está teniendo lugar. En la mayoría de los casos, conociendo los nombres de los sitios web visitados se puede obtener una idea bastante precisa de la comunicación que se ha producido. Además, a quien posea los datos sobre tráfico le resulta sencillo visitar el sitio y ver exactamente los contenidos a los que se accedió.

Así pues, el Grupo de Trabajo considera que los datos de navegación de un usuario de Internet deberían recibir la misma protección que los contenidos. Por consiguiente, esta forma de comunicación debería ser confidencial.

En este sentido, se puede considerar que las *series de clics* quedan dentro del ámbito de aplicación de este artículo.

En la letra c) del apartado 1 de su artículo 2, la nueva propuesta de revisión de la Directiva recoge la definición de "datos sobre tráfico": *(se entenderá por) "datos sobre tráfico", cualquier dato tratado en el curso de o a efectos de la transmisión de una comunicación a través de una red de comunicaciones electrónica*s. Por lo tanto, los datos de navegación quedarían incluidos en esta definición y se considerarían datos sobre tráfico.

La revisión de esta Directiva ha entrañado otras mejoras gracias a la ampliación del ámbito de aplicación del artículo 5 para abarcar no sólo el contenido de la comunicación, sino también los datos sobre tráfico correspondientes.

Al ofrecer la misma protección al contenido que a los datos sobre tráfico relacionados con él se resta importancia a la distinción, no siempre evidente, entre estos conceptos.

El Grupo de Trabajo acoge favorablemente esta mejora.

Artículo 6: Tráfico y facturación

Los datos sobre tráfico deberán destruirse o hacerse anónimos en cuanto *termine la comunicació*n. Con objeto de interpretar este artículo en el contexto de Internet es necesario definir lo que puede considerarse datos sobre tráfico y lo que puede entenderse por contenido de la comunicación.

Este artículo parece guardar una estrecha relación con las telecomunicaciones por conmutación de circuitos que conectan a dos o más partes de la comunicación. Los datos sobre tráfico se crean en el proceso de establecimiento y mantenimiento de esta conexión, lo que dificulta especialmente la aplicación de este artículo en el contexto de Internet.

En el tráfico de Internet, los paquetes que se transmiten están "envueltos" en varias cabeceras de *protocolo*s, tales como la cabecera TCP, la cabecera IP y la cabecera Ethernet. Estas cabeceras de *protocolos* se leen en cada uno de los nudos *(encaminadore*s) que atraviesa un paquete para decidir a dónde se dirigirá el siguiente envío de dicho paquete. Sin embargo, no parece necesario que cada nudo intermedio almacene datos de las cabeceras una vez que ha transmitido el paquete.

La información contenida en las cabeceras, que puede incluir datos sobre el contenido de los paquetes, se debería considerar datos sobre tráfico en el sentido del artículo 6 de la Directiva 97/66/CE y, por tanto, se debería tratar de forma anónima o borrarse una vez que estos datos ya no sean necesarios para el mantenimiento de la comunicación, es decir, tan pronto como el usuario de Internet acceda al sitio web.

No cabe duda de que algunos datos como los referentes a la conexión de la sesión (hora de conexión y desconexión, cantidad de datos transferidos, hora de inicio y fin de la sesión, etc.) deberían incluirse en el ámbito de aplicación del artículo 6.

La lista de sitios web visitados por un usuario de Internet (comportamiento de navegación) debe considerarse en cualquier caso datos sobre tráfico (y puede ser objeto de la misma protección que el contenido). Sobre todo, esta lista debería destruirse en principio *en cuanto termine la sesión de Interne* t.

Resulta interesante señalar que el ordenador personal conserva siempre un registro de las actividades de navegación del usuario de Internet. Esto puede ser un problema cuando varios usuarios comparten un ordenador.

En el pasado, el Grupo de Trabajo emitió dictámenes sobre la cuestión de los *proveedores de servicios de Internet* que almacenan datos sobre tráfico con fines de cumplimiento de la ley 103 . Esta Recomendación establece que, en princi-

pio, los datos sobre tráfico que no sean necesarios para la facturación no deberían conservarse. En el caso de *proveedores de servicios de Internet* gratuitos no sería necesario guardar datos sobre tráfico, ya que, al no requerirlos para la facturación, no habría necesidad de ellos una vez concluidas las operaciones normales.

La Directiva revisada sustituye la expresión "en cuanto termine la comunicación" por "en cuanto concluya la transmisión", que resulta más clara. Por lo tanto, los datos sobre comportamiento de navegación deberían eliminarse una vez finalizada la conexión a Internet.

El nuevo texto introduce la posibilidad de un tratamiento posterior para prestar servicios de valor añadido o para comercializar servicios propios de comunicación electrónica si el abonado ha dado su consentimiento. Sin embargo, el término "servicio de valor añadido" no se define en la propuesta. El Grupo de Trabajo considera necesario aclarar qué debería incluir esta definición para garantizar la limitación de los fines y reducir los nuevos riesgos para la privacidad. Del mismo modo, el Grupo de Trabajo recomienda que se incluya una "prueba de necesidad" relativa a la posibilidad de tratar datos sobre tráfico para las actividades comerciales propias del proveedor 104 .

Artículo 8: Identificación de la línea llamante y la línea conectada

En Internet no hay líneas llamantes que identificar. No hay un canal de encaminamiento separado que permita establecer la identidad de quien realiza la llamada antes de que se establezca la conexión.

En Internet, la dirección IP no se puede separar de la comunicación (los paquetes), por lo que el concepto de *identificación de la línea de llamada* no se puede aplicar directamente.

Técnicamente hablando, no es posible ofrecer servicios de telecomunicación relacionados con Internet sin transmitir y utilizar la dirección IP que el usuario ha empleado durante una sesión.

Por tanto, se puede concluir que el artículo 8 de la Directiva de telecomunicaciones no puede aplicarse a las direcciones IP del mismo modo que se aplica a los números de teléfono.

La propuesta de revisión de la Directiva de 12 de julio de 2000 sigue esta línea de pensamiento. La redacción de este artículo se mantiene prácticamente inalterada y sigue utilizando el término "llamada", un concepto que en el nuevo texto se reserva a los servicios de telefonía.

V. Medidas en favor de la privacidad

La protección real de la privacidad mientras se navega por Internet se puede garantizar de diversas formas. Presentamos aquí algunas opciones para aumentar el grado de protección de la privacidad del usuario 105 .

En primer lugar, muchos métodos de recopilación de datos personales se basan en el uso de *cookie*s. Los programas de navegación que emplea el usuario de Internet permiten impedir la instalación de éstas en su disco duro, ya sea de forma individual o de modo sistemático. Sin embargo, cabe señalar cada vez son más numerosos los sitios web que sólo ofrecen un servicio completo si se autorizan las funciones de la *cooki*e.

El 20 de julio de 2000 Microsoft anunció que la próxima versión de Internet Explorer incluiría la versión beta de un sistema de seguridad que permitiría una mejor gestión de las *cookies* de web 106 . La versión de prueba debería estar a disposición del público a finales de agosto.

De acuerdo con la información previa, dicho sistema presentará varias características que permitirán a los usuarios controlar las *cookies* de forma más eficaz. El navegador podrá diferenciar entre las *cookies* procedentes del interlocutor de la comunicación y las procedentes de terceros, y la instalación por defecto avisará al usuario cuando se esté instalando una *cookie* duradera procedente de éstos.

Las empresas publicitarias de Internet, como DoubleClick o Engage, recurren con mucha frecuencia a estas *cookies* procedentes de terceros para seguir la pista de las actividades de los usuarios. Además, la nueva función permitirá al usuario eliminar todas las *cookies* con un simple clic y facilitará el acceso a información sobre seguridad y privacidad. Sin embargo, este sistema de seguridad no aumentará el control del consumidor sobre el uso de *cookies* procedentes del interlocutor principal, muy habituales en sitios web comerciales.

El diseño de las características de gestión de las *cookies* va pisando los talones al de otros sistemas de seguridad creados recientemente por Microsoft para solucionar problemas de fuga de datos. En mayo de 2000, la empresa presentó una extensión del popular programa Outlook capaz de suprimir las *cookies* de los mensajes de correo electrónico.

Sin embargo, resulta lamentable que esta tecnología no permita todavía al sitio que origina la *cookie* indicar inmediatamente el fin con que ésta se utilizará.

En segundo lugar, el *proveedor de servicios de Internet* puede contribuir a la protección de la privacidad del usuario de Internet limitando los datos personales almacenados al mínimo necesario para el establecimiento de la conexión y el mantenimiento del funcionamiento técnico. En particular, en muchos casos el *proveedor de servicios de Internet* puede ocultar a un sitio web el número IP de un usuario de Internet mediante una conexión con dicho sitio desde un *servidor*

proxy especial.

En ese caso, sólo se transmite el número IP asignado por el *servidor proxy*, mientras que el *proveedor de servicios de Internet* conserva la dirección del usuario de Internet. Sin embargo, éstos servicios no se suelen ofrecer de modo estándar.

En tercer lugar, algunos *portales* pueden actuar como *organismos de confianza* que custodian los datos personales del usuario. Estos "informediarios" pueden actuar como vigilantes que sólo suministran datos de carácter personal a sitios web que respetan la privacidad del usuario de Internet, o pueden "negociar" con la información personal de que disponen para conseguir determinados beneficios, siempre que el titular esté al corriente de ello y haya dado su consentimiento 107 . Sin embargo, esta última opción debería considerarse con precaución.

El método que garantiza mayor rigor al usuario de Internet es la elección de servicios que ocultan de forma intencionada su dirección IP a los sitios web que visita. Determinados programas y sitios web permiten mantener en el anonimato las direcciones IP de los usuarios redireccionando la comunicación a través de servidores dedicados que sustituyen la dirección IP por otra.

La existencia de nuevos programas que controlan el software E.T. hace que se vuelvan a plantear cuestiones sobre las posibles medidas de protección.

Un método de protección posible 108 , aunque difícil de llevar a la práctica, consistiría en la segmentación física de los discos duros de los ordenadores en una parte pública y otra privada, de forma que los datos descargados no pudieran acceder a la información que se desee mantener confidencial. En cualquier caso, se recomienda ser extremadamente prudente al descargar aplicaciones procedentes de Internet o del correo electrónico.

VI. Conclusiones

* Es necesario ofrecer acceso anónimo a Internet a los usuarios que navegan o realizan búsquedas en la Red, por lo que se recomienda vivamente el uso de *servidores prox*y.

* El uso cada vez mayor de software de control es una tendencia que debería tomarse en consideración y recibir la atención debida, pues puede tener graves consecuencias en la privacidad de los usuarios de Internet.

* Ciertas definiciones y algunos conceptos utilizados en la redacción actual de la Directiva de telecomunicaciones no resultan fáciles de aplicar a los servicios relacionados con Internet.

- La diferenciación tradicional entre contenido y datos sobre tráfico no puede aplicarse fácilmente a las actividades de Internet, sobre todo en lo que respecta a la navegación: por una parte, el concepto de datos sobre tráfico debería interpretarse de forma amplia para incluir los datos contenidos en cabeceras y todos los datos de conexión; por otra, debería ofrecerse a los datos sobre comportamiento de navegación el mismo grado de protección que a los referentes al contenido.

- Las normas relativas a la *identificación de la línea llamante* deberían revisarse en el contexto de Internet.

* La revisión de esta Directiva ha provocado un gran avance en el primero de estos puntos gracias a la ampliación del ámbito de aplicación del artículo 5 con objeto de cubrir no sólo el contenido de la comunicación, sino también los datos sobre tráfico con él relacionados, y ofrecer así la misma protección a ambos. El Grupo de Trabajo acoge favorablemente esta mejora. El segundo problema también ha quedado resuelto tras aclarar que este precepto sólo se aplica a las llamadas telefónicas y no a Internet.

Con la revisión, la terminología se ha adaptado al nuevo contexto ampliado, lo que ha aclarado enormemente la Directiva y ha facilitado la interpretación de las disposiciones vigentes. No obstante, el Grupo de Trabajo desearía señalar que el concepto de "servicios de valor añadido" precisa una mayor especificación con objeto de evitar una interpretación demasiado amplia.

CAPÍTULO 6: PUBLICACIONES Y FOROS

I. Introducción

Las publicaciones y los foros disponibles en Internet tienen en común que en ellos se hacen públicos datos de carácter personal, ya sea con la participación del interesado, como sucede en los foros de debate públicos, ya sin ella, como en las guías. Los motivos por los que se publican estos datos personales son muy diversos.

El usuario de Internet puede comunicar cierta información porque así se le ha solicitado, por ejemplo, para poder entrar en una sala de charla, o puede suceder que sea un tercero quien publique los datos, como en el caso de un organismo público, con fines administrativos.

La cuestión principal que plantea esta difusión de información es la aplicación de los principios de privacidad a los

datos públicamente disponibles en la Web. En contra de lo que se piensa generalmente, la protección que ofrece la legislación sobre protección de datos se sigue aplicando a los datos publicados. En este capítulo se prestará especial atención a los motivos y las necesidades que llevan a la publicación de datos personales, al fin con que ésta se realiza y a los riesgos de abuso de los datos.

II. Descripción técnica

Foros públicos de debate Los aspectos técnicos del tratamiento de datos en foros públicos de debate varían según la naturaleza de éstos. Se pueden distinguir dos tipos principales de foros: los de debate y la charla electrónica.

Foros de debate

Los grupos de discusión son foros clasificados por tema sobre el que los usuarios pueden presentar sus aportaciones y respuestas, para lo cual todos los datos enviados por los usuarios se almacenan durante un determinado período de tiempo.

Toda cuestión o artículo consta de un "título" y de un "cuerpo". El enlace entre un artículo y la respuesta al mismo es un "hilo".

En la transmisión de los mensajes a los servidores de foros de debate se utilizan *protocolos* específicos. El *protocolo* habitual de tratamiento de noticias es el NNTP *(protocolo* de transferencia de noticias a través de la red), aunque algunos foros utilizan también el *protocolo* HTTP. El NNTP procesa conexiones permanentes entre servidores de foros de debate y actualiza automáticamente los mensajes.

El servidor del foro de debate almacena estos mensajes en un disco duro que cualquier persona conectada puede consultar. Las noticias se presentan en formato HTML.

Cada servidor compara con los demás su lista de artículos en cada foro de debate e intercambia con ellos nuevos artículos. Este proceso produce millones de intercambios de datos en Internet.

Dado el gran número de foros existentes, los usuarios sólo almacenan una lista reducida de ellos, debido a su gran número, y los programas de consulta sólo presentan los títulos de los artículos nuevos y dejan a iniciativa del interesado la descarga del texto del documento.

Charla electrónica

Existen tres tipos principales de charla en Internet: la charla interactiva Internet (IRC),la charla de página web *(Java*) y la charla ICQ ("I seek you" - te busco).

1. La charla interactiva Internet (IRC) es el modo original de charla electrónica. Utiliza un *protocolo* que permite a los usuarios comunicarse en tiempo real, ya sea públicamente, en un foro con un número indeterminado de personas, o en privado, con un único interlocutor. Al igual que los foros de debate, las salas de charla varían según los temas, pero se diferencian de éstos en que los canales se cancelan una vez concluido el debate.

Los retrasos en la transmisión de información en las principales charlas interactivas Internet han llevado a la creación de redes independientes, entre las que destacan EfNet, UnderNet y DalNet.

2. La charla de página web permite comunicarse sin necesidad de un programa separado: la única herramienta que se necesita es un navegador de Internet moderno. Existen dos tipos de charla de página web: la dedicada, disponible en la mayoría de los sitios de búsqueda de los *portales* de la Web, y la que el usuario instala en su propia página de inicio. Aunque la charla de página web resulta muy sencilla de utilizar, sus capacidades son limitadas: a diferencia de lo que sucede en la charla interactiva Internet (IRC), sólo permite intercambiar texto, y no modificar colores, enviar sonidos, mandar ni recibir ficheros, ejecutar scripts ni personalizar los elementos de la interfaz de charla.

3. La charla ICQ es una herramienta que informa al usuario que está continuamente en línea y le avisa cuando se conectan personas predefinidas (incluidas en una lista de contactos personales) y le permite contactar y charlar con ellas y enviarles mensajes mientras sigue navegando por la Red, siempre que todos los participantes estén utilizando ICQ. Se pueden dar instrucciones al programa para que señale al usuario como invisible, ausente o no disponible.

Publicaciones y guías

Normalmente, las publicaciones y las guías se publican en Internet en forma de bases de datos que ofrecen criterios de búsqueda para obtener información sobre una o varias personas.

Tradicionalmente, la fuente de información de las guías telefónicas es la guía oficial nacional que edita, según el país, el operador principal de telecomunicaciones o una empresa responsable de recabar los datos basándose en la lista de abonados.

Existen distintos medios de recopilación de listas de correo electrónico, desde la inscripción voluntaria de los usuarios de Internet en una lista que presenta un *proveedor de servicios de Internet*, a la recogida incontrolada de direcciones de

correo electrónico en sitios web, tales como los foros de debate.

Existen otras publicaciones sobre diversos temas, como las listas editadas por organismos públicos, que pueden incluir, por ejemplo, la jurisdicción de un país con los datos de las sentencias, los tribunales, la situación e incluso los nombres de las partes y del juez, así como un resumen del caso.

La mayoría de las bases de datos existentes en Internet ofrecen varios criterios de búsqueda que permiten acceder a la información de forma personalizada y organizan los resultados de distintas formas. En una guía telefónica se podría iniciar una búsqueda a partir de un nombre o un número de teléfono, mientras que en una base de datos de jurisprudencia el criterio podría ser la fecha de una sentencia, el nombre de una de las partes, etc.

III. Riesgos para la privacidad

Foros públicos de debate

La accesibilidad a los datos de carácter personal comunicados por el usuario de Internet constituye el principal riesgo para la privacidad 109 . La posibilidad de acceder a estos datos puede dar lugar a su recogida y posterior utilización con fines que el participante en los foros públicos no siempre es capaz de prever con claridad.

Por otra parte, el titular de los datos no siempre tiene conocimiento de los detalles que se publican habitualmente junto con el contenido de su aportación al foro.

En el caso de los foros de debate, por ejemplo, la dirección de correo electrónico del participante suele publicarse junto con su nombre o seudónimo 110 . Determinadas charlas electrónicas muestran, además del seudónimo del usuario que accede a ellas, la dirección IP de su ordenador. Algunos *proveedores de servicios de Internet* ofrecen la posibilidad de intervenir en un foro sin ser identificado por los demás participantes, pero también, por otro lado, la de acceder a la charla y que otros participantes lean un perfil específico del interesado.

La información de carácter personal disponible en línea varía según el foro. Como norma general, para dar acceso a un usuario a una sala de charla el *proveedor de servicios de*

Internet le pide que cumplimente un cuestionario de identificación detallado que normalmente incluye la dirección de correo electrónico, la fecha de nacimiento, el país, el sexo y, en ocasiones, ciertas preferencias del usuario.

Sin embargo, desde el punto de vista técnico la comunicación de esta información detallada no es necesaria para el buen funcionamiento del foro de debate o de la charla, en el sentido del artículo 6 de la Directiva 95/46/CE.

Además, posteriormente esta información registrada podría ser utilizada por el *proveedor de servicios de Internet* y se podría combinar con detalles adicionales sobre el interesado recabados en línea en salas de charla.

Dos de los motivos principales para utilizar los datos recopilados o publicados son:

1. Controlar la naturaleza del contenido difundido. El objetivo de esta medida es garantizar que no se publiquen contenidos inadecuados y establecer la responsabilidad en caso de que se publiquen contenidos ilegales 111 . Con este fin, y para que el contenido siga siendo identificable, se suele guardar el rastro de los datos sin realizar una selección previa, independientemente del tipo de información aportada, aunque quizá fuese suficiente la dirección de correo electrónico y, tal vez, el nombre del participante.

2. Confeccionar listas de datos personales. Los datos personales se pueden recopilar en la Web con software capaz de buscar en la red y reunir todos los datos disponibles sobre una persona determinada. El Grupo de Trabajo incluyó en su Recomendación 3/97 112 una cita de un artículo periodístico que explicaba *cómo se podría elaborar una biografía detallada de una persona seleccionada al azar utilizando estos programas y extraer información de todos los foros de debate en los que hubiera participad*o, incluyendo datos como su dirección, su número de teléfono, su lugar de nacimiento, su lugar de trabajo, su destino favorito para las vacaciones y otros intereses personales. Estos datos podrían recopilarse y tratarse después con fines diversos, como la venta directa, pero también con objeto de conocer su solvencia crediticia o para venderlos a compañías de seguros o a empresarios. Algunos sitios web ya ofrecen herramientas de acceso público que permiten obtener todas las aportaciones que una persona ha realizado en foros de debate a partir de su nombre o su dirección de correo electrónico 113 .

Publicaciones y guías La disponibilidad en línea de información de carácter personal extraída de registros públicos o de otras fuentes de acceso público, tales como guías, plantea cuestiones similares a las mencionadas que están relacionadas con la posible utilización posterior de datos personales a escala mundial con un fin distinto de aquél para el que se publicaron originalmente 114 .

Como ya se ha señalado, la informatización de los datos y la posibilidad de realizar búsquedas en textos completos ofrecen un número ilimitado de maneras de solicitar y clasificar información, y la extensión de Internet aumenta el riesgo de recopilación con fines inadecuados. Además, la informatización ha facilitado enormemente la combinación de datos de acceso público procedentes de distintas fuentes, lo que permite elaborar un perfil de la situación o el comportamiento de los usuarios. Por otra parte, se debería prestar especial atención a la utilidad de la publicación de datos de carácter personal como un modo de fomentar nuevas técnicas de *almacenamiento y minería de*

datos 115 . Estas técnicas permiten recabar datos sin especificar previamente el fin y no definirlo hasta el momento en que se utilice efectivamente la información 116 .

