COMPARECENCIA EN EL SENADO DEL DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, D. JOSE LUIS PIÑAR MAÑAS, ANTE LA COMISIÓN DE LA SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO EN EL SENADO

12 de Mayo de 2005

Gracias Señor Presidente. Con la venia de sus Señorías.

Quiero ante todo agradecer a esta Comisión la oportunidad que me ha brindado para poder comparecer ante la misma al objeto de exponer algunas de las acciones más importantes que tiene en marcha la Agencia Española de Protección de Datos, que me honro en dirigir, en el marco de la implantación de la Sociedad de la Información. Agradecimiento sincero por cuanto además es ésta la primera ocasión que tengo de comparecer ante el Senado y en consecuencia ante esta Comisión.

La Sociedad de la Información, es decir, la posibilidad de disponer de información veraz en tiempo real, está produciendo un cambio radical en nuestra sociedad y en todas las sociedades avanzadas. La implantación de nuevas tecnologías, y sobre todo la posibilidad de que el uso de tales tecnologías sea algo cotidiano, o tienda a serlo, está llamada a acabar con barreras discriminatorias y a facilitar la consolidación de una sociedad abierta y democrática. Pero al mismo tiempo puede implicar la aparición de nuevos riesgos para los derechos fundamentales si no se adoptan las medidas oportunas para evitarlos. Como es obvio me refiero fundamentalmente al riesgo que puede suponer para el derecho fundamental a la protección de datos personales; derecho autónomo e independiente que enlaza directamente con el derecho a la intimidad pero también y de modo muy principal con la dignidad

misma de la persona. Derecho que como SS.SS. conocen fue ya conceptualizado por nuestro Tribunal Constitucional en la notable Sentencia 292/2000, de 30 de noviembre; que recoge expresamente la Carta Europea de Derechos Fundamentales y que proclama, no en una, sino en dos ocasiones, la Constitución Europea, en sus artículos I-51 y II-68.

La Agencia Española de Protección de Datos debe velar para que ese derecho fundamental sea respetado y garantizado. Es la entidad pública independiente llamada a garantizar el derecho a la protección de datos personales. Autoridad Pública de la que no cabe prescindir, no sólo porque está prevista en la Ley Orgánica 15/1999, de Protección de Datos Personales, sino porque viene exigida por la Directiva 95/46/CE y, nada más y nada menos, por la propia Constitución Europea, que declara expresamente que en cada uno de los Estados miembros deberá existir una autoridad independiente de control que garantice el respeto a tal derecho. Autoridad Pública, en fin, que según la STC 290/2000, también de 30 de noviembre, como la que antes cité, está llamada a garantizar de forma homogénea el derecho a la protección de datos en todo el territorio nacional.

En este contexto, la Agencia desempeña un papel capital en la implantación y desarrollo de la sociedad de la información. Para ello cuenta con importantes competencias que le han sido atribuidas no solo en la antes citada LOPD, sino asimismo en la Ley 32/2003, General de Telecomunicaciones, recientemente desarrollada por el Real Decreto 424/2005**,** de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, y en la Ley 34/2002, de Servicios de la Sociedad de la Información. Tales competencias son como digo, y disculpen SS.SS. si insisto en ello, capitales para el desarrollo efectivo de la sociedad de la información.

Se considera que al día se envían y reciben decenas de miles de millones de correos electrónicos no deseados en el mundo. Se calcula que en 2001 el spam representaba sólo un 7% del tráfico mundial de correo electrónico; la cifra pasó al 29% en 2002, a más del 50% en 2003. Hoy supera seguramente el 70%. Como ha denunciado la Comisión Europea en su Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, sobre las comunicaciones comerciales no deseadas o spam, de 22 de enero de 2004, el spam constituye un problema desde muy diversos puntos de vista: Intimidad, fraude a consumidores, protección de menores y de la dignidad humana, costes suplementarios para las empresas, pérdida de productividad. Socava la confianza de los consumidores en el comercio electrónico, los servicios en línea, e incluso, en la sociedad de la información.

Para el ciudadano, para los particulares, el spam representa una intrusión en su intimidad, induce a error o engaño, suele responder a una voluntad clara de estafar a los destinatarios. Para las empresas genera costes muy considerables. Tanto directos (tiempo dedicado a eliminar correos no deseados –una media de 15-20 minutos al día por usuario-, recursos dedicados a solucionar el problema, coste de las medidas de seguridad...) como indirectos (no recepción de mensajes importantes como consecuencia de los sistemas de filtrado -falsos positivos-, o recepción de mensajes no deseados y no interceptados –falsos negativos-; coste derivados de los virus....). Se ha calculado que en 2002 el spam costó a las empresas europeas en torno a 2.500 millones de euros en pérdidas de productividad. Por otra parte, el spam socava la confianza de los ciudadanos en relación con el comercio electrónico y la sociedad de la información, como antes apunté.