Se pueden mencionar varios casos concretos para ilustrar esta preocupación: - Aunque las bases de datos de la jurisprudencia son instrumentos públicos de documentación jurídica, su publicación en formato electrónico en Internet, con criterios amplios de búsqueda de juicios, podría dar lugar a la creación de ficheros con información sobre individuos. Esto es lo que sucedería si se consultase una base de datos con el fin de obtener una lista de sentencias judiciales sobre una persona en vez de localizar sólo un caso jurídico.

- También se puede obtener información concreta sobre una persona combinando los datos existentes en bases de datos electrónicas separadas.

Por ejemplo, los nombres de las personas sin derecho a voto podrían recabarse cotejando los registros de población con los censos electorales.

- Generalmente, las guías de direcciones en Internet permiten buscar personas no sólo por su nombre, sino también por su dirección y su número de teléfono. Los interesados no prevén estas búsquedas inversas cuando dan su consentimiento para la publicación de su dirección en la guía telefónica en papel.

La disponibilidad de los datos en formato electrónico significa que éstos podrían utilizarse con fines diversos, como la venta directa, seleccionando categorías de personas que viven en la misma zona (tal vez para vender sistemas de alarma en zonas residenciales), o la identificación y el registro de una persona que realiza una llamada a una empresa para lo que considera una sencilla solicitud anónima de información.

Las publicaciones en Internet pueden dar lugar a otras formas de recogida de información personal que se centrarían no sólo en los datos de carácter personal de una charla, un registro público o un directorio, sino también en información directa ofrecida en una página web personal. La indización automática de estas páginas realizada con robots de búsqueda puede hacer posible que se elaboren ficheros con información personal extraída de esas páginas, lo que a su vez posibilitaría la comercialización o el envío de *buzonfia* ("spam") dirigida al autor de dichas páginas o a las personas que hayan participado en ellas.

IV. Análisis jurídico

Foros públicos

Se ha previsto imponer obligaciones a los *proveedores de servicios de Internet* con el fin de limitar los riesgos de recogida ilícita de datos personales publicados en salas de charla o foros de debate.

La Recomendación n§ R (99) 5 del Consejo de Europa relativa a la protección de la privacidad en Internet 117 establece para los *proveedores de servicios de Internet* la directriz de que informen a los usuarios, antes de que se abonen o empiecen a utilizar sus servicios, de los riesgos que el uso de Internet presenta para su privacidad. La información debe cubrir la *integridad de los datos*, la confidencialidad, la seguridad de la red y otros riesgos para la privacidad, como la recogida o la grabación invisible de datos.

El formulario de inscripción que los usuarios han de completar para solicitar acceso a un foro público debe respetar lo dispuesto en el artículo 6 de la Directiva 95/46/CE sobre el tratamiento leal de datos personales, que estipula que éstos deben recogerse con fines legítimos e impone la prohibición de recabar datos que no resulten necesarios ni pertinentes para dicho fin.

La legitimidad del fin puede determinarse sobre la base del artículo 7 de la Directiva 95/46/CE, que exige en particular el consentimiento explícito del titular para el tratamiento de sus datos personales, así como el equilibrio entre el interés legítimo del responsable del tratamiento y los derechos fundamentales del interesado (letras a y f del artículo 7).

Se deberá informar a los usuarios de una forma clara y visible sobre el fin del tratamiento, la calidad de los datos recabados y el posible período de almacenamiento. Si esta obligación no se respeta, la falta de respuesta del usuario no se podrá considerar un consentimiento tácito para que el responsable de los datos realice un tratamiento posterior de éstos (por ejemplo, con fines comerciales).

Cabe destacar que los proveedores de servicios no necesitan conocer en todo momento la identidad del usuario. Antes de aceptar las suscripciones y de conectar a los interesados a Internet deberían informarles sobre la posibilidad de acceso anónimo o con un seudónimo y de utilización anónima de sus servicios 118 .

El Grupo de Trabajo ha reconocido este principio en su Recomendación 3/97 sobre anonimato en Internet 119 . Aunque no cabe ninguna duda sobre la legitimidad del anonimato en situaciones como el intercambio de experiencias personales (alcohólicos o víctimas de abusos sexuales) o de opiniones políticas, el Grupo de Trabajo ha insistido en que la necesidad de anonimato en Internet va mucho más allá de estos casos concretos, *los datos transaccionales identificables crearán un medio a través del cual podrá*

*observarse y controlarse la actuación de las personas en una medida que hasta ahora no había sido posibl*e. El control

de los foros de debate y las charlas electrónicas con objeto de prohibir contenidos inapropiados debería ejercerse de conformidad con el principio de proporcionalidad establecido en el artículo 6 de la Directiva 95/46/CE. En este sentido, la identificación y recopilación de los datos personales aportados en un foro público se considera desproporcionada en relación con otros medios de control existentes. Se han propuesto otras posibilidades, como soluciones contractuales que ofrecen "calidad de contenido" o la participación de un moderador encargado de supervisar las aportaciones para detectar contenidos dañinos o ilegales.

Junto con estos principios fundamentales, cabría añadir que la conservación de datos sobre tráfico por parte de los *proveedores de servicios de Internet* se ha regulado de forma muy estricta, al igual que en el caso de los operadores de telecomunicaciones.

Como norma general, los datos sobre tráfico deben destruirse o hacerse anónimos en cuanto termine la comunicación (apartado 1 del artículo 6 de la Directiva 97/66/CE). Los operadores de telecomunicaciones y los *proveedores de servicios de Internet* no pueden recabar ni almacenar información sólo con fines de cumplimiento de la legislación, a menos que así se lo exija la ley por motivos concretos y en condiciones específicas 120 .

Publicaciones y guías

El Grupo de Trabajo ha reiterado 121 que la legislación europea sobre protección de datos se aplica a los datos personales de acceso público y que la protección de esos datos sigue siendo necesaria.

El principio fundamental aplicable a los datos públicos de carácter personal es el de finalidad o limitación de los fines, en virtud del cual los datos personales sólo se pueden recabar con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines (letra b) del apartado 1 del artículo 6 de la Directiva 95/46/CE).

El Grupo de Trabajo ha subrayado igualmente que los datos personales puestos a disposición del público no constituyen una categoría homogénea que pueda tratarse de manera uniforme desde el punto de vista de la protección de datos: el acceso público a los datos puede existir pero estar sujeto a ciertas condiciones, tales como la prueba del interés legítimo, y a restricciones de su uso posterior, como el uso con fines comerciales.

La publicación de datos personales en Internet podría dar lugar a un tratamiento posterior de los datos no previsto por el interesado. Los artículos 10, 11 y 14 de la Directiva 95/46/CE establecen a este respecto que el titular tiene derecho a recibir información sobre la utilización de sus datos personales. Además, ha de ser informado sobre su derecho a oponerse al tratamiento de datos personales con fines comerciales por medios sencillos y eficaces.

La idea de una "ventanilla única" para oponerse al tratamiento de datos personales por medio de una lista única puede constituir una solución interesante para las dificultades que los usuarios encuentran a la hora de evitar una operación de tratamiento de datos, dado el gran número de ellas que existen tanto a escala nacional como en el ámbito internacional 122 .

Si el fin previsto para el tratamiento resulta incompatible con el propósito original, el equilibrio entre el derecho a la intimidad y los intereses del responsable de los datos se logrará con la imposición de condiciones más estrictas a éste, que deberá solicitar el consentimiento del titular de los datos o demostrar que existe un fundamento jurídico o reglamentario para el tratamiento.

Sin embargo, no siempre queda claro si el responsable está obligado a respetar el derecho de oposición del titular o a solicitar su consentimiento a la hora de tratar sus datos.

La reglamentación de las guías de Internet en los distintos países es un ejemplo de la diversidad de enfoques. La cuestión radica en si es necesario el consentimiento previo cuando la publicación en formato electrónico de un directorio presenta criterios de búsqueda diferentes de los previstos originalmente en el directorio en papel.

Algunos países, como España y Bélgica, consideran que la ampliación de los criterios de búsqueda ofrece la posibilidad de tratar datos personales con fines incompatibles con el propósito original y que este tratamiento no debería autorizarse sin informar previamente al interesado y solicitar su consentimiento. En otros países, como el Reino Unido, en principio el cumplimiento del derecho a oponerse previsto en la Directiva parece considerarse suficiente, aunque dependerá de si existe o no obligación jurídica de publicar la información en la guía.

Estas interpretaciones de los textos jurídicos provocan diferencias en el grado de protección existente en los distintos países de la UE y conflictos prácticos cuando, por ejemplo, se publica en Internet una guía con datos personales de ciudadanos de un país en el que existe un grado elevado de protección desde otro en el que la política de protección es más permisiva.

Estos conflictos se han debatido a escala europea y la interpretación común que el Grupo de Trabajo ha hecho de los textos ha dado lugar a una posición oficial que recomienda la aplicación armonizada del principio en todos los Estados miembros de la UE 123 .

El artículo 12 de la propuesta de revisión de la Directiva 97/66/CE 124 establece el derecho de los abonados a determinar sin coste alguno si aprueban la incorporación de sus datos y cuáles de ellos podrán aparecer en guías públicas, con qué fin concreto y en qué medida. Esto constituye un avance en la dirección correcta y ha recibido el apoyo abso-

luto del Grupo de Trabajo.

V. Medidas en favor de la privacidad

Además de las disposiciones jurídicas mencionadas, existen soluciones técnicas que pueden aumentar la protección de los datos personales a distintas escalas.

Como principio general, el Grupo de Trabajo señala que los programas de navegación deberían configurarse por defecto de manera que sólo se trate la cantidad mínima de información necesaria para establecer la conexión a Internet 125 .

Anonimato en foros públicos

Con relación al anonimato en Internet, y en particular en los foros públicos, la idea de la "seudoidentidad" podría ofrecer una solución alternativa a la cuestión del equilibrio entre el control legítimo de los abusos y la protección de los datos personales. Este tipo de identidad se asignaría a una persona a través de un proveedor de servicios especializado.

De este modo se respetaría en principio el anonimato, pero el proveedor de servicios especializado podría reconstruir un enlace con la verdadera identidad del titular en determinados casos, tales como la sospecha de que existan actividades delictivas.

Respecto al correo electrónico, los reexpedidores anónimos asignan al usuario una dirección anónima a la que otras personas pueden enviar sus mensajes y desde la que

éstos se reenviarán a la verdadera dirección del usuario (lo que a veces se denomina servidor seudónimo), o bien envían el mensaje del emisor sin mencionar su nombre ni su dirección 126 .

Indización sistemática de los datos

También existen herramientas para garantizar que los autores de páginas personales no estén sujetos a la indización sistemática de sus páginas y a la recopilación de sus datos personales sin tener conocimiento de ello. El objetivo del *protocolo* de exclusión de robots es impedir que un motor de búsqueda pueda indizar automáticamente todas o parte de las páginas de un sitio web 127 .

La mayoría de los motores de búsqueda existentes en la Web pueden identificar este *protocol*o. El fichero "robots.txt", incluido en la dirección de Internet, contiene instrucciones para los robots de búsqueda en las que se establece que algunos de ellos no son bienvenidos o que sólo pueden leerse o indizarse algunas páginas identificadas en el sitio.

Dado que sólo un proveedor de servicios puede insertar un *protocolo* de exclusión de robots en la dirección del sitio, los autores de páginas web cuyo proveedor de servicios no acepte incorporar dicho *protocolo* pueden incluir una *metaetiqueta* de robots en cada una de las páginas que no quieran que se indice. La desventaja de estas *metaetiquetas* es que no todos los motores de búsqueda existentes en Internet las reconocen.

Acceso en línea a información pública

El último tema tratado en este capítulo se refiere al acceso en línea a información pública, que, no obstante, sigue estando sujeta a las normas de protección de la privacidad.

Las soluciones técnicas aplicadas a estas bases de datos pueden ayudar a limitar el uso ilegal de la información que contienen: - Los criterios de búsqueda deben definirse de modo que los datos sólo puedan utilizarse de acuerdo con el propósito original. El Grupo de Trabajo insistió en su Recomendación de 13 de julio de 2000 sobre guías inversas en que "el responsable del tratamiento (...) tiene la obligación de aplicar las medidas técnicas y de organización que resulten adecuadas en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse (véase el artículo 17 de la Directiva 95/46/CE). Esto significa, por ejemplo, que la base de datos debería diseñarse de forma que permita impedir posibles usos fraudulentos, tales como la modificación ilícita de los criterios de búsqueda o la posibilidad de copiar toda la base de datos o de acceder a ella con objeto de realizar un tratamiento posterior. Por ejemplo, los criterios de búsqueda deben ser suficientemente precisos para permitir la presentación exclusiva de un número limitado de resultados por página. El resultado debería ser que el fin para el que el abonado ha dado su consentimiento quede también garantizado con medios técnicos"128 .

- La consulta en línea de bases de datos se puede restringir, por ejemplo, limitando el campo o los criterios de consulta. No se debería permitir la recopilación de grandes cantidades de datos mediante una consulta amplia, como las primeras letras de un nombre. Del mismo modo, debería resultar técnicamente imposible solicitar sentencias judiciales basándose, por ejemplo, en el nombre de una persona, o solicitar el nombre de alguien a partir de su número de teléfono.

Con este fin, deberían configurarse y utilizarse herramientas técnicas coherentes con los principios jurídicos descritos en este capítulo.

VI. Conclusiones

En teoría, los regímenes jurídicos y los medios técnicos disponibles ofrecen una valiosa protección al titular de los datos en lo que respecta a la disponibilidad pública de algunos de sus datos personales en Internet. "El principio de finalidad, en virtud del cual los datos personales no pueden tratarse con fines incompatibles con los especificados en un principio, tiene una importancia fundamental en cuanto a los datos publicados en determinadas circunstancias".

También deberá prestarse especial atención al principio de limitación del período de almacenamiento de datos personales. Estos datos deberían destruirse al cabo de un tiempo razonable, a fin de impedir la elaboración de perfiles que reúnan, por ejemplo, los mensajes enviados por una persona a un foro de debate a lo largo de varios años.

Esas personas deberían conocer el período previsto de almacenamiento y disponibilidad en línea de dichos datos públicos.

En la actualidad, los problemas residen principalmente en la escasez de información de que disponen tanto los titula - res como los responsables del tratamiento de los datos sobre las disposiciones jurídicas que han de observar.

Para mejorar la situación, el objetivo principal consiste en incrementar los esfuerzos por conseguir mayor transparencia en Internet y por armonizar la interpretación de los principios fundamentales relativos al control que el titular de los datos puede tener sobre éstos.

La Directiva 97/66/CE, en su versión revisada de 12 de julio de 2000, ofrece una buena oportunidad para armonizar estas cuestiones.

CAPÍTULO 7: TRANSACCIONES ELECTRÓNICAS EN INTERNET

I. Introducción

El comercio electrónico se puede definir como "cualquier forma de transacción en la que la interacción entre los agen - tes es electrónica en lugar de basarse en intercambios físicos o en un contacto físico directo"129 .

Esta definición abarca las transacciones relacionadas con la compra de bienes o servicios, así como las utilizadas para mejorar la calidad de los servicios o la prestación de nuevos servicios por parte de entidades privadas y públicas.

Teniendo en cuenta la definición anterior, este capítulo, cuyo principal objetivo es estudiar cuestiones relacionadas con Internet, se centrará en las transacciones que tienen lugar a través de la Red y dejará al margen cualquier otra forma de interacción realizada por redes públicas o privadas.

Se prevé que las transacciones electrónicas tengan una repercusión mundial, ya que el comercio electrónico es global por definición y permite a cualquier empresa (independientemente de su tamaño o su volumen de negocios) ofrecer y vender sus productos en todo el mundo.

Las transacciones electrónicas permiten a las organizaciones ser más eficaces y flexibles, trabajar más estrechamente con sus proveedores y cubrir las necesidades y expectativas de sus clientes de una forma nueva con la que antes ni siquiera soñaban.

Sin embargo, para conseguir estos objetivos se necesita una cantidad enorme de información, lo que podría conducir a la invasión de áreas importantes de la privacidad individual.

II. Agentes

Los principales agentes que participan en las transacciones electrónicas son: - El usuario, en el contexto de la Directiva 95/46/CE, que es la persona física que quiere comprar un producto o solicita un servicio 130 .

- El operador de telecomunicaciones, que no participa especialmente en las transacciones comerciales electrónicas pero desempeña una función esencial en el envío de señales que hacen posible toda forma de transmisión electrónica de datos. La directivas prevén para este agente obligaciones específicas relativas a la seguridad.

- El *proveedor de servicios de Internet* que da acceso a Internet.

- El comerciante electrónico, que es la entidad que ofrece productos o servicios a través de la red.

- La plataforma financiera necesaria en la mayoría de los casos y en la que participan tanto el banco del comerciante como el del consumidor, y una pasarela de pagos que se encarga de los aspectos técnicos necesarios para autorizar la operación financiera y el pago. Esta pasarela de pagos se encarga de todas las conexiones entre instituciones financieras que posibilitan el intercambio de dinero digital asegurando que todos los agentes cumplen los requisitos necesarios para realizar la transacción.

- *Terceros de confianz*a, que son necesarios, en los casos más complejos y en que la seguridad es primordial, para autentificar las partes y proporcionar una *encriptación* suficientemente fuerte, con el fin de garantizar la confidencialidad de la transacción.

Existen tres modelos diferentes de transacción electrónica, dependiendo de las formas de comercio y de los agentes u operadores que participen en él 131 .

1) Suministro en línea de bienes y productos inmateriales.

Utilizado principalmente por casas de desarrollo de software y empresas de comunicaciones en las que la infraestructura de Internet resulta ideal para la venta y distribución remota en tiempo real.

Abarcan software, películas de vídeo, juegos y música en línea, así como suscripciones en línea a publicaciones, revistas o programas de apoyo técnico.

En este caso, aparte del ahorro obvio derivado del acceso directo a los consumidores, lo que evita la dependencia de intermediarios, las empresas que utilizan este tipo de comercio tienen una gran ventaja: pueden obtener información precisa y exacta del consumidor final, sus aficiones, intereses y hábitos de compra.

Esta categoría también abarca a la mayoría de los servicios que ofrecen las organizaciones del sector público, como la autoliquidación o devolución tributaria en línea, los formularios electrónicos o las peticiones de pagos por prestaciones sociales y las acciones de seguimiento.

2) Solicitud electrónica de bienes materiales.

Esta categoría abarca muchos tipos diferentes de empresas, entre las que se incluyen, en primer lugar, las grandes empresas que utilizan Internet para tener acceso directo al consumidor.

Los fabricantes de hardware de tecnología de la información y los minoristas han sido los primeros en usar este canal comercial, lo que es fácilmente comprensible dada la naturaleza del usuario de Internet. En la actualidad, cada vez son más numerosas las empresas que venden ropa, perfumes, libros, CD, billetes de avión, etc.

Internet brinda a las pequeñas y medianas empresas la oportunidad de desarrollar nuevas actividades comerciales a una escala que sería inalcanzable con sus recursos tradicionales. De hecho, y como han advertido algunos observadores, hay una gran diferencia entre la inversión inicial necesaria para ofrecer cien mil CD musicales en una tienda electrónica de Internet y tratar de hacerlo abriendo una tienda en el centro de una ciudad.

Además, todos los sitios de comercio electrónico que suministran bienes materiales dependen en última instancia de una organización logística para entregar los artículos al consumidor final en su dirección personal. Hoy en día, tales organizaciones logísticas están invirtiendo en tecnología de Internet de apoyo a los pedidos electrónicos y la trazabilidad de los envíos entre empresas socias y entre la empresa logística y el consumidor final, de tal forma que todos los participantes pueden averiguar en tiempo real la ubicación de los bienes solicitados y cuándo se espera que se entreguen. En este contexto es bastante posible que determinados distribuidores y expertos en logística decidan fusionarse en un futuro próximo para poder utilizar la información clave que poseen las empresas logísticas acerca del proceso de distribución (principalmente, direcciones de recogida y suministro).

3) Redes y centros comerciales.

El comercio en línea no excluye a los distribuidores tradicionales que no tienen un conocimiento particular de las nuevas tecnologías. Éstos tienen la posibilidad de integrarse en una estructura denominada "centros comerciales virtuales", que les brinda la oportunidad de combinar sus mercancías en los escaparates de un centro comercial virtual. En estos centros, las tiendas están clasificadas por categorías y los visitantes utilizan un sistema interno de búsqueda para encontrar una lista de sitios que ofrecen el producto solicitado. Se pueden colocar *pancartas* publicitarias basándose en las palabras clave mecanografiadas o en las tiendas visitadas, y el centro comercial virtual ofrece a sus miembros una infraestructura de pago segura.

Dependiendo de su función, es frecuente que los centros comerciales virtuales recojan información muy detallada y exacta sobre sus visitantes y compradores (tiendas visitadas, intereses, hábitos de compra, direcciones, detalles personales e información sobre el pago) que puede resultar de gran interés para establecer perfiles de consumidores a la hora de desarrollar estrategias publicitarias o comerciales 132 .

El papel de estos centros comerciales puede cambiar en el futuro si se integran en sitios más amplios, los denominados *portales,* "supersitios" web que proporcionan una gama de servicios entre los que se incluyen la búsqueda en la Web, noticias, guías de páginas blancas y amarillas, mensajería electrónica gratuita, grupos de debate, compras en línea y vínculos con otros sitios.

Estos *portales* modernos ofrecen oportunidades cada vez mayores de realizar compras en todo el mundo, tanto mediante anuncios clasificados como a través de motores de búsqueda. Además, nada impide que en un futuro próximo ofrezcan sus propias plataformas seguras de pago y agentes usuarios inteligentes que puedan buscar en la Web, negociar precios (incluso los términos de privacidad de un contrato comercial)133 y celebrar acuerdos en nombre

del consumidor.

III. Seguridad en los pagos

La creciente importancia del comercio electrónico lleva consigo una necesidad de sistemas de pago adecuados para la venta de bienes y servicios.

Dos de los factores que limitan la expansión del comercio electrónico son las preocupaciones acerca de los riesgos que implica el envío por Internet de detalles sobre la tarjeta de crédito y la posibilidad de que se revele información personal confidencial a terceros no autorizados.

Se han desarrollado y se siguen desarrollando diversos métodos para abordar estas preocupaciones. Hoy en día, el más común de ellos es la capa de conexiones seguras 134 , que se implementa en los navegadores más utilizados y establece un canal seguro entre los ordenadores del consumidor y del comerciante a través de *encriptación* y *certificados electrónico* s.

El sistema de capa de conexiones seguras funciona, básicamente, como sigue. Antes de que el ordenador del comerciante (servidor) pueda iniciar una conexión segura con el ordenador del consumidor (cliente), el cliente ha de asegurarse de estar conectado a un servidor seguro. Para comprobar la identidad del servidor se utiliza su *certificado electrónic*o. Una vez que se ha autentificado el servidor, el cliente y éste pueden encriptar los datos que se envían y garantizar su *integrida*d, incluido el número de tarjeta de crédito que se use en la transacción y cualquier otro detalle personal.

Conviene tener en cuenta que el sistema de capa de conexiones seguras no permite al consumidor controlar el uso o tratamiento que el comerciante haga posteriormente de sus datos personales, y que la *autentificación* del cliente no es obligatoria, con lo que el uso indebido de la identidad de otra persona constituye una posibilidad de fraude.

Para tratar estas dificultades y proporcionar un marco totalmente fiable en las transacciones comerciales electrónicas, algunas empresas de tarjetas de crédito han desarrollado conjuntamente un nuevo *protocolo* con el apoyo de los principales desarrolladores de software. Este *protocol*o, denominado SET ("*secure electronic transaction*s" o transacciones electrónicas seguras), proporciona transmisiones confidenciales (utilizando la *encriptació*n), *autentificación* de las partes (titular de la tarjeta, emisor, vendedor, comprador y pasarela de pagos a través de certificados electrónicos), e *integridad* e irrevocabilidad de los pagos de bienes y servicios (mediante *firmas electrónica* s)135 .

Dado que el sistema mencionado no es muy adecuado si se necesita realizar un número elevado de transacciones de pequeño valor, se está desarrollando un método alternativo denominado dinero digital o *"e-cas*h". El principio general consiste en descargar el dinero en el disco duro de un ordenador (o, en un futuro próximo, en el chip de una tarjeta inteligente). Cada vez que se efectúe un pago en línea, el usuario transferirá unidades de dinero (fichas) desde su ordenador o tarjeta inteligente a la cuenta del vendedor o del proveedor de servicios. En esta área hay varias tecnologías en competición. Las más interesantes desde el punto de vista de la protección de la información personal son los sistemas de pago completamente anónimo basados en un mecanismo de firma ciega 136 . Estos mecanismos podrían impedir la trazabilidad de las transacciones, pues el banco que "firma" el *e-cash* no vincula al consumidor con una transacción concreta.

IV. Riesgos para la privacidad

Independientemente del tipo de transacción realizada o del sistema de pago utilizado, la diferencia esencial entre el mundo físico y el electrónico es que muchas actividades del primero pueden quedar en el anonimato (mirar escaparates, pasear por diversas tiendas, examinar productos y, si se paga en efectivo, comprar bienes), mientras que en el segundo puede grabarse todo, añadirse a información previa o nueva y tratarse casi sin ningún coste para producir información más amplia sobre cada persona. Y todo ello puede hacerse sin el consentimiento del ciudadano afectado e incluso sin su conocimiento. Además, con las actuales tecnologías de *almacenamiento de información* y *minería de datos* 137 se puede tratar una cantidad enorme de información, no sólo para seleccionar a las personas que cumplen ciertos requisitos o criterios, sino también para descubrir relaciones ocultas entre datos sin una conexión aparente, con lo que se explicitan algunos patrones de conducta que se podrían utilizar para tomar decisiones comerciales o administrativas en relación con determinados ciudadanos.

En la mayoría de los casos, cuando un sujeto registrado realiza una compra o contrata un servicio (como una suscripción), es obligatorio que proporcione detalles personales al vendedor o al proveedor de servicios para que lo autentifique, se garantice el pago y se comunique una dirección física o electrónica para la entrega de los bienes o servicios. De este modo, a menos que se pague utilizando *e-cash* o tecnologías de protección de la privacidad para ocultar la dirección IP y comprar un bien inmaterial, hoy en día es muy raro que el anonimato sea posible en la red.

Este capítulo se centrará en los riesgos asociados al uso secundario no autorizado de datos personales y en los relacionados con el incumplimiento de la confidencialidad o la suplantación de la personalidad.

1. Uno de los usos secundarios de datos personales más frecuentes es la publicidad. Una vez identificado el comprador, bien porque sea él mismo quien proporcione información al conectarse al servidor, bien a través de otros dispositivos tecnológicos como las *cookie*s, se utiliza información previa sobre él para hacer publicidad personalizada según

sus hábitos, intereses, *series de clics* o hábitos de compra. Y no se trata sólo de anuncios relacionados con los servicios y las ofertas del propietario del sitio web, sino también de los emitidos por terceras partes que tienen acuerdos para apoyar el coste derivado de la gestión del servidor mediante la exposición de sus anuncios publicitarios.

Los paradigmas de la publicidad de Internet son las técnicas utilizadas por agencias publicitarias como DoubleClick, cuyas actividades se basan en proporcionar espacio publicitario en la Red y facilitar a los anunciantes la elección del espacio adecuado para sus actividades de comunicación. El otro elemento vital en el éxito de DoubleClick es la tecnología de la información, que hace posible aislar criterios de identificación y ofrecer a los anunciantes herramientas para dirigir a los usuarios anuncios individualizados. Esta tecnología recurre a una base de datos que contiene información acerca de varios millones de usuarios de Internet, con lo que se garantiza que durante las campañas publicitarias sólo se contactará con la audiencia deseada.

Para lograrlo, DoubleClick recoge y trata datos personales que permiten identificar a los usuarios, describir sus hábitos y determinar en tiempo real los elementos de la población que probablemente satisfarán los criterios de los objetivos de las campañas publicitarias existentes. DoubleClick asigna un número de identificación único a cada usuario que visita uno de los sitios web de su red y coloca una *cookie* que más tarde se utilizará para identificar al usuario cuando se conecte a otro de los sitios de DoubleClick y, de acuerdo con los datos que se tengan de tal usuario, personalizar el anuncio más adecuado. Aunque el visitante no acepte la *cookie* se puede elaborar su perfil, sobre todo si tiene una dirección IP estática.

Los datos personales registrados en la base de datos de DoubleClick son los siguientes: parte permanente de la dirección IP (es decir, la dirección en la Red), dominio, país, Estado (en Estados Unidos), código postal, código SIC (código del Sistema de clasificación industrial normalizada, EE.UU.), tamaño y volumen de negocios de la empresa (optativo), sistema operativo utilizado y número de versión del mismo, proveedor del servicio, número de identificación (asignado por DoubleClick) y referencia de las actividades de navegación (recogida y análisis de sitios visitados por el usuario)138 .

El 23 de noviembre de 1999 DoubleClick se fusionó con Abacus Direct Corporation.

Abacus, que ahora es un departamento de DoubleClick, seguirá explotando Abacus Direct, el elemento de publicidad directa de Abacus Alliance.

Además, se ha anunciado que Abacus ha empezado a crear Abacus Online, el elemento de Internet de Abacus Alliance.

De acuerdo con la información disponible en el sitio web de DoubleClick, la parte de Abacus Online de Abacus Alliance permitirá a los usuarios estadounidenses de Internet recibir mensajes publicitarios personalizados según sus intereses individuales 139 .

Una ciudadana californiana presentó una demanda relativa a dicha fusión ante el Tribunal Supremo del Estado de California tratando de conseguir un requerimiento judicial contra DoubleClick por realizar en Internet prácticas comerciales fraudulentas y engañosas que violan los derechos de privacidad del público en general.

La demanda también afirmaba que DoubleClick engaña y ha engañado al público en general *"(...) dándole una idea falsa de la privacidad y de la seguridad en su uso de Internet, adquiriendo, almacenando y vendiendo, de un modo encubierto, millones de datos privados e íntimos de los usuarios de Internet, y sacando provecho de ello. (...) Cuando un usuario de Internet visita un sitio web participativo, una* cookie *con una identificación única se coloca en su ordenador. A partir de ese momento, cada vez que ese usuario visite un sitio web que contenga información sobre su identidad (...), ésta se vinculará a la* cookie *identificativa.*

Los demandados son capaces de obtener una cantidad potencialmente grande de información personal sobre el usuario utilizando la base de datos Abacus. Por otra parte, los hábitos de compra del usuario de Internet, sus respuestas a la publicidad y los sitios web que visita se rastrean y registran" 140 .

DoubleClick afirma que, dadas las reacciones públicas ante este proyecto de cotejar su base de datos con la de Abacus, hasta ahora no se han dado los pasos efectivos para lanzar tal unión.

Otro ejemplo de cómo tratar los datos personales de una forma que el usuario medio de Internet no puede esperar es el trabajo que realiza SurfAid, una pequeña empresa que forma parte del departamento de servicios globales de IBM situado en Somers (Nueva York)141 . Esta empresa recibe a diario los ficheros históricos de acceso de sus clientes y los pretrata para averiguar la ruta que han seguido los visitantes del sitio web cliente. A continuación se utilizan diversas herramientas de *minería de datos* de gran capacidad para explorar el archivo del cliente, que en algunos casos contiene más de ciento cincuenta millones de peticiones de información, y se produce un informe diario al que pueden acceder los clientes. Posteriormente, el cliente puede utilizar programas de *OLAP* para desglosar y analizar la información.

2. Otro riesgo al que se enfrentan las personas cuando realizan transacciones comerciales es el incumplimiento de la confidencialidad de la información transmitida. Dado que Internet es una red pública abierta con *protocolos* bien conocidos y destinados a compartir información más que a proteger la confidencialidad o seguridad, no resulta muy difícil, para quienes tengan algunos conocimientos técnicos, encontrar numerosas herramientas de programación que permitan interceptar y revelar los datos transmitidos a través de la Red. También es posible hacerse pasar por una

empresa o institución para obtener información que, posteriormente, se podría utilizar para cometer algún fraude o delito.

3. Se está desarrollando una nueva forma de comercio: el comercio electrónico móvil, basado en la tercera generación de teléfonos celulares y otros aparatos portátiles que pueden acceder de forma segura al comercio electrónico y a las páginas web gracias a la utilización de un nuevo *protocolo* 142 . Por consiguiente, la localización y el tráfico de datos, así como los hábitos de viaje, se pueden añadir a los datos sobre transacciones y navegación para elaborar un perfil incluso más detallado del consumidor. Y si se tienen en cuenta las fusiones y las concentraciones entre empresas de telecomunicaciones, proveedores de servicios, *portales* y empresas de contenido, la posibilidad de agregación, integración y tratamiento conjunto aumenta de manera exponencial.

A modo de simple ejemplo de lo que podría ocurrir en un futuro próximo, se puede prever que los anuncios publicitarios perseguirán por todas partes a las personas a través de sus teléfonos móviles o sus asistentes electrónicos personales. "Es un tipo de posicionamiento global de los objetivos, y no está lejos" afirmó un portavoz de DoubleClick 143 .

Otro ejemplo es el proyecto conjunto de Yahoo! y CellPoint Systems AB para comercializar un localizador personal utilizando teléfonos móviles. El sistema "Find-A-Friend" de Yahoo! se puede utilizar para obtener información del tipo: "Juan está cerca de Piccadilly Circus, más o menos a 3,2 km de tí en dirección noroeste", gracias a los recursos de la red GSM de teléfonos móviles. Aunque se exige el consentimiento personal para entrar a formar parte del plan, este ejemplo nos muestra las posibilidades de las nuevas tecnologías de las telecomunicaciones, que pueden localizar al usuario mediante aparatos portátiles 144 .

V. Análisis jurídico

Antes de nada conviene recordar que, como ya se explicó detalladamente en el capítulo 3, las normas sobre protección de datos de las Directivas 95/46/CE y 97/66/CE son aplicables a Internet y a los datos personales tratados en las transacciones electrónicas 145 . Los párrafos que siguen se centrarán en los aspectos de estos textos legales especialmente pertinentes en el ámbito de las transacciones electrónicas.

Legitimidad del tratamiento: principio de finalidad (artículos 5 a 7 de la

Directiva 95/46/CE)

El primer aspecto que cabe considerar es que tanto la recogida de datos como su tratamiento se haga de forma justa y legal, teniendo en cuenta los principios de finalidad y proporcionalidad. En el contexto de las transacciones electrónicas, es importante considerar que la recogida de datos personales puede resultar "invisible" para su titular.

El Grupo de Trabajo ha comunicado con frecuencia su preocupación acerca de todos los tipos de operaciones de tratamiento que en la actualidad se realizan en Internet mediante software y hardware sin el conocimiento del interesado, y que, por lo tanto, resultan "invisibles" para él 146 .

Cuando se recaban datos personales sobre un usuario de Internet, se le debe dar información clara acerca del propósito de su tratamiento y de los destinatarios y categorías de destinatarios de tal información, de manera que el interesado pueda decidir si desea llevar a cabo la transacción en dichas condiciones.

Por otra parte, también se habrían de explicitar los usos secundarios de datos personales, que, en caso de que no se consideren compatibles con el propósito principal, deberían estar sujetos al consentimiento del interesado. Algunos ejemplos de usos secundarios incompatibles son la comunicación de datos sobre transacciones a terceras partes para permitirles establecer perfiles de compradores en sus campañas publicitarias 147 o la utilización de herramientas de *minería de datos* para averiguar los hábitos de comportamiento de una lista de nombres de sitios web visitados por un usuario de Internet.

Conviene destacar que el consentimiento del usuario registrado, necesario para tratar sus datos personales en el marco de una transacción comercial electrónica, no es preciso para recabar los datos que se necesitan para realizar tal transacción.

En sí mismo, esto constituye una base legítima para procesar los datos personales del usuario necesarios en esta tarea, como se afirma en la letra b) del artículo 7 de la Directiva. Cualquier otro dato relacionado, incluidos los datos invisibles que no son necesarios para realizar la transacción, sólo se puede tratar partiendo de otras bases legítimas mencionadas en el artículo 7 de la Directiva, es decir, consentimiento inequívoco, cumplimiento de las obligaciones jurídicas, interés vital del interesado o interés legítimo de los responsables del tratamiento, siempre que no prevalezcan los derechos fundamentales del interesado.

Esto también es aplicable a las transacciones de los organismos oficiales, pues la legitimidad de la recogida de datos y el tratamiento de datos personales por parte de los organismos públicos se basa en reglamentaciones jurídicas 148 .

Un uso secundario que los responsables del tratamiento de los sitios web personales mencionan a menudo es el mantenimiento técnico y el dimensionamiento del equipo de tecnología de la información. No cabe duda de que se trata de una preocupación legítima si se quiere ofrecer un buen servicio a los clientes, pero que se puede satisfacer

plenamente utilizando datos no identificables, pues para dimensionar los ordenadores y las líneas de telecomunicaciones basta con cifras agregadas.

Los responsables de tratamiento sólo pueden conservar datos personales por razones técnicas cuando resulta estrictamente necesario para alcanzar este propósito y es aplicable una de las bases legítimas para el tratamiento de datos.

Información al interesado (artículo 10 de la Directiva 95/46/CE)

Además, el responsable del tratamiento debe proporcionar información precisa al interesado, incluida la identidad del responsable, los fines del tratamiento, los destinatarios de la información, el carácter obligatorio o no de la respuesta y las considerar que la recogida de datos personales puede resultar "invisible" para su titular.

El Grupo de Trabajo ha comunicado con frecuencia su preocupación acerca de todos los tipos de operaciones de tratamiento que en la actualidad se realizan en Internet mediante software y hardware sin el conocimiento del interesado, y que, por lo tanto, resultan "invisibles" para él 146 .

Cuando se recaban datos personales sobre un usuario de Internet, se le debe dar información clara acerca del propósito de su tratamiento y de los destinatarios y categorías de destinatarios de tal información, de manera que el interesado pueda decidir si desea llevar a cabo la transacción en dichas condiciones.

Por otra parte, también se habrían de explicitar los usos secundarios de datos personales, que, en caso de que no se consideren compatibles con el propósito principal, deberían estar sujetos al consentimiento del interesado. Algunos ejemplos de usos secundarios incompatibles son la comunicación de datos sobre transacciones a terceras partes para permitirles establecer perfiles de compradores en sus campañas publicitarias 147 o la utilización de herramientas de *minería de datos* para averiguar los hábitos de comportamiento de una lista de nombres de sitios web visitados por un usuario de Internet.

Conviene destacar que el consentimiento del usuario registrado, necesario para tratar sus datos personales en el marco de una transacción comercial electrónica, no es preciso para recabar los datos que se necesitan para realizar tal transacción.

En sí mismo, esto constituye una base legítima para procesar los datos personales del usuario necesarios en esta tarea, como se afirma en la letra b) del artículo 7 de la Directiva. Cualquier otro dato relacionado, incluidos los datos invisibles que no son necesarios para realizar la transacción, sólo se puede tratar partiendo de otras bases legítimas mencionadas en el artículo 7 de la Directiva, es decir, consentimiento inequívoco, cumplimiento de las obligaciones jurídicas, interés vital del interesado o interés legítimo de los responsables del tratamiento, siempre que no prevalezcan los derechos fundamentales del interesado.

Esto también es aplicable a las transacciones de los organismos oficiales, pues la legitimidad de la recogida de datos y el tratamiento de datos personales por parte de los organismos públicos se basa en reglamentaciones jurídicas 148 .

Un uso secundario que los responsables del tratamiento de los sitios web personales mencionan a menudo es el mantenimiento técnico y el dimensionamiento del equipo de tecnología de la información. No cabe duda de que se trata de una preocupación legítima si se quiere ofrecer un buen servicio a los clientes, pero que se puede satisfacer plenamente utilizando datos no identificables, pues para dimensionar los ordenadores y las líneas de telecomunicaciones basta con cifras agregadas.

Los responsables de tratamiento sólo pueden conservar datos personales por razones técnicas cuando resulta estrictamente necesario para alcanzar este propósito y es aplicable una de las bases legítimas para el tratamiento de datos.

Información al interesado (artículo 10 de la Directiva 95/46/CE)

Además, el responsable del tratamiento debe proporcionar información precisa al interesado, incluida la identidad del responsable, los fines del tratamiento, los destinatarios de la información, el carácter obligatorio o no de la respuesta y las se haya acordado por contrato o así lo autorice una ley, y el derecho a conocer la lógica de cualquier tratamiento automático de datos que afecte al titular.

Derechos de los interesados (artículo 12 de la Directiva 95/46/CE)

También es obligatorio establecer procedimientos claros y eficaces que permitan a los titulares de los datos ejercer sus derechos de acceso, rectificación, supresión o bloqueo.

Cuando los titulares ejercen sus derechos, el responsable del tratamiento debe proporcionarles información transparente sobre si sus archivos contienen (o no) datos personales registrados y, en caso de que así sea, sobre qué datos se están tratando, su origen, los fines del tratamiento, las categorías de datos afectadas y los destinatarios o categorías de destinatarios a los que se prevé que se les comunicarán. Esta información debería estar disponible de forma inteligible. Además, en el contexto de las transacciones electrónicas es recomendable que la información se proporcione mediante la conexión en línea establecida, siempre y cuando el interesado no haya solicitado recibirla de otra forma normalizada.

Una cuestión muy importante relativa al acceso a los datos relacionados con transacciones electrónicas o recabados

mediante ellas es el derecho de su titular a obtener información no sólo sobre la información básica o primaria, sino también sobre la derivada o consolidada. Esto significa que si se ha elaborado algún tipo de perfil personal, se ha realizado alguna clasificación o división en categorías o se han añadido datos procedentes de terceras partes, esta información tratada también debería estar a disposición del interesado, tal y cómo se especifica en la letra a) del artículo 12 de la Directiva.

Obligaciones del responsable del tratamiento: confidencialidad y seguridad

(artículos 16 y 17 de la Directiva 95/46/CE y 4 y 5 de la Directiva 97/66/CE)

Respecto a las cuestiones relacionadas con la confidencialidad y la seguridad, los responsables del tratamiento han de tomar medidas apropiadas para proteger la información que les suministran sus clientes de la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, como ocurre en el caso de las transacciones electrónicas en Internet. Estas medidas han de tener en cuenta los riesgos de seguridad y confidencialidad, la naturaleza de los datos y las tecnologías de vanguardia.

Legislación aplicable (artículo 4 de la Directiva 95/46/CE)

Otra cuestión preocupante en relación con el comercio electrónico en Internet es la legislación aplicable al tratamiento de datos personales recabados de sitios web que están fuera de la UE/EEE. Esto suscita una serie de asuntos problemáticos que deberían analizarse uno a uno. Sin embargo, tal análisis debería tener en cuenta que la Directiva 95/46/CE es claramente aplicable a las operaciones de tratamiento de datos realizadas con equipos localizados, total o parcialmente, en el territorio de la UE, incluso cuando los responsables del tratamiento se encuentran fuera de la Comunidad 153 .

VI. Conclusiones

* Al titular de los datos se le debería proporcionar información clara y comprensible que satisfaga plenamente el principio de información. En particular, durante el proceso de transacción electrónica se debería mostrar obligatoriamente la información sobre protección de datos estrechamente relacionada con la realización de la transacción, con el fin de garantizar que el interesado pueda disponer de ella.

Esto ha de entenderse independientemente de la información destinada a los visitantes de sitios web que no realicen compras. Como medida suplementaria, se deberá poner a disposición del interesado una *firma electrónica* de las condiciones de tratamiento de los datos personales para que posteriormente pueda comprobar que tales condiciones no han sido modificadas.

* Se ha de respetar plenamente el principio de proporcionalidad. Sólo se deberán recabar los datos necesarios para la transacción electrónica.

Por otra parte, el tratamiento de datos (especialmente si se tratan de una forma que resulta invisible para el interesado) se ha de justificar a partir de una de las bases legítimas mencionadas en el artículo 7 de la Directiva.

* Si el interesado decide no proporcionar más detalles personales que los necesarios para que se realice la transacción electrónica, no se deberá ejercer ningún tipo de discriminación contra él en las condiciones ofrecidas para la transacción.

* No se debe efectuar ningún tratamiento secundario sin el conocimiento del titular de los datos, quien, por otra parte, cuando desee acceder a estos procesos deberá recibir información completa sobre la lógica que los rige.

Además, para que el tratamiento se considere legal será necesario un consentimiento sin ambigüedades o alguno de los otros criterios de legitimidad previstos en la Directiva 95/46/CE.

* En la medida de lo posible, se debería utilizar la tecnología de la *encriptació*n, sujeta a las reglamentaciones legales existentes, para proteger la confidencialidad de las transacciones electrónicas y garantizar la *integridad* de los mensajes por medio de una *firma electrónic*a.

* Cuando sea necesario para dar mayor seguridad a las transacciones, sería recomendable utilizar la tecnología de los *certificados electrónico*s. Si es necesaria una mayor seguridad, estos *certificados* se podrían almacenar en tarjetas inteligentes.

* Desde el punto de vista de la protección de los datos personales, la posibilidad de usar métodos de pago seguros y anónimos es un elemento muy importante de la privacidad en Internet.

* La recogida y el tratamiento de datos personales utilizando equipos automatizados u otros situados en el territorio de la UE/EEE están sujetos a las disposiciones legislativas comunitarias de protección de datos.

* Con relación al tráfico de datos, se han de observar las estrictas limitaciones impuestas por el artículo 6 de la Directiva 97/66/CE y se debería tener en cuenta la Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación.

CAPÍTULO 8: CIBERMARKETING

I. Introducción

Internet no es simplemente una plataforma mundial de información, sino también un mercado mundial en el que empresas competidoras tratan de atraer a clientes potenciales.

El éxito depende de llegar a tantos clientes como sea posible, y especialmente a los que de verdad están interesados por el producto o servicio que se les ofrece. Para lograrlo se utilizan perfiles y anuncios publicitarios dirigidos basados en perfiles que se lanzan en *pancartas* colocadas en los sitios web.

Otra forma de conseguir clientes, considerada a veces la más eficaz, es el correo electrónico comercial y el envío de un gran número de mensajes no solicitados a direcciones de personas encontradas en espacios públicos de Internet. Este impopular tipo de correo electrónico se denomina *buzonfia* ("spam")154 .

En ambos casos es necesario poseer datos personales de los clientes, que a menudo se pueden recabar fácilmente en Internet. Muchos usuarios de Internet no son conscientes de que mientras están navegando por la red dejan tras ellos un gran volumen de datos que se pueden utilizar para hacer suposiciones sobre sus intereses, sus preferencias y su comportamiento 155 .

La publicidad dirigida puede ser aceptable hasta cierto punto, cuando va en interés del consumidor; pero si el usuario no sabe qué datos se están recabando, quién los recopila ni con qué fin serán utilizados, pierde el control de sus datos personales. Por lo tanto, no es correcto recabar datos sin el consentimiento y el conocimiento del usuario.

II. Descripción técnica

Publicidad y elaboración del perfil en línea 156

La elaboración del perfil personal en línea se puede realizar de diferentes formas: - Un sitio web crea perfiles mediante la recogida de datos sobre sus clientes que se basan en las interacciones con ellos. Para hacerlo se utilizan *cookies* que rastrean las acciones del usuario en la Web. Dependiendo de cómo esté configurado el navegador del usuario, éste puede no ser consciente de que el sitio web está instalando una *cookie* en su ordenador. Basándose en el perfil del cliente, el sitio web le ofrecerá productos (por ejemplo, libros) o referencias a otros sitios web que le pueden interesar.

- En el ámbito del "cibermarketing de incentivos", los usuarios pueden participar en un juego o un concurso siempre y cuando proporcionen datos personales que servirán para elaborar los perfiles. En este caso, normalmente el titular de los datos está al corriente de que se han recabado, y por lo tanto da su consentimiento 157 .

- Empresas publicitarias de la Red (como DoubleClick o Engage 158) gestionan y proporcionan *pancartas* publicitarias 159 (en lo sucesivo, *pancarta*s) sobre una base contractual en muchos sitios web. Las *pancartas* se colocan en el sitio web solicitado mediante un *hipervínculo* invisible con la empresa de publicidad.

Para hacer llegar al cliente la *pancarta* más adecuada, los anunciantes de la red elaboran perfiles mediante *cookies* colocadas a través del *hipervínculo* invisible.

Dependiendo de la configuración del navegador, el usuario puede ser consciente de que se está colocando una *cookie* y tiene la opción de dar o no dar su consentimiento.

El perfil del cliente está vinculado al número de identificación de la *cookie* de la empresa publicitaria, de modo que se puede ampliar cada vez que el cliente visita un sitio web que ha firmado un contrato con el anunciante.

Tras ser analizados, los datos recabados se pueden completar con información demográfica (edad, género, etc.) y combinarse con otros datos característicos del grupo al que es obvio que pertenece el usuario, determinado por su comportamiento en la red (por ejemplo, por sus intereses). El trabajo de analizar y completar los datos lo pueden realizar programas especiales (especialmente herramientas de *minería de datos*) disponibles en el mercado.

Estos procedimientos dan como resultado perfiles muy detallados que permiten a la empresa o al anunciante de la Red prever los gustos, las necesidades y los hábitos de compra del consumidor y, a partir de estas premisas, hacerle llegar *pancartas* que se adecuen lo más posible a sus intereses.

Cuando los datos recabados, reunidos mediante el número de identificación de la *cookie* del anunciante, no están vinculados a datos identificables 160 de una persona en concreto, se pueden considerar anónimos. Pero en circunstancias frecuentes, por ejemplo cuando el cliente rellena un pedido en el sitio web en que el anunciante ha colocado la *pancart*a, los datos identificables se podrían vincular o unir a datos existentes ya situados en la *cooki*e, lo que permitiría elaborar un perfil identificable de la persona en cuestión 161 .

Correo electrónico comercial

Para realizar una campaña comercial por correo, una empresa tiene que conseguir una lista extensa y apropiada de direcciones de correo electrónico de usuarios potenciales.

Como ya se ha mencionado, a menudo resulta muy fácil utilizar recursos disponibles en Internet.

Existen tres formas diferentes de recabar direcciones de correo electrónico a partir de Internet 162 : recogida directa de clientes o visitantes de sitios web, compra o alquiler de listas a terceros 163 y recogida a partir de espacios públicos 164 tales como guías públicas de correo electrónico o listas de correo electrónico, foros de debate o salas de charla.

Ciertas herramientas disponibles en Internet ayudan a recabar direcciones de correo electrónico. Estos programas buscan sitios web o partes de la Usenet que se han de especificar de antemano mediante una lista de URL o de palabras clave relacionadas con un ámbito de interés predefinido (por ejemplo, deporte, viajes, etc.) y posteriormente proporcionan todas las direcciones de correo electrónico que se han encontrado en los sitios/páginas o en los foros. Existen diversos servicios que funcionan como corredores de listas, recabando direcciones de correo electrónico y vendiéndolas o alquilándolas a precios muy bajos.

Además, hay otras herramientas especializadas en enviar mensajes como "proveedores de servicios de correo electrónico", es decir, sin utilizar un *proveedor de servicios de*

Internet ni ningún otro proveedor que ofrezca un servicio de correo electrónico. Por una parte, estos programas garantizan que se esquivan todos los filtros antibuzonfia instalados por dichos proveedores, y por otra permiten un funcionamiento rápido y automático. Si el emisor lo desea, puede recurrir a un servidor de *buzonfi*a, en el que un tercero se encarga de este tipo de envíos, también a bajo precio.

III. Análisis jurídico

Existen diversas directivas aplicables a la elaboración de perfiles en línea y al correo electrónico comercial.

La Directiva de protección de datos

La Directiva general establece que los datos personales se traten de manera leal, se recojan con fines determinados, explícitos y legítimos y se utilicen de forma leal y legal de acuerdo con los fines establecidos 165 .

El tratamiento debe desarrollarse sobre bases legítimas como el consentimiento, un contrato, la ley o el equilibrio de intereses 166 . Por otra parte, se ha de informar al interesado del tratamiento que se quiera realizar, lo que incluye la comunicación a terceros, antes de que ésta tenga lugar 167 , y el titular tiene derecho a oponerse al tratamiento de sus datos personales con fines comerciales directos 168 . El interesado también tiene derecho a acceder a sus datos, rectificarlos, suprimirlos o bloquearlos 169 .

La Directiva de venta a distancia

La Directiva de venta a distancia 170 establece, como mínimo, el derecho de los consumidores a oponerse a las comunicaciones a distancia realizadas por medio de correo electrónico 171 .

La Directiva específica sobre la intimidad en las telecomunicaciones

La Directiva 97/66/CE da a los legisladores nacionales la posibilidad de aplicar normas que les permiten optar por recibir o no recibir comunicaciones comerciales que no hayan solicitado 172 . Los casos en los que se utilicen aparatos de llamada automática o faxes con fines de venta directa están sujetos al consentimiento previo del consumidor 173 . La definición de aparatos de llamada automática, formulada en términos muy imprecisos, se podría aplicar fácilmente al correo electrónico.

En julio de 2000, la Comisión Europea presentó una propuesta de Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas en sustitución de la Directiva 97/66/CE.

En esta propuesta, el artículo relativo a las comunicaciones comerciales no solicitadas incluye de manera explícita el correo electrónico, que sólo está permitido en caso de que los abonados hayan dado su consentimiento previo.

La Directiva de comercio electrónico

La Directiva de comercio electrónico 174 establece que los mensajes electrónicos comerciales han identificarse como tales 175 y que los registros de no participación, en los que pueden inscribirse las personas que no deseen recibir tales mensajes electrónicos, se deben consultar periódicamente y se han de respetar 176.

Aunque ni la Directiva general ni la de telecomunicaciones se refieren explícitamente al comercio electrónico, se deben aplicar a este ámbito: los considerandos y la letra b) del apartado 5 del artículo 1 de la Directiva sobre comercio electrónico establecen claramente que dicha Directiva no está en modo alguno destinada a modificar los principios y

requisitos legales del marco legislativo existente.

De ello se deduce que la ejecución de la Directiva sobre comercio electrónico ha de estar totalmente de acuerdo con los principios de protección de datos definidos en la legislación correspondiente. Por lo tanto, la legislación nacional sobre protección de datos seguirá siendo aplicable a las empresas responsables del tratamiento de datos personales 177 . Además, los Estados miembros podrían aplicar reglamentos encarnados en la Directiva sobre telecomunicaciones y que amplíen los requisitos de la Directiva sobre comercio electrónico, es decir, las comunicaciones comerciales podrían quedar sujetas al consentimiento previo del destinatario 178 .

IV. Conclusiones

Las normas establecidas en la Directiva general, la Directiva sobre comercio electrónico, la Directiva sobre venta a distancia y la Directiva sobre telecomunicaciones son aplicables al uso de correo electrónico comercial con fines de cibermarketing.

Sólo la Directiva general se aplica a la elaboración del perfil en línea. Aunque forma parte del comercio electrónico, la elaboración del perfil en línea no se trata en la directiva correspondiente. Además, la Directiva revisada sobre telecomunicaciones tampoco abarca la publicidad en Internet, pues los proveedores que prestan este servicio están excluidos explícitamente de su alcance.

Por lo tanto, se pueden extraer las siguientes conclusiones:

Elaboración del perfil en línea y publicidad 179

- Los *proveedores de servicios de Internet* deben informar a los usuarios antes de recoger sus datos sobre el tratamiento que se les quiere aplicar 180 . Esto incluye el tipo, el ámbito y la duración del almacenamiento, así como los fines del tratamiento, es decir, su uso para elaboración de perfiles 181 . Si los datos se comunican a terceros, ello se ha de mencionar de forma explícita.

También se debe informar cuando los datos se recojan utilizando seudónimos o números de identificación no personalizados. En particular, se ha de informar a los usuarios antes de la colocación de una *cookie* para elaborar un perfil personal. Esto debería hacerse mediante un cuadro especial (aviso) que se activase incluso si el navegador no notifica al usuario la colocación de la *cooki*e.

- En todo momento, y como mínimo, se ha de dar a los usuarios el derecho a negarse al tratamiento de sus datos 182 . En ese caso, los datos recabados durante el uso de Internet no se deberán usar para ampliar un fichero existente, lo que también es aplicable cuando el tratamiento esté sujeto al consentimiento previo del usuario.

- La personalización de perfiles ha de estar sujeta a la información y al consentimiento previo de los interesados, que deberán tener derecho a retirar su aprobación en cualquier momento y con efecto futuro.

- Los usuarios han de tener en todo momento la oportunidad de acceder a sus perfiles para inspeccionarlos y han de gozar del derecho de corregir y suprimir los datos almacenados 183 .

Correo electrónico comercial

- La empresa que recoja una dirección de correo electrónico *directamente a partir del*

usuario con vistas a enviar mensajes electrónicos comerciales o a que lo haga un tercero al que comunique la dirección tiene que informar al usuario, utilizando los medios técnicos adecuados, de los objetivos que perseguía cuando recabó la dirección 184 .

- Mientras los Estados miembros puedan elegir entre el consentimiento y la oposición a la recepción de mensajes electrónicos comerciales, las empresas que envíen mensajes electrónicos comerciales deberán asegurarse, utilizando los medios técnicos adecuados, de que el usuario pueda identificar como tales dichos mensajes 185 .

- Mientras los Estados miembros puedan elegir entre el consentimiento y la oposición a la recepción de mensajes electrónicos comerciales, antes de enviar uno de estos mensajes la empresa deberá consultar los registros donde figuren los usuarios que hayan optado por oponerse. Estos registros se han de respetar en todos los casos 186 .

La existencia de registros internacionales de los usuarios que no desean recibir este tipo de mensajes sería muy beneficiosa.

- La recogida de direcciones de correo electrónico *en espacios públicos de Internet* y su utilización para enviar mensajes comerciales va en contra de la legislación comunitaria pertinente, es decir, de la Directiva general 187 . En primer lugar, esta práctica constituye un tratamiento ilegal de datos personales 188 ; en segundo lugar, va en contra del principio de finalidad 189 , pues los usuarios publican su dirección personal con un fin específico, como participar en un foro de debate, muy diferente de la recepción de mensajes electrónicos comerciales; en tercer lugar, no se puede considerar que satisface el criterio del equilibrio de intereses 190 , pues el destinatario sale perdiendo en cuestión de tiempo y dinero y sufre molestias irrazonables.

- Cinco Estados miembros (Alemania, Austria, Italia, Finlandia y Dinamarca) han adoptado medidas dirigidas a prohibir las comunicaciones comerciales no solicitadas.

En algunos de los Estados miembros restantes existe un sistema de oposición a la recepción de dichos mensajes; en otros, la situación no está muy clara. Las empresas de los países que disponen de tal sistema de oposición pueden enviar mensajes no sólo a direcciones de correo electrónico de su propio país, sino también a consumidores de otros Estados miembros donde exista un sistema de consentimiento.

Además, al ser frecuente que las direcciones de correo electrónico no indiquen el país de residencia de los destinatarios, un sistema de regímenes divergentes dentro del mercado interior no proporciona una solución común para proteger la privacidad del consumidor. Por lo tanto, el sistema de consentimiento es una solución bien equilibrada y eficaz para suprimir los obstáculos a la transmisión de comunicaciones comerciales al mismo tiempo que se protege el derecho fundamental de privacidad de los consumidores. Así pues, el Grupo de Trabajo acoge favorablemente y apoya la propuesta de tratar los mensajes electrónicos no comerciales de la misma manera que los aparatos de llamada automática y los facsímiles.

En todas estas situaciones, el abonado no cuenta con un interlocutor humano y corre como mínimo con una parte de los costes de la comunicación. El grado de invasión de la privacidad y la carga económica son comparables 191 .

CAPÍTULO 9: MEDIDAS EN FAVOR DE LA PRIVACIDAD

I. Introducción

La Directiva comunitaria sobre protección de datos contiene dos principios con consecuencias directas en el diseño y el uso de nuevas tecnologías: - Su "principio de finalidad" exige que los datos personales se utilicen únicamente cuando sea necesario con un fin específico legítimo; es decir, no se permite el uso de los datos personales sin una razón legítima, y el individuo guarda el anonimato (letra b del primer apartado del artículo 6 y artículo 7).

- Su "principio de seguridad de los datos" exige que los responsables del tratamiento apliquen medidas de seguridad apropiadas a los riesgos que afectan al almacenamiento o la comunicación de los datos personales, con vistas a protegerlos contra la destrucción accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento conlleve la transmisión de datos dentro de una red, y contra otra forma ilícita de tratamiento (artículo 17).

El principio de "finalidad" mencionado es el motivo subyacente del concepto de tecnologías de protección de la privacidad, que se refiere a una serie de tecnologías que salvaguardan la privacidad personal, sobre todo minimizando o eliminando la recogida o el tratamiento de datos identificables 192 .

Las tecnologías de protección de la privacidad intentan obstaculizar cualquier forma ilegal de tratamiento, por ejemplo haciendo técnicamente imposible que personas no autorizadas accedan a datos personales, con lo que se evita la destrucción, la alteración y la revelación de tales datos.

La aplicación práctica de este concepto requiere soluciones organizativas y técnicas.

A menudo estas tecnologías se basan en el uso de un protector de la identidad 193 , que se puede considerar un elemento del sistema que controla la divulgación de la identidad verdadera de una persona en diversos procesos del sistema de información.

Su efecto es el acordonamiento de determinadas áreas del sistema que no requieren acceso a la identidad verdadera. Una de las funciones más importantes del protector de la identidad es la de convertir la identidad real de un usuario en una seudoidentidad, una identidad sustitutiva (digital) que el usuario puede adoptar cuando utiliza el sistema.

Para introducir un protector de la identidad en un sistema de información se pueden utilizar varias técnicas, entre las que encontramos las de *encriptación* con *firmas*

*electrónica*s, firmas ciegas, seudónimos electrónicos y *terceros de confianza.*

II. Tecnologías en favor de la privacidad

Este apartado describe y analiza diversas tecnologías en favor de la privacidad 194 .

Anuladores de*cookies*

A continuación se analizan dos tipos diferentes de respuesta a los problemas de privacidad que suscitan las *cookie*s. El primero surgió de la propia industria de Internet y se ha incorporado a los principales navegadores del mercado, mientras que el segundo procede de diversos grupos defensores de la privacidad o empresas de software y consiste en una serie de herramientas que permiten borrar todas las *cookies* o una parte de ellas.

Mecanismos de oposición a las cookies *utilizados por la industria* El único intento visible de resolver el problema de las *cookies* es el mecanismo de oposición a las *cookies* utilizado a partir de la versión 3 de los navegadores más extendidos. Al configurar el navegador, el usuario precavido puede elegir entre tres opciones: - Aceptar todas las *cookies.*

- Rechazar todas las *cookies* o las *cookies* que no se vuelven a enviar al servidor de origen (Netscape).

- Ser consultado en cada caso.

No obstante, los mecanismos de oposición a las *cookies* siguen siendo insuficientes por muchos motivos: 1. Normalmente, la configuración por defecto (aceptar todas las *cookie*s) es la que más invade la privacidad, y el usuario medio de Internet ignora el amplio uso que las empresas de cibermarketing, por ejemplo, hacen de las *cookies* para rastrear palabras clave en motores de búsqueda a través de medios invisibles de tratamiento.

2. El mecanismo de bloqueo de *cookies* impide la recepción de nuevas *cookies,* pero no el envío sistemático e invisible de las *cookies* que ya se han recibido.

3. Las *cookies* pueden presentar naturalezas muy diferentes: algunas resultan útiles y no son identificativas (por ejemplo, la lengua preferida); otras son identificativas pero pueden respetar las reglas de privacidad. En general, se puede decir que las *cookies* de sesión 195 son mucho menos invasivas de la privacidad que las duraderas. Al usuario de Internet podría no interesarle rechazar todas las *cookie*s.

4. Ciertos sitios web deniegan el acceso a los usuarios que no quieren aceptar *cookie*s.

5. Ciertos sitios web (sitios web con *hipervínculos* invisibles) envían series de *cookie*s.

Un enfoque caso por caso obliga al usuario a rechazar cada una de ellas una tras otra, lo que origina una "fatiga del clic" que lleva al usuario a aceptar la *cookie* para que no lo interrumpan más.

6. En algunos casos, el mensaje que transmite la *cookie* 196 parece estar incompleto y puede inducir a error.

7. Al instalar un navegador, el primer sitio que se visite (por defecto, el sitio del fabricante del navegador) puede enviar una *cookie* antes de que el usuario haya tenido la oportunidad de desactivar la aceptación de *cookie*s.

En julio de 2000, Microsoft anunció que en la siguiente versión de Internet Explorer iba a introducir la versión beta de un programa complementario de seguridad que permitiría gestionar mejor las *cookies* de la red 197 . Según las primeras descripciones, este programa incluirá diversas características que permitirán a los usuarios controlar mejor las *cookie*s.

El navegador será capaz de diferenciar entre las *cookies* procedentes del interlocutor y las de terceras partes, y la configuración por defecto advertirá al usuario cuando se esté instalando una *cookie* duradera procedente de terceras partes.

Además, la nueva funcionalidad permitirá a los usuarios de Internet suprimir todas las *cookies* con un simple clic y dará un acceso más fácil a la información sobre seguridad y privacidad. Sin embargo, este programa complementario de seguridad no aumenta el control del consumidor sobre el uso de *cookies* del interlocutor, frecuentes en los sitios web comerciales.

Programas independientes

"Cookie washer", "Cookie cutter", "Cookie master" y "Cookie cruncher" son algunos de los programas de software gratuito o *software compartido* que todo usuario puede descargar y utilizar en la red 198 . Sobre ellos se pueden formular comentarios similares a los anteriores: 1. El usuario de Internet ha de tratar sus propios ficheros *cookies* a diario y caso por caso debido a las diferentes naturalezas de las *cookie*s.

2. En el caso de programas de *software compartid*o, en ocasiones el usuario de Internet ha de pagar por protegerse.

3. El mecanismo de manejo de *cookies* no es siempre fácil de utilizar o de comprender para un usuario medio de Internet.

Servidores proxy

El *servidor proxy* es un servidor intermediario entre el usuario de Internet y la Red.

Actúa como una *caché web* y mejora de un modo extraordinario el funcionamiento de Internet, por lo que muchas grandes organizaciones o proveedores de acceso a Internet ya han aplicado esta solución. Cada página, imagen o logotipo descargado desde el exterior por un miembro de una organización se almacena en una caché en el *servidor proxy* y queda automáticamente disponible para los otros miembros de la misma organización.

En este caso no es necesario que cada miembro de la organización situado ante el *servidor proxy* tenga su propia dirección IP, pues no accede directamente a Internet.

Además, normalmente el *servidor proxy* no transmitirá 199 la dirección IP del usuario de Internet al sitio web y puede filtrar el charloteo del navegador.

Dado que el *servidor proxy* maneja el *protocolo* HTTP, puede suprimir, cambiar o almacenar fácilmente las *cookies* almacenadas en la cabecera HTTP.

Software que garantiza el anonimato

Estos programas permiten a los usuarios interactuar de forma anónima cuando visitan sitios web, pues primero pasan por un sitio que garantiza su anonimato disfrazando su identidad 200 .

Deteniéndose en un sitio web que garantiza el anonimato antes de ir a ningún otro, el usuario puede permitir que se oculten datos personales, como su dirección IP, al sitio web que visite. Los sitios de anonimato bloquean también el envío de datos del sistema (como el sistema operativo y el navegador que se están utilizando) a los sitios web, impiden se instalen *cookies* en los navegadores y bloquean los módulos *Java* y *JavaScrip*t, que en otro caso pueden acceder a datos personales de los navegadores.

Anonymizer 201 y Zero Knowledge System 202 son dos buenos ejemplos de ello.

Anonymizer pretende:

* actuar como un intermediario entre el usuario y los sitios que visita, ocultando su identidad ante medidas invasivas de rastreo;

* bloquear los programas incluidos en la página web *(Java* y *JavaScrip*t) que pueden dañar el ordenador del usuario o reunir datos personales confidenciales.

Anonymizer ofrece dos servicios (la navegación anónima y el correo electrónico anónimo) y un producto (el servidor que garantiza el anonimato), que permite a cualquier usuario crear un sitio propio que garantice el anonimato.

En ocasiones, el usuario de Internet ha de pagar para poder aprovechar plenamente las ventajas de los servicios que garantizan el anonimato. Para poder utilizar los servicios del sitio web de Anonymizer ha de estar continuamente conectado a él, lo que significa que este servicio es muy vulnerable a la vigilancia de terceras partes.

Anonymizer puede prestar servicios anónimos como la navegación, el correo o la transferencia de ficheros.

Técnicamente hablando, Anonymizer actúa como un *servidor proxy* y ocultará el charloteo del navegador HTTP y la dirección IP del usuario.

El principal problema que presenta el uso de este servicio es que el usuario de Internet tiene que depositar su confianza en una empresa específica que estará al corriente de cada paso que el usuario dé en la red.

Zero Knowledge System propone un programa denominado "Freedom" que se basa al menos en tres retransmisores TCP/IP combinados con una *encriptación* muy fuerte (de 128 bits como mínimo). Dado que todos los servicios de la red utilizan el *protocolo* TCP/IP, con este sistema todos quedan encriptados y en el anonimato.

Cada una de las tres estaciones retransmisoras TCP/IP conoce únicamente la dirección TCP de su predecesora. No llevan ningún fichero registro, por lo que incluso dos retransmisores unidos serían incapaces de rastrear la información solicitada o recuperada. La ruta de la información es, por supuesto, dinámica, y es probable que cambie incluso durante una comunicación muy corta. Parece ser que en Freedom se ha integrado un sistema de gestión de *cookie*s.

Otro ejemplo de este tipo de servicios es el que ofrece **privada.com**, empresa que presta servicios de apoyo a todos los tipos de transacciones de la red, incluidos la navegación, el correo electrónico, la mensajería y, pronto, el comercio. La infraestructura de Privada se basa en un sistema de compartimentación y *encriptació* n.

El usuario recibe un CD-ROM o descarga una aplicación cliente, PrivadaControl, desde su *proveedor de servicios de Internet*. PrivadaControl se comunica con los servidores de la red de Privada situados en las instalaciones del *proveedor de servicios de Internet* y funciona como un *cortafuegos* para la privacidad personal del usuario. PrivadaControl está orientado a proteger toda la información y los datos de los usuarios desde el punto de la transacción y a través de su camino por la red, garantizando la privacidad del usuario desde todos los puntos de vista, incluido el de Privada y el del *proveedor de servicios de Internet*.

Al usar PrivadaControl, el usuario crea una cuenta electrónica privada que representa sus actividades en línea al tiempo de disocia completamente toda la información personal del usuario de la actividad en línea. PrivadaControl parece permitir que el usuario cree o suprima identidades electrónicas, elija entre ellas mientras interactúa en línea y configure sus propios atributos y características.

Este sistema no bloquea todas las aplicacioncitas en *Java*, *cookie*s, o controles ActiveX, pero permite al usuario decidir a qué nivel pueden funcionar la personalización y los servicios de la red. Las *cookies* no se colocan en el ordenador personal del usuario, sino en servidores centralizados de la red Privada. Todos los ficheros históricos o intentos de

minería de datos por parte de un sitio web están asociados con la identidad del usuario en línea, y no con su identidad real. Privada afirma que los usuarios pueden suprimir fácilmente una o todas las *cookies* que se hayan instalado.

El sistema propuesto por **iPrivacy** está diseñado para permitir el comercio electrónico anónimo, desde navegar, hasta comprar y enviar. Permite a los consumidores navegar, buscar y comprar en la Red de forma privada y recibir lo que hayan comprado sin que se revele la identidad del destinatario. De acuerdo con la empresa, ni siquiera ellos mismos podrían conocer la verdadera identidad de los clientes que hacen uso de sus servicios. En cuanto a la transacción, sólo el cliente y el usuario de la tarjeta de crédito conocerían información personal sobre la compra realizada en línea 203 .

Filtros de correo electrónico y correo electrónico anónimo 204

Estos sistemas ya se han descrito en el capítulo sobre el correo electrónico. Lo que sigue es un resumen de sus rasgos principales: - Los filtros de correo electrónico examinan los mensajes electrónicos que llegan a un usuario y sólo dejan pasar los que dicho usuario ha indicado que quiere recibir. Se suelen utilizar para descartar la propaganda por correo.

- El correo electrónico anónimo permite a los usuarios ofrecer su dirección de correo electrónico en línea sin tener que revelar su identidad 205 . Actualmente se puede acceder de forma gratuita a este servicio en Internet a través de una serie de empresas que prestan servicios "de reenvío" eliminando la identidad del usuario antes de volver a enviar el mensaje electrónico.

Informediarios

Un usuario puede también decidir utilizar lo que se denomina un informediario 206 , que se ha descrito como "una persona de confianza o una organización con acceso a la red especializada en servicios de información y conocimientos destinados a la comunidad virtual, sobre ella y en su nombre. El informediario facilita y estimula la comunicación inteligente y la interacción entre los miembros de dicha comunidad. También administra y cultiva un activo de conocimiento privado con contenido e *hipervínculos* de interés específico para la comunidad. De acuerdo con los condicionantes de la privacidad que exige la comunidad virtual, el informediario reúne, organiza y libera de forma selectiva información acerca de la comunidad y de sus miembros para cubrir las necesidades de la comunidad virtual... ".

El informediario es un nuevo tipo de intermediario empresarial que ayuda a los clientes a captar, gestionar y maximizar el valor de sus datos personales 207 . Los consumidores han demostrado que están dispuestos a dar información personal siempre y cuando puedan sacar algún provecho de ello, aunque cada vez se dan más cuenta de que están vendiendo su privacidad a un precio muy bajo a empresas que la utilizan en beneficio propio. Lo que consiguen gracias a la información que divulgan es, en una palabra, insatisfactorio 208 .

Los informediarios podrían ayudar a los consumidores a cerrar mejores tratos con los vendedores, agregando sus datos a los de los consumidores y usando su poder de mercado conjunto para negociar por su cuenta con los vendedores.

Actúan como guardianes, agentes y corredores de información de los consumidores, vendiéndola a empresas (y ofreciéndoles acceso a ella) en nombre del consumidor, al mismo tiempo que protegen sus datos personales del abuso.

El aspecto positivo de los informediarios es que, en muchos casos, pueden comprar los bienes o servicios que desean y hacerlos llegar al consumidor final sin que éste salga del anonimato. También pueden proporcionar agentes inteligentes que ayuden a los abonados a cumplir su tarea.

En teoría, los clientes de los informediarios tendrán la opción de seguir en el anonimato mientras navegan por la Web y realizan compras en línea.

Sin embargo, se les instará a que no lo hagan, pues cada vez que accedan a divulgar su identidad o su dirección de correo de electrónico, los vendedores les pagarán una pequeña cuota o les aplicarán un descuento en el precio del producto vendido.

Los clientes también recibirán pagos en metálico si dan a determinadas empresas acceso a su perfil personal. El importe del pago dependerá de las preferencias de privacidad de cada cliente. Quienes elijan seguir en el anonimato total renunciarán a los pagos en metálico, a cambio de la garantía de su privacidad, mientras que quienes acepten los controles impuestos por el intermediario sobre el acceso a su información y entiendan el interés de una revelación selectiva pueden ganar dinero.

En conclusión, se puede afirmar que si un informediario puede desempeñar una papel positivo a la hora de proteger los datos de los usuarios con los que mantiene una relación de confianza, la base de este acuerdo es la posibilidad de generar beneficios divulgando los datos personales de los clientes y dando acceso a ellos.

Según las circunstancias y la naturaleza del informediario, éste puede ser tanto un protector de la privacidad como un invasor de la misma.

III. Otras medidas en favor de la privacidad

También se pueden utilizar otras técnicas para mejorar la transparencia del tratamiento o facilitar el ejercicio de los derechos del interesado. A continuación se dan algunos ejemplos:
 P3P P3P significa Plataforma de Preferencias de Privacidad 209 . Su objetivo es permitir que los sitios web expresen sus preferencias de privacidad y los usuarios ejerzan sus preferencias sobre estas prácticas, de forma que puedan tomar decisiones con conocimiento de causa sobre sus experiencias en la Web y controlar el uso de su información.

Toda la comunidad de protección de datos ha seguido el desarrollo de la P3P con gran interés.

En abril de 1998, el Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones emitió una posición común sobre los puntos esenciales de las tecnologías en favor de la privacidad (por ejemplo, P3P) en la World Wide Web 210 . Este documento establece las condiciones esenciales que ha de satisfacer cualquier plataforma técnica para la protección de la privacidad en la World Wide Web, con el objetivo de evitar la recogida sistemática de datos personales:

1. La tecnología en sí misma no puede garantizar la privacidad en la Web y se ha de aplicar siguiendo un marco normativo.

2. Cualquier usuario debería tener la posibilidad de navegar de forma anónima, lo que también es aplicable a la descarga de información del dominio público.

3. Antes de que un proveedor de sitios web trate datos personales, y sobre todo los revelados por el usuario, se ha de obtener el consentimiento fundamentado de éste.

Además, en la configuración por defecto de la plataforma técnica se deberían introducir ciertas reglas de base ineludi - bles.

Dos meses más tarde, en junio de 1998, el Grupo de Trabajo emitió también un dictamen 211 que hacía hincapié en que una plataforma técnica de protección de la privacidad no sería suficiente, por sí sola, para proteger la privacidad en la Web. La plataforma se ha de aplicar en el contexto de un marco de normativas aplicables sobre protección de datos que proporcionen un nivel mínimo, no negociable, de protección de la privacidad para todas las personas. El dictamen mencionaba asimismo una serie de cuestiones específicas que surgirían con la aplicación de tal sistema en la Unión Europea.

En septiembre de 1999 se organizó un seminario conjunto para investigar la aplicación de la P3P en el contexto de la Directiva europea sobre protección de datos y fomentar la comunicación entre la comunidad de protección de datos de la UE y los desarrolladores de software. En el seminario participaron una delegación de alto nivel del W3C y miembros del Grupo operativo sobre Internet. En él se demostró que todavía se ha de tratar un buen número de cuestiones.

Una vez que se solucionen, la P3P podría desempeñar un papel positivo si se aplica en el marco adecuado. Los prin - cipales aspectos positivos de la P3P son los siguientes 212 : - La P3P puede ayudar a normalizar los avisos relacio - nados con la privacidad. Aunque en sí mismo esto no puede proteger la privacidad, si se ejecuta podría proporcionar mucha más transparencia y utilizarse para apoyar los esfuerzos por mejorar la protección de la privacidad.

- La P3P puede apoyar el aumento de las posibilidades de privacidad, incluidos el anonimato y el uso de seudónimos.

Sin embargo, conviene ser consciente de las limitaciones 213 de la P3P: - La P3P no puede proteger a los usuarios en países cuya legislación sobre la privacidad es insuficiente, pues no puede crear medidas públicas ni exigir que sus especificaciones se sigan en el mercado.

- La P3P no puede garantizar que las empresas sigan las políticas de privacidad. De hecho, no puede garantizar que el sitio esté haciendo lo que afirma hacer. Las sanciones por incumplir una declaración de intenciones sólo pueden establecerse por ley o mediante la adhesión a un organismo autorregulador.

La etiqueta de privacidad

Se trata de un sello de calidad que se impone a un sitio web. A lo largo de los años han aparecido diversas etiquetas de privacidad, entre las que destacan las de TRUSTe 214 , Privaseek 215 , Better Business Bureau 216 y WebTrust 217 . Algunas de estas organizaciones estadounidenses opera en el ámbito internacional, incluida Europa; otras aspi - ran a hacerlo. Al mismo tiempo, en Europa están surgiendo iniciativas similares con fines internacionales, por ejemplo L&belsite en Francia.

Las etiquetas de privacidad se otorgan a las empresas que cumplen una serie de requisitos especificados por el orga - nismo que las concede, que puede ejercer algún tipo de control sobre el cumplimiento de las políticas de privacidad de las empresas que las poseen mediante revisiones periódicas de sus actividades. En algunos casos, el organismo que concede la etiqueta se encarga también de las quejas presentadas contra empresas que tienen la etiqueta en sus sitios web.

La etiqueta de privacidad plantea una serie de cuestiones: 1. La primera se refiere al contenido de la etiqueta. El derecho a la información y al acceso, el principio de minimización de datos, el derecho a oponerse, el principio de legitimidad y proporcionalidad y la obligación de notificar a la autoridad nacional de protección de datos son algunas de las piedras angulares de los principios europeos de protección de datos. El principal riesgo social sería la difusión

de etiquetas de privacidad en toda Europa, lo que confundiría a los usuarios y a los responsables del tratamiento.

Aunque pueden dar esta impresión, no todas las etiquetas garantizan seriamente todos los principios de protección de datos mencionados.

2. El segundo problema radica en el control de las prácticas de privacidad de los sitios web. Se pueden practicar numerosos tipos de control. Algunas de las principales preocupaciones al respecto son: - ¨Quién tiene el control? ¨Cómo lo ejerce? ¨Con qué clase de mandato otorgado por la empresa controlada? En el peor de los casos, parece que el responsable del tratamiento será, principalmente, el propio interesado, con todos los problemas que esto conlleva a la hora de identificar los fallos en la observación de las prácticas de privacidad declaradas, demostrarlos y notificarlos a la empresa que asigna las etiquetas. Además, no todos los organismos que conceden etiquetas pueden garantizar que las empresas actúen según pretenden sus políticas.

- ¨Quién pagará? Dado que la asignación de etiquetas es una iniciativa privada que a menudo no cuenta con apoyo económico gubernamental, algunos organismos que conceden etiquetas sufrirán la presión de las empresas que supuestamente controlan.

- ¨Qué sanciones se impondrán, si se impone alguna? Sin embargo, no se deben subestimar los posibles efectos de las etiquetas de privacidad en la protección de ésta, pues pueden ayudar a concienciar a los usuarios de Internet sobre la privacidad. Se pueden formular algunas propuestas para abordar los problemas mencionados: 1. El conte - nido de la etiqueta: Con el fin de garantizar que las etiquetas de privacidad cumplen las normas de la legislación europea sobre protección de datos, el Grupo de

Trabajo podría acordar una norma europea de etiquetas de privacidad con los requisitos que debe cumplir una etiqueta 218 .

Mientras los usuarios de Internet tengan claro qué etiquetas son las que cumplen las normas europeas, pueden coexistir varias.

2. El control de las prácticas de privacidad del sitio web: La fiabilidad de las prácticas de privacidad del sitio web podría mejorar considerablemente si se obligase a los sitios dotados de una etiqueta a someterse a auditorías periódicas.

La norma europea de etiquetas de privacidad podría incluir este requisito y determinar posibles formas de llevar a cabo estos controles obligatorios: auditoría realizada por el propio sitio con la ayuda de una lista de control, auditoría realizada por terceros, etc.

IV. Conclusiones

* Se deberían emitir recomendaciones sobre el diseño de navegadores conformes a la protección de la privacidad y cuya configuración por defecto respete la privacidad al máximo.

* Los *servidores proxy* anónimos pueden ocultar la dirección IP. Todos los *proveedores de servicios de Internet* los podrían ofrecer como un elemento gratuito estándar con cada suscripción a Internet.

* Los sitios web no deberían denegar el acceso a los usuarios que no quieran aceptar *cookie*s, a menos que sean indispensables *cookies* de sesión para establecer un vínculo entre el usuario y sus diversas compras en la red y hacer así posible que la facturación se realice de forma adecuada.

* Se debería fomentar el uso de tecnologías a favor de la privacidad, especialmente si quienes las instalan son los *proveedores de servicios de Internet* u otros agentes.

* Parece ser que los usuarios necesitan más información sobre la existencia de tecnologías en favor de la privacidad. El sector público debería dar los pasos necesarios para concienciar más sobre este tema y apoyar el desarrollo de este tipo de soluciones, además de utilizarlas y fomentarlas 219 .

* El Grupo de Trabajo podría acordar una norma europea sobre etiquetas de privacidad que debería incluir la obliga - ción de que los sitios web se sometan a auditorías periódicas.

CAPÍTULO 10: CONCLUSIONES

En este documento se ha abordado una serie de temas presentados en capítulos separados. Cada uno de ellos incluye comentarios exclusivos sobre cuestiones concretas.

Sin embargo, ciertas cuestiones comunes que guardan relación con todos los servicios de Internet descritos en el documento merecen tratarse en términos más generales.

Tras resumir las tendencias y de los riesgos de la privacidad que se han observado en los diversos aspectos del uso de Internet, se ha intentado ofrecer algunas directrices y recomendaciones, teniendo en cuenta acciones que podrían desarrollarse a varios niveles.

1. Tendencias y riesgos

El desarrollo de Internet es exponencial. El usuario de Internet dispone de un número cada vez mayor de servicios, desde realizar compras en línea hasta participar en foros con gente de todo el mundo. Debido a la complejidad de la Red, cada ver resulta más difícil formarse una visión general de todas las posibilidades que se ofrecen al usuario. Las empresas buscan una forma de atraerlo y destacarse de otras ofreciendo servicios personalizados y/o gratuitos.

La personalización de los servicios depende de la utilización de datos personales de los usuarios, que las empresas tratan de conseguir de diversas formas, como animar a los propios usuarios a que los proporcionen en el marco de programas de fidelidad, hacerles regalos o prestarles servicios gratuitos, recogerlos de fuentes públicas, etc.

Los perfiles que se elaboran no sólo son valiosos para las empresas que quieren dirigirse al consumidor, sino que además tienen un valor económico en sí mismos, pues a menudo se venden y alquilan a otras empresas.

El desarrollo de nuevas tecnologías facilita el seguimiento de los usuarios de Internet.

Por ejemplo, cuando un consumidor utiliza un teléfono móvil para conectarse a Internet se pueden generar datos que indiquen su situación.

Cuando el usuario se conecta a Internet a través de nuevos medios como las líneas *ADSL* o el cable, se le asigna una dirección IP estática que facilita su rastreo de una sesión a otra. Las nuevas generaciones de software y hardware ofrecen características que aumentan la capacidad de controlar las actividades del usuario en tiempo real, a menudo sin que ellos mismos lo sepan. En todo este documento se dan numerosos ejemplos de tratamiento invisible y programas E.T.

En este contexto, el usuario medio cada vez tiene más difícil mantenerse en el anonimato mientras navega por la red.

La combinación de estas capacidades en desarrollo conlleva nuevos riesgos para la privacidad del usuario de Internet, sobre todo cuando los datos están concentrados en las manos de uno o de pocos responsables del tratamiento.

Cuando los responsables del tratamiento utilizan las tecnologías de *minería de dato*s, por ejemplo, técnicamente no sólo tienen la posibilidad de tratar y reorganizar los datos, sino también de descubrir nuevos vínculos y características relacionadas con su titular, que normalmente no es consciente de esta posibilidad y no espera que se trate esa información.

Estos riesgos se deben también a que algunos datos se conservan en línea durante un período muy largo de tiempo; por ejemplo, son muchos los mensajes enviados a los foros de debate y las listas de correo que se conservan durante varios años y se pueden consultar mediante herramientas de búsqueda inversa.

Esta disponibilidad de datos personales permite usos secundarios inesperados que suelen ser incompatibles con el fin para el que se recabaron en principio.

2. Directrices y recomendaciones

2.1. Concienciación del usuario de Internet

Dado que, como ya se ha mencionado, los riesgos para la privacidad del usuario son cada vez mayores, resulta especialmente importante garantizar que se utilizan medios adecuados a la hora de garantizar que éste recibe toda la información que precisa para tomar una decisión con conocimiento de causa. En este proceso de informar al usuario participan varios agentes.

En primer lugar, cualquier responsable del tratamiento que recabe datos personales debe proporcionar al interesado toda la información necesaria.

Dicha información, mencionada en el artículo 10 de la Directiva 95/46/CE, ha de proporcionarse en todos los casos en el momento en que se produzca la recogida de datos. Aunque un sitio web haga pública su política de privacidad, lo que resulta útil para que el público esté informado, cada vez que se recojan datos se ha de informar a su titular de una forma simple y accesible; por ejemplo, en la misma pantalla en la que se han de introducir los datos o mediante un cuadro de diálogo.

Cuando el responsable del tratamiento es una empresa privada, el cumplimiento de estas normas no es sólo importante en términos legales, sino también para sus propios intereses, pues propiciará una mayor confianza de los usuarios, lo que podría repercutir en la implicación de éstos en la empresa. En cuanto al desarrollo del comercio electrónico, por ejemplo, se observa que cuando los usuarios temen que sus datos personales no van a contar con una protección y una seguridad correctas se muestran reacios a emprender transacciones electrónicas.

Si el responsable del tratamiento es una autoridad pública, el cumplimiento de las normas de protección de datos es un elemento clave, pues su comportamiento dará ejemplo al público en general. Por ejemplo, las autoridades públicas

que realizan actividades electrónicas gubernamentales deberían basarse en la privacidad como una de las piedras angulares del sistema de intercambio de datos. Además, incluso cuando no desempeñan el papel de responsable del tratamiento, la responsabilidad de estas autoridades reside en la educación general y la información del público.

En particular, a las autoridades de protección de datos se les ha confiado la tarea de concienciar a la población sobre los riesgos relacionados con el uso de Internet, pero también sobre los derechos y las obligaciones que prevé la legislación. Esto se puede conseguir de diferentes formas, como la publicación de folletos, informes, comunicados de prensa y recomendaciones prácticas incluidas en las solicitudes de notificación, así como mediante la organización de conferencias o seminarios sobre estos asuntos, dirigidos a los diferentes agentes y sectores de la sociedad, o la participación en ellos.

Tradicionalmente, los defensores de la privacidad han asumido la función de la concienciación pública y en ocasiones sus esfuerzos han conducido a mejoras significativas del respeto de la privacidad de los productos de Internet.

En varios países de la Unión Europea se ha observado que las asociaciones de consumidores tienen una participación y un interés crecientes en las cuestiones relacionadas con la privacidad de las actividades de los consumidores.

Este papel puede ser especialmente positivo, ya que no se limita a proporcionar información, sino que además incluye la representación de los consumidores en su relación con las empresas o las autoridades públicas. Estas asociaciones, por ejemplo, pueden controlar que los *proveedores de servicios de Internet* cumplan la ley, o informar a las autoridades públicas de las quejas que reciben sobre un sitio web concreto o sobre una empresa de Internet.

Las asociaciones profesionales también pueden influir positivamente informando a los nuevos agentes sobre sus obligaciones legales.

Todas las partes aquí mencionadas desempeñan un papel significativo a la hora de facilitar al consumidor la información que necesita para poder tomar decisiones tomar una decisión con conocimiento de causa. En este proceso de informar al usuario participan varios agentes.

En primer lugar, cualquier responsable del tratamiento que recabe datos personales debe proporcionar al interesado toda la información necesaria.

Dicha información, mencionada en el artículo 10 de la Directiva 95/46/CE, ha de proporcionarse en todos los casos en el momento en que se produzca la recogida de datos. Aunque un sitio web haga pública su política de privacidad, lo que resulta útil para que el público esté informado, cada vez que se recojan datos se ha de informar a su titular de una forma simple y accesible; por ejemplo, en la misma pantalla en la que se han de introducir los datos o mediante un cuadro de diálogo.

Cuando el responsable del tratamiento es una empresa privada, el cumplimiento de estas normas no es sólo importante en términos legales, sino también para sus propios intereses, pues propiciará una mayor confianza de los usuarios, lo que podría repercutir en la implicación de éstos en la empresa. En cuanto al desarrollo del comercio electrónico, por ejemplo, se observa que cuando los usuarios temen que sus datos personales no van a contar con una protección y una seguridad correctas se muestran reacios a emprender transacciones electrónicas.

Si el responsable del tratamiento es una autoridad pública, el cumplimiento de las normas de protección de datos es un elemento clave, pues su comportamiento dará ejemplo al público en general. Por ejemplo, las autoridades públicas que realizan actividades electrónicas gubernamentales deberían basarse en la privacidad como una de las piedras angulares del sistema de intercambio de datos. Además, incluso cuando no desempeñan el papel de responsable del tratamiento, la responsabilidad de estas autoridades reside en la educación general y la información del público.

En particular, a las autoridades de protección de datos se les ha confiado la tarea de concienciar a la población sobre los riesgos relacionados con el uso de Internet, pero también sobre los derechos y las obligaciones que prevé la legislación. Esto se puede conseguir de diferentes formas, como la publicación de folletos, informes, comunicados de prensa y recomendaciones prácticas incluidas en las solicitudes de notificación, así como mediante la organización de conferencias o seminarios sobre estos asuntos, dirigidos a los diferentes agentes y sectores de la sociedad, o la participación en ellos.

Tradicionalmente, los defensores de la privacidad han asumido la función de la concienciación pública y en ocasiones sus esfuerzos han conducido a mejoras significativas del respeto de la privacidad de los productos de Internet.

En varios países de la Unión Europea se ha observado que las asociaciones de consumidores tienen una participación y un interés crecientes en las cuestiones relacionadas con la privacidad de las actividades de los consumidores.

Este papel puede ser especialmente positivo, ya que no se limita a proporcionar información, sino que además incluye la representación de los consumidores en su relación con las empresas o las autoridades públicas. Estas asociaciones, por ejemplo, pueden controlar que los *proveedores de servicios de Internet* cumplan la ley, o informar a las autoridades públicas de las quejas que reciben sobre un sitio web concreto o sobre una empresa de Internet.

Las asociaciones profesionales también pueden influir positivamente informando a los nuevos agentes sobre sus obligaciones legales.

Todas las partes aquí mencionadas desempeñan un papel significativo a la hora de facilitar al consumidor la información que necesita para poder tomar decisiones reconocimiento sencillo de los productos que cumplen los requisitos de protección de datos.

Por otra parte, aunque es frecuente que las nuevas tecnologías se consideren una amenaza para la privacidad, convendría destacar que también representan una herramienta útil de salvaguardia de la misma.

En primer lugar, algunas de las tecnologías existentes pueden utilizarse para mejorar la transparencia y la facilidad de manejo de la información que se proporciona al interesado, por ejemplo dando a los usuarios información simple y accesible en el momento de recabar sus datos personales.

En segundo lugar, pueden constituir una herramienta útil para simplificar el ejercicio de los derechos de los titulares de los datos, por ejemplo permitiendo un acceso directo en línea a los datos personales del usuario o dando la posibilidad de oponerse al proceso.

Si se tiene en cuenta que el usuario medio no está necesariamente familiarizado con los aspectos técnicos del uso de Internet y que no siempre está en situación de decidir sobre la configuración del hardware y el software, ni de cambiarla, es de vital importancia que las configuraciones por defecto de los productos ofrezcan el máximo nivel de protección de la privacidad.

Se ha desarrollado una serie de herramientas adicionales, más conocidas como "tecnologías a favor de la privacidad", para ayudar a los usuarios a salvaguardar su privacidad, sobre todo minimizando o eliminando la recogida o el posterior tratamiento de datos identificables y dificultando técnicamente cualquier forma ilegal de tratamiento.

Algunos ejemplos de estas herramientas son los *servidores prox*y, los anuladores de *cookie*s, el software que garantiza el anonimato, las herramientas de elaboración de seudónimos (especialmente valiosas en la elaboración de perfiles), los filtros de correo electrónico, etc. Entre los posibles nuevos productos podrían estar las tarjetas inteligentes con un protector portátil de la identidad que el usuario podría introducir en cualquier máquina con la que se conectase en línea.

De todos los agentes mencionados en el apartado 2.1., la industria y el sector público son los primeros que deberían invertir en el desarrollo y la ejecución de tecnologías a favor de la privacidad y fomentarlas. Se debería concienciar al usuario de la existencia de estos medios, que, por otra parte, deberían estar disponibles a precios razonables.

2.4. Establecimiento de mecanismos fiables de control y retroalimentación

Los datos en línea sólo se pueden proteger de forma eficaz si se dispone de los medios adecuados para controlar y evaluar el respeto del marco legal y de los requisitos técnicos explicados anteriormente.

Para lograrlo, aunque las principales encargadas de ese control son las autoridades de protección de datos, otros agentes están tomando medidas dirigidas a la autoevaluación, pues han comprendido el impacto de su política de privacidad en el comportamiento de sus consumidores hacia ellos.

Las autoridades de protección de datos pueden contribuir al desarrollo y al buen funcionamiento de estos sistemas de autoevaluación proporcionando orientación, por ejemplo, en forma de listas de control de autoevaluación normalizadas a escala europea.

Además, se podrían conceder etiquetas para ayudar a los consumidores a conseguir una indicación fiable acerca del respeto de la legislación comunitaria sobre protección de datos en el tratamiento de éstos. El Grupo de Trabajo pretende actuar en este ámbito principalmente para garantizar que las etiquetas de privacidad se asignan a sitios web que respetan esta legislación.

El Grupo de Trabajo invita a todos los agentes que participan en actividades de Internet a que tengan en cuenta este documento de trabajo y den los pasos necesarios para llevar a la práctica sus recomendaciones.

El Grupo de Trabajo espera que este documento de trabajo contribuya a concienciar a los usuarios y que fomente un debate público sobre el tema que, sin duda, requerirá un análisis más profundo y un futuro seguimiento.

GLOSARIO DE TÉRMINOS TÉCNICOS

ADSL

La línea de suscripción asimétrica digital o *ADSL* es un *protocolo* de telecomunicaciones que se puede utilizar con los pares trenzados de cobre clásicos.

Permite alcanzar una velocidad de hasta 1 Mbps, mientras que, simultáneamente, la línea permanece libre para una conversación telefónica normal. Las líneas *ADSL* requieren *módems ADSL* dedicados en ambos extremos de la línea local.

Almacén de información

Base de datos diseñada para prestar asistencia a la toma de decisiones en una organización y que puede contener enormes cantidades de datos. Por ejemplo, las grandes organizaciones minoristas pueden tener 100 GB o más de historial de transacciones. Cuando la base de datos está organizada para un departamento o una función, se puede llamar "mercado de datos" ("data mart") en lugar de *"almacén de información"*.

Autentificación

Verificación de la identidad de un usuario que se conecta a un sistema informático o verificación de la *integridad* de un mensaje transmitido.

Buzonfia ("spam")

Envío de grandes cantidades de publicidad no solicitada a través del correo electrónico.

Caché web

Sistema informático de una red que guarda, en su memoria o en disco, copias de las páginas web que se han solicitado más recientemente, para agilizar su recuperación. Si la siguiente página que se solicita ya se ha almacenado en la caché, se recupera localmente y no desde Internet. Los servidores de *caché web* están situados en el lado interior del *cortafuegos* de la empresa y permiten que las páginas más solicitadas estén disponibles instantáneamente. Dado que el contenido de las páginas web puede variar, los programas que gestionan la memoria de almacenamiento temporal revisan sin cesar si hay nuevas versiones de la página y las descargan. Tras un período determinado de inactividad, las páginas se borran de la caché.

Certificado electrónico

Un *certificado electrónico* es un documento electrónico que contiene dos grupos de información y que se considera una prueba de identidad en el mundo electrónico. El primer grupo de información es el propio certificado de información, que incluye el nombre o el seudónimo de la persona física o jurídica que solicita el certificado, su clave pública, las fechas de validez del certificado y el nombre la autoridad certificadora. El segundo grupo es la *firma digital* de la autoridad certificadora.

Todo el mensaje tiene la *firma digital* de una autoridad certificadora, que goza de la confianza de numerosos servidores (las autoridades certificadoras son un tipo especial de *terceros de confianza)* y puede verificar la relación entre la persona física o jurídica y su clave pública.

Cookies

Las *cookies* son datos que crea un servidor web y pueden almacenarse en ficheros de texto en el disco duro del usuario de Internet, y de los que el sitio web puede conservar una copia. Forman parte del tráfico HTTP, por lo que se pueden transportar sin problemas con el tráfico IP. Una *cookie* puede contener un número único (identificador global único - GUID, "Global Unique Identifier") que permite realizar una mejor identificación que las direcciones IP dinámicas y proporciona al sitio web una forma de rastrear las pautas de comportamiento y las preferencias del usuario.

Las *cookies* contienen una gama de URL (direcciones) para los que son válidas. Cuando el navegador vuelve a encontrar estos URL envía esas *cookies* específicas al servidor web.

Existen diferentes tipos de *cookie*s: pueden ser duraderas o, como es el caso de las denominadas *cookies* de sesión, tener una duración limitada.

Se puede hacer que el ordenador desactive las *cookies* o que avise al usuario antes de aceptar una.

Correo web

Sistemas de correo electrónico que utilizan páginas web como interfaz (por ejemplo, Yahoo, HotMail, etc.). Al *correo web* se puede acceder desde cualquier sitio y el usuario no necesita conectarse a un *proveedor de servicios de Internet* concreto como cuando utiliza una cuenta normal de correo electrónico.

Cortafuegos

Es un método para garantizar la seguridad de una red. Se puede implementar en un *encaminador* único que filtra los paquetes indeseados, o puede hacer uso de una combinación de tecnologías de *encaminadores* y ordenadores centrales. Los *cortafuegos* se utilizan a menudo para proporcionar a los usuarios un acceso seguro a Internet, así como para separar el servidor web público de una empresa de su red interna. También se usan para mantener seguros segmentos de la red interna; por ejemplo, para proteger una subred de búsqueda o contabilidad que podría ser accesible a usuarios internos indiscretos de otros departamentos.

Encaminador

Un *encaminador* es un dispositivo que proporciona rutas a las *redes TCP/I*P, lo que significa que la ruta TCP/IP es

dinámica, y depende de los fallos o la sobrecarga de ciertas rutas o vínculos. También se puede utilizar como un *corta-fuegos* entre un organismo e Internet y garantiza que de un *proveedor de servicios de Internet* determinado sólo puedan proceder direcciones IP autorizadas.

Encriptación

Codificación de información y mensajes de forma que, en principio, no pueda leerlos nadie aparte del destinatario previsto, que dispone de la clave o contraseña. Existen dos tipos principales de sistemas de *encriptación*: - El sistema simétrico o de clave privada, que utiliza una clave secreta compartida por el emisor y el destinatario de un mensaje. Su principal ventaja es la velocidad de tratamiento y su principal inconveniente es la dificultad de compartir claves seguras con un gran número de usuarios.

- El sistema asimétrico o de clave pública, que utiliza un par de claves, generadas de forma que, incluso sabiendo una de ellas, es prácticamente imposible adivinar la otra.

Los mensajes encriptados con una de las claves se desencriptan con la otra. Una de las claves se hace pública y se usa para encriptar los mensajes que cada usuario desencripta con su clave privada secreta. La clave privada se usa también para firmar mensajes digitalmente.

Firma digital

Una *firma digital* es una cadena de datos que se añade a un mensaje y garantiza su *integridad* encriptándolo (o encriptando un resumen del mensaje) con la clave privada del firmante. Cualquiera que reciba el mensaje firmado puede comprobar si ha sido modificado simplemente desencriptando la firma con la clave pública del emisor y comparando la cadena desencriptada con el mensaje original o su resumen.

Firma electrónica

Datos electrónicos adjuntos o asociados lógicamente a otros datos electrónicos que sirven como método de *autentificación* (apartado 1 del artículo 2 de la Directiva sobre *firmas electrónica*s).

Hipervínculo

Un vínculo predefinido entre dos objetos. El vínculo se muestra como texto o como un icono. En las páginas web, un *hipervínculo* de texto se muestra como texto subrayado, normalmente en azul, mientras que un *hipervínculo* gráfico es una pequeña imagen.

Husmeo

Los programas de *husmeo* pueden leer todos los paquetes de datos de una red y presentar en texto claro toda comunicación no encriptada. La forma más sencilla de *husmeo* se puede realizar utilizando un ordenador personal normal conectado a una red, con programas que se pueden encontrar fácilmente.

Identificación de la línea de llamada (CLI)

Cuando se realiza una llamada, la CLI permite al usuario que la recibe identificar al usuario que lo llama mostrando el número de la línea de llamada.

Integridad de los datos

Proceso con el que se evita la destrucción o la adulteración accidental de una base de datos.

Java y JavaScript

Java es un lenguaje de programación que no puede ser utilizado por el programador ocasional, ni mucho menos por el usuario. *JavaScript* es un lenguaje de scripts que utiliza una sintaxis similar a *Jav*a, pero que no está compilado en un código de bytes.

Permanece en código fuente incrustado en un documento HTML y el intérprete de *JavaScript* lo tiene que traducir línea por línea a código de máquina. El *JavaScript* está muy extendido y lo aceptan todos los navegadores de la Web. Su alcance es más limitado que el de *Jav*a, y principalmente se aplica a los elementos de la propia página.

Metaetiquetas

Las *metaetiquetas* son etiquetas HTML que proporcionan información sobre una página web. Al contrario que las etiquetas HTML normales, las *metaetiquetas* no afectan al modo en que se muestra la página, sino que dan información sobre su creador, la frecuencia de las actualizaciones, el tema que trata y las palabras clave que representan el contenido de la página. Muchos motores de búsqueda utilizan esta información al establecer sus índices.

Minería de datos

Implica "excavar toneladas de datos" para descubrir patrones y relaciones contenidos en la actividad y el pasado de la empresa. Normalmente se realiza con programas que analizan los datos automáticamente.

Módem

(MOdulador-DEModulador) Aparato que adapta un terminal u ordenador a una línea de teléfono analógica convirtiendo cada señal digital en frecuencias de audio y viceversa.

Normalmente, el término se refiere a *módems* de 56 kbps (V.90), la máxima velocidad actual, o a *módems* más antiguos de 28,8 kbps (V.34), aunque también se puede aplicar a *módems* de velocidad superior, a *módems* de línea de suscripción digital, o a adaptadores de terminal RDSI, todos ellos digitales y no *módems* técnicamente. Un *módem* es un convertidor analógico-digital y digital-analógico que también puede conectar con la línea, responder la llamada y controlar la velocidad de transmisión. Los *módems* han evolucionado de 300, 1 200, 2 400, 9 600, 14 400, 28 800 y 33 300 a 56 000 bps.

Cualquiera que sea su velocidad máxima, el *módem* siempre es capaz de funcionar a ciertas velocidades inferiores para poder acomodarse a *módems* más antiguos o adaptarse a una velocidad inferior en caso de líneas telefónicas de menor calidad.

OLAP

"On Line Analytical Processing" (tratamiento analítico en línea). Software de apoyo para la toma de decisiones que permite al usuario analizar rápidamente información resumida en jerarquías y vistas multidimensionales. Por ejemplo, las herramientas de *OLAP* se utilizan para analizar tendencias de ventas e información financiera. Permiten que los usuarios exploren grandes cantidades de estadísticas para aislar los productos más volátiles. Los productos *OLAP* tradicionales, también conocidos como *OLAP* multidimensional o MOLAP, resumen transacciones en vistas multidimensionales preparadas de antemano. Las consultas de los usuarios a este tipo de bases de datos son extremadamente rápidas, pues la consolidación ya se ha realizado. El *OLAP* coloca los datos en una estructura cúbica que el usuario puede girar, lo que resulta especialmente indicado para análisis financieros.

Pancarta

Las *pancartas* publicitarias son pequeños cuadros gráficos que aparecen sobre el contenido del sitio web o están integrados en él.

Portal

Los *portales* proporcionan una vista general de los vínculos web de una manera ordenada. Pasando por un *portal*, el usuario de Internet puede visitar fácilmente otros sitios web seleccionados de otros proveedores de contenidos.

Los *portales* modernos son "supersitios" que ofrecen una serie de servicios tales como búsqueda en la Web, noticias, guías de páginas blancas y amarillas, correo electrónico gratuito, grupos de debate, compras en línea y vínculos con otros sitios.

Protocolo

En este contexto, un *protocolo* es una serie de normas técnicas que han de observar los dos participantes en un intercambio de información. Los *protocolos* están organizados en una jerarquía de lo que se denomina capas. Cada capa se encarga de manejar un aspecto particular del proceso de las telecomunicaciones y ofrece funciones básicas que utilizarán las capas superiores. Tradicionalmente, en Internet el *protocolo* TCP/IP se utiliza siempre como una capa intermedia. Ethernet (utilizado en redes locales), *ADSL* (usado en las líneas telefónicas), ATM (modo de transferencia asíncrona, usado por los operadores de telecomunicaciones), X-75 (usado en líneas RDSI) y PPP *(protocolo de punto a*

*punt*o, usado en líneas telefónicas normales) son ejemplos de *protocolos* de nivel inferior.

En el otro extremo, HTTP (para navegar), SMTP *(protocolo* simple de transferencia de correo, para el correo electrónico), POP *(protocolo* de oficina de correo, también para el correo electrónico) y FTP (para transferir ficheros) son *protocolos* de nivel superior. Esto significa que cualquier amenaza potencial a la privacidad del *protocolo* TCP/IP será una de las debilidades de los *protocolos* superiores. Básicamente, las capas son una serie de subprogramas instalados en un ordenador conectado a Internet.

Protocolo de configuración dinámica del host (DHCP)

El *protocolo de configuración dinámica del host* (DHCP) es un *protocolo* de Internet para automatizar la configuración de los ordenadores que utilizan TCP/IP. El DHCP se puede utilizar para asignar automáticamente direcciones IP (http://www.dhcp.org).

Protocolo de punto a punto

El *protocolo de punto a punto* es un *protocolo* de telecomunicación muy utilizado para conectar dos ordenadores a través de su puerto serie o un *módem* conectado en él.

Es el *protocolo* de capa inferior más usado entre el ordenador personal de un usuario privado y el servidor de acceso a Internet de un *proveedor de servicios de Internet* cuando se establece una conexión TCP/IP con líneas telefónicas clásicas.

Proveedor de servicios de Internet

Empresa que proporciona acceso y conexiones a Internet a particulares y empresas.

Los pequeños *proveedores de servicios de Internet* proporcionan el servicio mediante *módems* y RDSI, mientras que los mayores ofrecen también conexiones de línea privada.

Generalmente, los consumidores pagan un precio fijo al mes, pero a éste se pueden sumar otros costes. Pagando una cuota se puede crear y mantener un sitio web en el servidor del *proveedor de servicios de Interne*t, lo que permite a una organización pequeña estar presente en la Web con su propio nombre de dominio.

Los grandes *proveedores de servicios de Internet* también ofrecen bases de datos privadas, foros y otros servicios.

En este informe, el término *proveedor de servicios de Internet* incluye normalmente a los proveedores de acceso a Internet, término que únicamente se utiliza cuando es obvio que sólo se habla del acceso a Internet.

En el resto de los casos se habla de *proveedor de*

servicios de Internet.

Red TCP/IP

Las *redes TCP/IP (protocolo* de control de transporte/*protocolo* de Internet) se basan en la transmisión de paquetes pequeños de información, cada uno de los cuales contiene la dirección IP del emisor y del destinatario.

Estas redes funcionan sin conexiones, lo que significa que, al contrario de lo que sucede con la red telefónica, por ejemplo, no es necesaria una conexión previa entre dos dispositivos para iniciar la comunicación. Esto permite igualmente mantener diversas comunicaciones con interlocutores distintos de forma simultánea.

Series de clics

Información derivada del comportamiento de un individuo, su recorrido o las elecciones que ha realizado durante su visita a un sitio web. Contienen los vínculos que un usuario ha seguido y están almacenados en el servidor web (el ordenador del *proveedor de servicios de Interne* t, en el caso de los usuarios que no tengan un servidor web propio).

Servidor proxy

El *servidor proxy* es un servidor intermediario entre el usuario de Internet y la Red.

Actúa como una *caché web* y mejora de una forma espectacular el funcionamiento de Internet. Muchas grandes organizaciones o proveedores de acceso a Internet ya han aplicado esta solución. Cada página, imagen o logotipo descargado desde el exterior por un miembro de una organización se almacena en una caché en el *servidor proxy* y queda automáticamente disponible para los otros miembros de la misma organización.

Ya no es necesario que cada miembro de la organización situado antes del *servidor proxy* tenga su propia dirección IP, pues no accede directamente a Internet.

Sistema de nombres de dominio (DNS)

El DNS *(sistema de nombres de dominio)* es un mecanismo para asignar nombres a ordenadores identificados con una dirección IP. Estos nombres adoptan la forma <nombre>.dominio de nivel superior, donde <nombre> es una cadena formada por una o varias subcadenas separadas por un punto.

Software compartido

Software que se puede descargar de Internet. Normalmente, se puede descargar de forma gratuita para probarlo, pero para que su uso sea legal posteriormente se ha de pagar por él. Los programas que se pueden descargar y usar completamente gratis se conocen con el nombre *software gratuito*.

Terceros de confianza

Un *tercero de confianza* se puede describir como una entidad a la que otras entidades confían sus actividades y servicios relacionados con la seguridad.

Un *tercero de confianza* ofrecerá servicios de valor añadido a los usuarios que deseen aumentar la seguridad y la confianza de los servicios que reciben y facilitar la realización de comunicaciones seguras con sus socios empresariales. Los *terceros de confianza* han de demostrar un alto nivel de *integrida*d, confidencialidad y garantía en los resultados de los servicios y la información necesarios para las comunicaciones entre aplicaciones comerciales. Por otra parte, los usuarios requerirán los servicios de los *terceros de confianza* cuando los necesiten, en el marco de un contrato de prestación de servicios.

Normalmente, un *tercero de confianza* será una organización que ha obtenido una licencia o acreditación de una autoridad reguladora y que, partiendo de una base comercial, presta servicios de seguridad a una amplia gama de órganos, incluidos los de los sectores de las telecomunicaciones, las finanzas y el comercio minorista.

Por ejemplo, se podría recurrir a un *tercero de confianza* para garantizar la asignación de *firmas digitales* que garanticen la *integridad* de los documentos. Además, pueden ofrecer servicios de *encriptación* de extremo a extremo a los usuarios y proponer, por ejemplo, funciones de almacenamiento o recuperación de claves para recuperar ficheros en caso de pérdida de la clave de *encriptación* (normalmente, en caso de documentos o archivos encriptados por empleados) o como apoyo en peticiones de interceptación legal.

El recurso a *terceros de confianza* está sujeto fundamentalmente a la confianza que tengan en él las entidades a las que prestan servicios.

UMTS

El *UMTS* (sistema universal de telecomunicaciones móviles) es un *protocolo* de banda ancha de "tercera generación" de transmisión en paquetes e inalámbrico, que ofrecerá una velocidad de transmisión superior a 2 Mbps. Este nuevo *protocolo* de banda ancha permitirá la transmisión de señales digitales de vídeo a aparatos portátiles con la misma calidad que en la televisión. Actualmente, la red GSM permite velocidades en torno a los 11 kbps, suficientes para transmitir señales sonoras pero no imágenes en movimiento 222 .

WAP

El *WAP (protocolo* de aplicación inalámbrica) es un *protocolo* de telecomunicaciones diseñado entre diversos fabricantes de teléfonos móviles. Permite el acceso a servicios de Internet como el correo, la charla electrónica o la navegación por la Web, desde un teléfono móvil especializado 223 .

NOTAS:

1 En particular: Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles abierta (OPS), adoptado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 16 de junio de 1998; Documento de trabajo: Tratamiento de datos personales en Internet, aprobado por el Grupo de Trabajo el 23 de febrero de 1999, WP 16, 5013/99/ES/final; Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardwar*e, adoptado por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17; Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18; Dictamen nº3/99 relativo a información del sector público y protección de datos personales, aprobado por el Grupo de Trabajo el 3 de mayo de 1999;
Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicios de Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999, 5085/99/ES/final, WP 25; Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, 5007/00/ES/final, WP 28; WP 29: Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, WP 29, 5009/00/ES/final; Dictamen 5/2000 sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multicriterio (guías inversas), WP 33, adoptado el 13 de julio de 2000, y Dictamen 7/2000 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de julio de 2000, COM (2000) 385, adoptado el 2 de noviembre de 2000, WP 36.
2 Así se ha señalado en un estudio semestral recientemente publicado por la Fundación Markle. Véase el artículo de AARON, D., *A Euro-American proposal for privacy on the Net,* Washington Post, 2 de agosto de 2000.
3 Los aspectos técnicos descritos en este trabajo se han simplificado enormemente para que los comprendan los profanos en la materia. Para más detalles, véase: *Comunicación de la Comisión al Consejo y al Parlamento Europeo, La organización y gestión de Internet,* Cuestiones de política europea e internacional 1998 - 2000 COM (2000) 202 final, 11 de abril de 2000.
4 Véase la sentencia Reno contra ACLU de 26 de junio de 1997, Tribunal Supremo de los Estados Unidos, disponible en: www2.epic.org/cda/cda_decision.html.
5 Véase la sentencia Reno contra ACLU de 26 de junio de 1997.
6 Actualmente se está desarrollando la versión mejorada (Ipv6) del sistema de direccionamiento IP sobre la base de números de 128 bits de longitud.
7 La Corporación Internet para la asignación de nombres y números (ICANN) es un organismo sin ánimo de lucro fundado para asumir la responsabilidad de la asignación de espacio de dirección IP (http://www.icann.org). En Europa, el espacio de direccionamiento está gestionado por la organización RIPE (Réseaux IP Européens) (http://www.ripe.net).

Para más detalles sobre la evolución del proceso de los nombres de dominio de Internet, véase la Comunicación de la Comisión mencionada en la nota al pie 3.
8 El *Protocolo de configuración dinámica del host* (DHCP) es un *protocolo* de Internet destinado a automatizar la configuración de los ordenadores que usan el TCP/IP. El DHCP puede utilizarse para asignar automáticamente direcciones IP (http://www.dhcp.org).
9 El tiempo de tratamiento y almacenamiento de estos datos está sujeto a condiciones jurídicas estrictas, como se explica más adelante.
10 Una pequeña empresa también puede firmar un contrato de estas características, pero tales casos no se tendrán en cuenta en este documento.
11 Este documento no se referirá a los *proveedores de servicios de Internet* como proveedores de contenidos, aunque algunos de ellos los ofrezcan en determinadas circunstancias (por ejemplo, en el caso de los *proveedores de servicios de Internet* que tienen su propio *porta*l).
12 Se puede consultar una descripción pormenorizada de estos servicios en la sentencia Reno contra ACLU de 26 de junio de 1997.
13 La Comisión Nacional de la Informática y de las Libertades (CNIL) francesa cuenta en su sitio web con una sección llamada "Sus huellas" en la que los usuarios de Internet pueden visualizar las huellas que han dejado tras de sí al utilizar Internet. Esta sección se encuentra disponible en francés, inglés y español. Véase www.cnil.fr
14 Para más detalles sobre esta cuestión, véase el capítulo 2.
15 Véase DINANT, Jean-Marc, Law and Technology Convergence in the Data Protection Field? *Electronic threats to personal data and electronic data protection on the Internet,* Proyecto ESPRIT 27028, "Electronic Commerce Legal Issues Platform".
16 Véase el libro de HAGEL III, J. y SINGER, M., *Net Worth: the emerging role of the informediary in the race for customer information,* Harvard Business School Press, 1999, p. 275.
17 Técnicamente hablando, también es posible implementar *cookies* en *JavaScript* o en los campos <META-HTTP EQUIV> ubicados en el código HTML.
18 Las *cookies* sin duración fija se llaman *"cookies* de sesión" y desaparecen cuando el navegador o la conexión se cierran.
19 GAUTHRONET, Serge , "On-line services and data protection and the protection of privacy", Comisión Europea, 1998, pp. 31 y 92, disponible en: http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm
20 Sólo con DoubleClick, unos 26 millones de usuarios de Internet en marzo de 1997 (GAUTHRONET, *op. ci*t., p. 86) y más de un millardo de *pancartas* publicitarias descargadas cada mes fuera de los Estados Unidos *(ibid*., p. 96). En la actualidad, cada día se envían más de 500 000 000 *pancartas* publicitarias por empresa de cibermarketing. Véase http://www.doubleclick.net/company_info/investor_relations/financials/analyst_metrics.htm.
21 El *World Wide Web Consortium* (W3C) es una organización sin ánimo de lucro albergada por el Inria (Francia), el Instituto tecnológico de Massachusetts (EE.UU.) y la Universidad de Keio (Japón). Entre sus miembros destacan Microsoft, AOL, Netscape y el "Center for Democracy and Technology". (http://www.w3.org/Consortium/Member/List). El W3C genera normas no vinculantes pero aplicables de hecho destinadas a garantizar la interoperabilidad de los ordenadores en Internet.
22 http://www.w3.org/Protocols/rfc2068/rfc2068. La paginación entre corchetes corresponde a la del *W3*C.
23 El campo de cabecera "From" se utiliza para designar la página remitente.
24 La palabra "privacidad" aparece 18 veces en el RFC 2068.
25 Véase la sentencia Reno contra ACLU de 26 de junio de 1997. 26 Comunicado de prensa de la Comisión Europea, *Commission welcomes new legal framework to guarantee security of electronic signatures,* 30 de noviembre de 1999.
27 Véase el libro *Net Worth (op. cit.*), página xiii (prefacio).
28 Citado de M. HALPERN y HARMON, *E-mergers trigger privacy worries* de Deborah KONG, http://www.mercurycenter.com/svtech/news/indepth/docs/consum012400.htm.
29 http://www.truste.org/users/users_investigations.html.
30 Véase, por ejemplo, el debate sobre los informediarios en el capítulo 9.
31 Véase WP 16, Documento de trabajo: *Tratamiento de datos personales en Interne*t, aprobado por el Grupo de Trabajo el 23 de febrero de 1999, 5013/99/ES/final.
32 Véase también el considerando 26 del preámbulo de la Directiva.
33 En este documento, la expresión "la Directiva" se referirá a la Directiva 95/46/CE.
34 Véase el considerando 11 de la Directiva 97/66/CE.
35 En principio, el término *proveedor de servicios de Interne*t, tal y como se emplea en este documento, se refiere también a los proveedores de acceso a Internet (véase la definición en el glosario). Este documento sólo se referirá a proveedores de acceso a Internet cuando aborde cuestiones que se refieran exclusivamente a ellos.
36 En la página 275 del libro *Net Worth (op. cit.)* se menciona: "Dado que las *cookies* se pueden utilizar también para relacionar hábitos y preferencias de navegación, se está extendiendo su uso para dirigir los anuncios a usuarios específicos. Doubleclick, Globaltrash y ADSmart son ejemplos de empresas que utilizan *cookies* para adaptar los anuncios a los consumidores en los sitios web programados".
37 Documento COM (1999) 539.
38 Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, WP 29, 5009/00/ES/final. 39 Documento COM (2000) 385.
40 La Comisión propone una revisión de la normativa sobre comunicación electrónica, Bruselas, 12 de julio de 2000, IP/00/749.
41 COM (2000) 393.
42 Esta cuestión no se estudia en este documento.
43 Asunto C-109/92 Wirth [1993] Rec I-6447, 15. 44 Directiva 1999/93/CE de 13 de diciembre de 1999, por la que se establece un marco comunitario para la *firma electrónic*a, Diario Oficial de las Comunidades Europeas, 19 de enero de 2000, L 13/12 a 13/20.
45 Directiva 1997/7/CE de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a

distancia, Diario Oficial de las Comunidades Europeas, 4 de junio de 1997, L 144.
46 Directiva 2000/31/CE de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), Diario Oficial de las Comunidades Europeas, 17 de julio de 2000, L 178/1 a 178/16.
47 El operador de telecomunicaciones no participa específicamente en el proceso de envío de correo electrónico, pero desempeña un papel fundamental en la transmisión de señales que hace posible toda forma de comunicación por correo electrónico. Este agente tiene obligaciones específicas relativas a la seguridad establecidas por las Directivas.
48 La autoridad francesa en materia de protección de datos, conocida como CNIL, ha realizado otras investigaciones sobre la *buzonfia* y la recopilación de direcciones de correo electrónico. Véase, en particular, el informe de la CNIL sobre correo electrónico y protección de datos del 14 de octubre de 1999, disponible en el sitio web de la CNIL: www.cnil.fr.
49 Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999, 5085/99/ES/final, WP 25.
50 Para más información, consúltese la Comisión de Libertades y Derechos de los Ciudadanos, Justicia y Asuntos Interiores del Parlamento Europeo: http://www.europarl.eu.int/committees/es/default.htm. Véase también EPIC, Alert 7.07, 20 de abril de 2000.
51 Informe sobre las capacidades de interceptación en 2000, mayo de 1999.
52 Agencia nacional de seguridad, Estados Unidos.
53 Centro gubernamental de comunicaciones, homólogo británico de la NSA.
54 EPIC Alert 7.15, 3 de agosto de 2000.
55 El texto del proyecto se encuentra a disposición del público en: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.
56 Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18.
57 Conviene destacar que las garantías fundamentales reconocidas por el Consejo de Europa en relación con la interceptación de telecomunicaciones establecen obligaciones para los Estados miembros independientemente de las distinciones hechas en la Unión Europea de acuerdo con la naturaleza comunitaria o intergubernamental de los campos abordados.
58 El Convenio n§ 108 del Consejo de Europa estipula igualmente que la interceptación sólo puede permitirse cuando en una sociedad democrática resulta necesaria para la protección de los intereses nacionales enumerados en el apartado segundo del artículo 9 de dicho Convenio y está estrictamente definida en función de esta finalidad.
59 Véase el informe de la CNIL sobre correo electrónico y protección de datos, 14 de octubre de 1999.
60 Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, 5007/00/ES/final, WP 28.
61 Artículo 10 de la Directiva 95/46/CE.
62 Artículo 14 de la Directiva 95/46/CE.
63 En él se requiere (uno de los posibles fundamentos legítimos del tratamiento) que el tratamiento de datos sea "necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento... siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado".
64 El operador de telecomunicaciones cuando el abonado utiliza un *módem*. En otro caso, si el usuario emplea una línea arrendada, aunque el coste no aumente inmediatamente a causa del mensaje de *spam* (tarifa plana*),* desde un punto de vista macroeconómico resulta evidente que los costes indirectos del tráfico relacionados con la *buzonfia* masiva se cargan al *proveedor de servicios de Interne*t, con las consecuencias que esto conlleva para los precios de las líneas arrendadas.
65 Véase la página 3 del libro *Net Worth (op. cit.*).
66 Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la *firma electrónic* a, Diario Oficial de las Comunidades Europeas, 19 de enero de 2000, L 13/12 a 13/20.
67 Para más detalles, véase el capítulo 9, sobre medidas en favor de la privacidad.
68 Véanse las páginas 275 y siguientes del libro *Net Worth (op. cit.*),.
69 Este documento se refiere también a este tipo de servicio en el apartado V del capítulo 6 (publicaciones y foros), relativo a las medidas sobre protección de la intimidad.
70 Para más detalles, véase el capítulo 6.
71 Este principio se desarrolla en mayor medida en la Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardwar*e, adoptada por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17.
72 Véase también la Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada por el Grupo de Trabajo el 7 de septiembre de 1999.
73 Véase, en este contexto, la Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18.
74 A veces, un mismo usuario utiliza direcciones IP estáticas durante un largo período de tiempo. Este tipo de direcciones IP se suelen emplear cuando se utilizan tecnologías alternativas de acceso (líneas *ADS*L, televisión por cable, telefonía móvil). Al generalizarse estas tecnologías se está observando un aumento relativo de la utilización de direcciones IP estáticas.
75 En algunos casos, también otras partes, tales como universidades, organizaciones o empresas, pueden desempeñar el papel de *proveedores de servicios de Interne* t.
76 Hasta cierto punto, las direcciones IP también se asignan con criterios geográficos.
77 Para más detalles, véase el capítulo 2.
78 En este caso nos referimos a las *cookies* permanentes, es decir, a las que permanecen más de una sesión.
79 Véase el informe de la Registratiekamer (ARTZ, M.J.T. y VAN EIJK, M.M.M.), *Klant in het web: Privacywaarborgen voor Internettoegang,* Achtergrondstudies en verkenningen, 17 de junio de 2000, disponible en: www.registratiekamer.nl.

Este informe subraya que casi todos los proveedores de acceso a Internet de los Países Bajos poseen su propia página de inicio, que también se utiliza como *portal* para iniciar la navegación.
80 En este contexto cabe mencionar la posición común sobre los motores de búsqueda adoptada por el Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones en la reunión celebrada en Hong Kong el 15 de abril de 1998, disponible en: http://www.datenschutz-berlin. de/doc/int/iwgdpt/pr_en.htm.
81 El Grupo de Trabajo del artículo 29 ya abordó esta cuestión en su Recomendación 1/99, adoptada el 23 de febrero de 1999: Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardwar*e, adoptada por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17.
82 Véase EPIC Alert 6.10, 30 de junio de 1999. La misma preocupación surgió ya durante el caso de Harriet M. Judnick contra DoubleClick en el Tribunal Superior del Estado de California.
83 www.doubleclick.net:8080/privacy_policy/ Esta fusión se analiza en detalle en el capítulo 7 sobre transacciones electrónicas en Internet.
84 Véase el tema de portada de la revista Time del 31 de julio de 2000, de COHEN, Adam: *Cómo proteger tu intimidad: ¨quién te observa? Se llaman programas E.T. Te espían y "llaman a casa" para contarlo. Millones de personas los descargan de forma involuntaria.*
85 http://www.narus.com.
86 Véase PALTRIDGE, Sam, *Mining and Mapping Web Conten*t, en: Inf*o, The Journal of policy, regulation and strategy for telecommunications, information and medi* a, vol. 1, n§ 4, agosto de 1999, pp. 327-342.
87 http://www.alexa.com.
88 Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.*). 89 Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.*).
90 Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.*).
91 Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.*).
92 Véase WP 16, Documento de trabajo: *Tratamiento de datos personales en Interne*t, aprobado por el Grupo de Trabajo el 23 de febrero de 1999, 5013/99/ES/final.
93 Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardwar*e, adoptado por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17.
94 La información debería incluir, al menos, detalles sobre el responsable del tratamiento, los fines del mismo y, si procede, el derecho a oponerse a él.
95 Estudio *"Surfer Beware III: Privacy Policies Without Privacy Protectio*n", véase EPIC Alert 7.01, 12 de enero de 2000. Disponible en: www.epic.org/reports/surfer-beware.html.
96 En EE.UU., las Prácticas leales de información sirven como directrices básicas para proteger la información personal.
97 *Klant in het web: Privacywaarborgen voor Internettoegang (op. cit.).*
98 Véase el capítulo 9.
99 Véase PALTRIGDE, S., *Search engines and content demand,* in *Mining and Mapping Web Conten*t, en: *Info, The Journal of policy, regulation and strategy for telecommunications, information and medi*a, vol. 1, n§ 4, agosto de 1999, pp. 330-333.
100 COM (2000) 385.
101 "Llamada" se referirá a una conexión establecida por medio de un servicio telefónico disponible al público que permita la comunicación bidireccional en tiempo real.
102 A este respecto, véase la Recomendación 2/99 sobre la protección de la intimidad en el contexto de la intercepta-ción de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18.
103 Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999, 5085/99/ES/final WP 25.
104 Véase el Dictamen 7/2000 del Grupo de Trabajo, adoptado el 2 de noviembre de 2000, WP 36.
105 Para más detalles, véase el capítulo 9 sobre medidas en favor de la privacidad.
106 EPIC Alert 7.14, 27 de julio de 2000.
107 Para más detalles, véase el libro *Net Worth (op. cit.*).
108 Así lo sugirió Cheswick, investigador jefe de Lucent technologies, en el artículo de COHEN, A., en la revista Time *(op. cit.*).
109 La Agencia Española de Protección de Datos ha tratado esta cuestión en su documento "Recomendaciones a los usuarios de Internet", disponible en español e inglés en su sitio web: www.agenciaprotecciondatos.org.
110 Es frecuente que la primera parte de una dirección de correo electrónico coincida con el nombre del usuario, sobre todo cuando ha sido definida automáticamente por un proveedor de acceso a Internet a partir de su nombre registrado. Sin embargo, por lo general el usuario puede modificar esa parte de la dirección y utilizar, por ejemplo, un seudónimo. También se puede solicitar una segunda dirección; en este caso el proveedor de acceso permitirá al usuario elegir un nombre.
111 Tal vez para impedir que la responsabilidad recaiga en el proveedor de servicios responsable del foro.
112 Recomendación 3/97 sobre anonimato en Internet, adoptada por el Grupo de Trabajo el 3 de diciembre de 1997.
113 Véase, por ejemplo, el sitio Internet de Deja: "http://www.deja.com/home_ps.shtml?", que ofrece una "potente herramienta de búsqueda" con varios criterios de búsqueda, incluido el autor de mensajes en foros de debate. El sitio afirma que dispone de la mayor base de datos de la red sobre aportaciones a foros de debate.
114 Con relación a este tema, véase la aportación del Sr. Marcel PINET, miembro de la CNIL, en la Conferencia internacional sobre protección de datos, celebrada en Santiago de Compostela en septiembre de 1998, disponible en: www.cnil.fr, en el apartado Internet, Initiatives.
115 El *almacenamiento* y la *minería de datos* implican "excavar en toneladas de datos" para descubrir modelos y relaciones existentes, por ejemplo, en la historia y la actividad comercial de una organización. Se considera que el almacenamiento de datos debe prestar apoyo a la toma de decisiones. El tratamiento de la ingente cantidad de información se realiza con ayuda de software que permite una conexión sencilla entre informaciones relacionadas de la base datos. Véase el informe de la Registratiekamer (BORKING, J., ARTZ, M. y VAN ALMELO, L.), *Gouden bergen van gegevens:*

over datawarehousing, datamining en privacy, Achtergrondstudies en verkenningen 10 de septiembre de 1998, disponible en: www.registratiekamer.nl.
116 Dictamen nº3/99 relativo a información del sector público y protección de datos personales, aprobado por el Grupo de Trabajo el 3 de mayo de 1999.
117 Recomendación del Comité de Ministros a los Estados miembros adoptada el 23 de febrero de 1999. Disponible en: www.coe.int/dataprotection/.
118 S. LOUVEAUX, A. SALAÚN, Y. POULLET, *User protection in the cyberspace: some recommendation*s, CRID, p. 12, disponible en: http://www.droit.fundp.ac.be/crid/.
119 Recomendación adoptada por el Grupo de Trabajo el 3 de diciembre de 1997.
120 Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los *proveedores de servicio Internet* a efectos de cumplimiento de la legislación, aprobada por el Grupo de Trabajo el 7 de septiembre de 1999.
121 Dictamen nº3/99. Véase más arriba.
122 Esto podría resultar especialmente útil en lo que respecta a la difusión de guías en Internet. A menudo, las reclamaciones gestionadas por las autoridades de protección de datos se basan en la publicación de datos desde un determinado país cuando el afectado se ha registrado en una lista de oposición, pero sólo en su propio país.
123 Dictamen 5/2000 sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multicriterio (guías inversas), WP 33, adoptado el 13 de julio de 2000.
124 En su versión pública de 12 de julio de 2000, COM(2000) 385.
125 Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardwar*e, adoptado por el Grupo de Trabajo el 23 de febrero de 1999.
126 Los responsables del reenvío de primera generación se llaman Cipherpunk, mientras que los de segunda generación, que emplean técnicas más avanzadas, se denominan Mixmaster. Los servidores anónimos más famosos en la red eran "anon.penet.fi" o "alpha.c2.org". Sin embargo, parece que ninguno de los dos sigue operativo hoy en día. Uno nuevo es "Nym.alias.net". Los mensajes anónimos también pueden enviarse a través de un documento HTML. En este caso, el mensaje y el destinatario final se envían sin encriptar al servidor WWW utilizado.
127 Dictamen 3/99, véase más arriba.
128 El Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones había adoptado una recomendación similar sobre guías inversas en su reunión de Hong Kong de 15 de abril de 1998: *Aunque las guías inversas no están prohibidas por la ley, son servicios que requieren un consentimiento expreso y voluntario. Deberían garantizarse, al menos, el derecho de oposición y el derecho de acceso, generalmente reconocidos por las normativas vigentes, nacionales e internacionales, sobre protección de datos personales. En cualquier caso, se ha de garantizar a las personas el derecho a ser informadas por su proveedor de servicios de correo electrónico o de telefonía, en el momento de recabar sus datos o, si ya se han abonado, por medios de información específicos, de la existencia de servicios de búsqueda inversa y (si no se exige el consentimiento explícito) de su derecho a oponerse, de forma totalmente gratuita, a esta búsqueda.* El texto completo de esta recomendación se puede obtener en: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm.
129 Oficina de Proyectos de la Sociedad de la Información de la Comisión Europea, *Electronic Commerce -An Introduction* (http://www.ispo.cec.be/ecommerce/answers/introduction.html).
130 En la actualidad, la mayoría de las transacciones comerciales electrónicas (en torno al 90 %) se realizan entre empresas (es decir, entre personas jurídicas) que no están cubiertas por la Directiva 95/46/CE (véanse la letra a del artículo 2 y el apartado 1 del artículo 3).
131 La siguiente clasificación se ha tomado de un estudio realizado por la Comisión de las Comunidades Europeas *"On-line services and data protection and the protection of privacy*", disponible en http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf.
132 La forma en que se recoge esta información se explica con más detalle en el capítulo 5, "Navegación y búsqueda".
133 Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS), adoptado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 16 de junio de 1998. (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm). Véase también el libro de HAGEL III, J. y SINGER, M., *Net Worth: the emerging role of the informediary in the race for customer information*, Harvard Business School Press, 1999 y el informe *Intelligent software agents and privacy*, de J. BORKING, B.M.A. VAN ECK y P. SIEPEL, Registratiekamer en colaboración con el Comisario de información y privacidad de Ontario, Achtergrondstudies y verkenningen, enero de 1999, disponible en www.registratieakamer.nl.
134 Se puede consultar una descripción completa del sistema de capa de conexiones seguras en http://developer.netscape.com/tech/security/ssl/howitworks.html y http://home.netscape.com/eng/server/console/4.0/help/app_ssl.htm.
135 Utilizando el *protocolo* SET durante la transacción, las partes se comunican por medio de dos pares de claves de *encriptación* únicas y asimétricas: claves de *encriptación* públicas para firmar documentos relativos a la transacción (es decir, la oferta de compra) y claves privadas, entre las que se incluye la *firma electrónica* de la transacción real (es decir, la instrucción de pago), que garantizan la *integridad* de la transmisión y que la orden no sea revocada. El sistema funciona como una doble firma: ambas claves interactúan de tal forma que un pago no se puede validar a menos que la oferta de compra sea aceptada por el vendedor y la orden real no se paga hasta que la institución financiera ha dado su aprobación. El vendedor no conoce las instrucciones de pago y el banco no tiene acceso a los contenidos de la orden. Para obtener una descripción funcional del complejo *protocolo* SET, *véase SET Secure Electronic Transaction Specification Book 1.* En http://www.setco.org/download.html se puede consultar una descripción comercial. Véase también GARFINKEL, S., *Web security and commerce,* Oreilly associates, junio de 1997, capítulo 12: *Understanding SSL and TLS.*
136 Para acceder a un debate teórico sobre cómo funcionan estos sistemas, véase, CHAUM, David *"A Cryptographic Invention Known as a Blind Signature Permits Numbers to Serve as Electronic Cash or to Replace Conventional Identification. The Author Hopes It May Return Control of Personal Information to the Individual"* http://www.eff.org/pub/Privacy/chaum_privacy_id_Article, que se publicó en *Scientific American* en agosto de 1992.
137 Véase el informe de la Registratiekamer (BORKING, J., ARTZ, M. y VAN ALMELO, L.), *Gouden bergen van gegevens: over datawarehousing, datamining en privacy,* Achtergrondstudies en verkenningen, 10 de septiembre de 1998,

disponible en www.registratiekamer.nl.
138 Como se menciona en el estudio *On-line services and data protection and privacy,* de GAUTHRONET, S. y NATHAN, F., publicado por la Comisión de las Comunidades Europeas y disponible en http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf.
139 www.doubleclick.net:8080/privacy_policy/.
140 Harriet M. Judnick contra DoubleClick, Inc.
141 WATTERSON, Karen, *La minería de datos ya es una tendencia dominante*; DATAMATION (Edición española), febrero de 2000.
142 *Protocolo* de aplicación inalámbrica *(WA*P).
143 Jane Weaver, MS NBC, 16/04/2000.
144 Para más información, véase http://www.cellpt.com/v2/000504.htm.
145 Tratamiento de datos personales en Internet, documento de trabajo aprobado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 23 de febrero de 1999 (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm).
146 Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardwar*e, adoptado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 23 de febrero de 1999 (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm).
147 Letra b) del artículo 14 de la Directiva 95/46/CE.
148 Véase también el capítulo 6 en relación con el debate sobre el propósito del principio de especificación aplicado a datos disponibles públicamente.
149 Directiva 2000/31/CE de 8 de junio de 2000.
150 Véase http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm.
151 Respecto a este tema, véase también la declaración oficial, ya mencionada, que los Comisarios europeos de protección de datos formularon en Estocolmo, según la cual en los casos específicos en que se han de conservar datos sobre tráfico deberá existir una necesidad demostrable, el período de conservación deberá ser lo más breve posible y la práctica deberá estar claramente regulada por la ley.
152 Véase también el tercer párrafo de la letra a) del artículo 12 de la Directiva 95/46/CE.
153 Para más detalles, véase el capítulo 3.
154 Véase el apartado V, "Análisis de cuestiones especiales. Buzonfia", del capítulo 4, "Correo electrónico".
155 Véanse, en el capítulo 5, "Navegación y búsqueda", más detalles sobre los datos generados durante el proceso de navegación.
156 En este contexto es importante mencionar la posición común referente a los perfiles en línea de Internet, adoptada por el Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones en la 27ª reunión del Grupo de Trabajo, celebrada los días 4 y 5 de mayo del 2000 en Rethymnon / Creta. El texto de esta recomendación está disponible en: http://www.datenschutz-berlin. de/doc/int/iwgdpt/pr_en.htm.
157 Sólo será así cuando un sitio web ofrezca información suficiente al usuario sobre los datos tratados, el fin del tratamiento, la identidad del responsable del tratamiento, etc. Véase el artículo 10 de la Directiva.
158 Se pueden encontrar más detalles sobre las técnicas utilizadas por tales empresas publicitarias en el apartado "Riesgos para la privacidad" del capítulo 5, "Navegación y búsqueda", así como en el capítulo 7, "Transacciones electrónicas en Internet".
159 Las *pancartas* publicitarias son pequeños cuadros gráficos que aparecen sobre el contenido de un sitio web o integrados en él.
160 Conviene tener en cuenta que la definición de datos identificables de la letra a) del artículo 2 de la Directiva CE/95/46 es muy amplia: "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".
161 Véase el apartado I, "Cuestiones jurídicas generales: Datos personales en Internet", del capítulo 3, "Aplicación de la legislación relativa a la protección de datos".
162 Se pueden obtener más detalles sobre la recogida de direcciones de correo electrónico en el capítulo 4, relativo al correo electrónico.
163 Estas listas también pueden contener direcciones de correo electrónico recogidas de espacios públicos de Internet.
164 Véase el capítulo 6 acerca de publicaciones y foros.
165 Artículo 6 de la Directiva 95/46/CE.
166 Artículo 7 de la Directiva 95/46/CE.
167 Artículo 10 de la Directiva 95/46/CE. 168 Artículo 14 de la Directiva 95/46/CE. 169 Artículo 12 de la Directiva 95/46/CE.
170 Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia.
171 Artículo 10 de la Directiva 97/7/CE.
172 Apartado 2 del artículo 12 de la Directiva 97/66/CE.
173 Apartado 1 del artículo 12 de la Directiva 97/66/CE.
174 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
175 Artículo 7 de la Directiva 2000/31/CE.
176 Artículo 7 de la Directiva 2000/31/CE.
177 Artículo 4 de la Directiva 95/46/CE.
178 Artículo 12 de la Directiva 97/66/CE. Propuesta de Directiva relativa al tratamiento de los datos personales y a la protección de la privacidad en el sector de las telecomunicaciones, artículo 13 relativo a las comunicaciones comerciales no solicitadas.

179 Estas conclusiones se basan en la decisión alcanzada por la autoridad alemana de protección de datos relativa a un anunciante específico de la red. El Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones adoptó una posición común que también refleja esta decisión. Véase http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm.
180 Artículo 10 de la Directiva 95/46/CE.
181 Artículo 6 de la Directiva 95/46/CE.
182 Artículo 14 de la Directiva 95/46/CE.
183 Artículo 12 de la Directiva 95/46/CE.
184 Artículo 10 de la Directiva 95/46/CE.
185 Artículo 7 de la Directiva 2000/31/CE.
186 Artículo 7 de la Directiva 2000/31/CE.
187 Véase el Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, presentado por el Grupo operativo sobre Internet (WP 28).
188 Letra a) del primer apartado del artículo 6 de la Directiva 95/46/CE.
189 Letra b) del primer apartado del artículo 6 de la Directiva 95/46/CE.
190 Letra f) del artículo 7 de la Directiva 95/46/CE.
191 Véase el Dictamen 7/2000 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la privacidad en el sector de las comunicaciones electrónicas, de 12 de julio de 2000, COM (2000) 385, adoptado el 2 de noviembre de 2000, WP 36.
192 Véase el informe de HES, R. y BORKING, J. (editores), *Privacy-enhancing technologies: the path to anonymity (revised edition),* Registratiekamer, en colaboración con el Comisario de información y privacidad de Ontario, Achtergrondstudies en Verkenningen 11, La Haya, noviembre de 1998. Disponible en www.registratiekamer.nl.
193 Para obtener más detalles, véase el informe de la Registratiekamer sobre las tecnologías de protección de la privacidad *(op cit.*), y en particular sus páginas 7 y ss.
194 Véase también la guía EPIC en línea sobre herramientas prácticas de privacidad, disponible en www.epic.org/privacy/tools.html.
195 Las *cookies* sin duración fija no se almacenarán en el disco duro, sino sólo en la memoria RAM.
196 En MSIE 4.O UK, los avisos de *cookies* están redactados como sigue: *'¨Permite que este sitio web introduzca información en su ordenador para obtener una experiencia navegadora más personal? Si pulsa el "Sí", el sitio web guardará un fichero en su ordenador. Si pulsa el "No", la página web actual puede no mostrarse correctamente".* El usuario debe entonces pulsar otro botón para conocer el dominio (no el emisor) de la *cookie* y su duración.
197 EPIC Alert 7.14, 27 de julio de 2000.
198 Algunos de estos programas pueden encontrarse en http://tucows.belgium.eu.net/cookie95.html.
199 Lamentablemente, algunos *proxies* añaden a la cabecera HTTP la dirección TCP-IP del PC para el que están trabajando.
200 Véase el libro "Net Worth" *(op. cit.*), páginas 273 y ss.
201 http://www.anonymizer.com/3.0/index.shtml .
202 http://www.zeroknowledge.com.
203 http://www.iprivacy.com.
204 Véase el libro "Net Worth" *(op. cit.*), páginas 275 y ss.
205 Este tipo de servicios se comentan también en el apartado sobre medidas en favor de la privacidad del capítulo 6, "Publicaciones y foros".
206 http://www.fourthwavegroup.com/Publicx/1635w.htm.
207 Uno de los estudios más completos sobre este nuevo órgano es el libro *"Net Worth: the emerging role of the infomediary in the race for customer information* "; HAGEL III, J. y SINGER, M., Harvard Business School Press.
208 HAGEL III, J. y SINGER, M.*(op. cit*).
209 El último borrador de trabajo del *protocolo* P3P se puede consultar en el sitio web del W3C, en http://www.w3.org/TR/1999/WD-P3P.
210 Este texto está disponible en: http://www.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm.
211 Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS), adoptado el 16 de junio de 1998, WP 11, XV D/5032/98.
212 Véase el artículo de CAVOUKIAN, A. y GURSKI, M. (Comisario de información y privacidad de Ontario) y MULLIGAN, D. y SCHWARTZ, A. ("Center for Democracy and Technology"), *P3P and privacy: an update for the Privacy Community,* disponible en: wysiwyg://16/http://www.cdt.org/privacy/pet/p3pprivacy.
213 Véase la nota al pie anterior.
214 http://www.truste.org.
215 http://www.privaseek.com.
216 http://www.bbbonline.org/businesses/privacy/index.html.
217 http://www.cpawebtrust.org/consumer/index.html.
218 La autoridad francesa para la protección de datos (CNIL) ha realizado un trabajo muy interesante en este ámbito que podría servir para inspirar la norma europea. Véase www.cnil.fr.
219 En los Países Bajos se aprobó una moción durante el debate parlamentario sobre la nueva legislación de protección de datos en la Segunda Cámara, por la que se pidió al Gobierno que fomentase el desarrollo y el uso de las tecnologías de protección de la privacidad y que instase al sector público a tomar la iniciativa como promotor de este tipo de tecnologías en su propio tratamiento de datos personales. Moción número 31 de NICOLAÍ C.S., presentada el 18 de noviembre de 1999 con relación al proyecto de ley 25 892 *(Regels inzake de bescherming van persoonsgegevens, Wet bescherming persoonsgegeven* s), La Haya, Tweede Kamer, vergaderjaar 1999-2000, 25 892, n§ 31.
220 Algunas de estas definiciones se han extraído de las siguientes fuentes: - http://www.techweb.com/encyclopedia - http://webopedia.Internet.com - *Personal Data Privacy and the Internet: a guide for data user*s, Office of the Privacy Commissioner for Personal Data, Hong Kong, 1998.
221 Definición tomada del ETSI (Instituto Europeo de Normas de Telecomunicaciones), *"Requirements for TTP services".*

222 Véase http://www.umts-forum.org/.
223 Para obtener más información, véase: http://www.wapforum.org.