La UE hizo frente a esta situación adoptando la Directiva 2002/58/CE, sobre la intimidad y las comunicaciones electrónicas. Se trata en definitiva de

adoptar medidas que -pese a ser costosas- son necesarias si, como señala la Comisión Europea, “se quiere que el correo electrónico y los servicios electrónicos sigan constituyendo una herramienta de comunicación eficiente”, imprescindibles para la sociedad de la información.

La Comisión ha recomendado vivamente que se adopten medidas que permitan luchar eficazmente contra el spam. De modo que se garantice la aplicación y cumplimiento de la legislación; se adopten soluciones técnicas eficaces; se potencie la autorregulación por parte de la industria y se incremente la sensibilización entre los usuarios.

La antes citada Directiva 2002/58/CE ha previsto un riguroso régimen jurídico aplicable a las comunicaciones comerciales, que entre otras medidas incluye la identificación de las comunicaciones comerciales electrónicas como publicidad; Identificación del remitente (no basta la identificación a través de una denominación comercial); Inclusión de una dirección de respuesta válida para oponerse a los envíos; exigencia de consentimiento previo para el envío de mensajes comerciales (salvo que exista una relación contractual previa y las comunicaciones se refieran a Servicios propios de la entidad análogos a los contratados); Posibilidad de oponerse en cualquier momento (revocación del consentimiento).

Este régimen ha sido transpuesto al ordenamiento español mediante la nueva Ley General de Telecomunicaciones (en cuya redacción la Agencia Española de Protección de Datos desempeñó un importante papel), que como ya antes adelantaba ha sido recientemente desarrollada, en parte, por el y RD 424/2005. Asimismo debe tenerse en cuenta la también citada LSSI. Se establece así un régimen jurídico que no sólo protege a las personas físicas, sino también a las personas jurídicas, y que se basa en la atribución a la AEPD (desde el 20 de marzo de 2004) de notables competencias de inspección y

sanción. De modo que es posible afirmar que España cuenta con uno de los sistemas más garantistas frente al spam de todos los países de la Unión Europea. Hasta al fecha se han iniciado 97 expedientes de investigación y se han iniciado 14 procedimientos sancionadores, de los que se han resuelto 6, siendo los casos más repetidamente planteados aquellos que tiene que ver con el envío de correos electrónicos sin consentimiento previo del destinatario.

En cualquier caso, debo decir que en no pocas ocasiones la lucha contra el spam ofrece enormes dificultados debido a que los correos electrónicos provienen de más allá de nuestras fronteras. El spam, en efecto, no conoce fronteras, pero quienes envían correos no solicitados saben perfectamente que los vacíos legales les amparan. Por eso la AEPD ha iniciado unas fructíferas relaciones con otras autoridades de control, que se enmarcan en la vocación de cooperación internacional que informa la actividad de la Agencia, y que se plasma entre otras cosas, en que en estos momentos tengo el honor de ostentar la vicepresidencia del Grupo Europeo de Autoridades de Control de Protección de Datos, conocido como Grupo del Artículo 29 (por ser el artículo 29 de la Directiva 95/46/CE el que lo estableció) y la presidencia de la Red Iberoamericana de Protección de Datos. Además, la Agencia participa en numerosos foros internacionales como los talleres de la OCDE de lucha contra el spam o el Grupo CNSA (Contact Network of Spam Authorities) de la Comisión Europea. Querría destacar especialmente nuestra activa participación en la iniciativa denominada London Action Plan, surgida bajo los auspicios de la OCDE el 1 de octubr de 2004 (en cuya creación e impulso participó y participa activamente la Agencia), que reune a casi una veintena de autoridades de quince países para luchar eficazmente contra el spam mediante el desarrollo de iniciativas concretas y prácticas, como la Operación Zombie Drone.

La iniciativa “Zombie Drones”, enmarcada dentro del Plan de Acción de Londres, pretende luchar contra una de las técnicas de envío mas utilizadas por los spammers, según la tendencia actual.

Los spammers, explotando los fallos de seguridad de los equipos conectados a Internet - normalmente los ordenadores personales de los usuarios conectados mediante una línea de alta capacidad (como ADSL) - introducen en los equipos aplicaciones maliciosas (“*malware”*) que les permiten tomar el control de los mismos, pudiendo emitir spam desde ellos. Estas pequeñas aplicaciones se denominan “zombie drones”.

De esta forma los spammers ocultan su identidad, pareciendo que los mensajes son emitidos por el usuario habitual del equipo.

La iniciativa en marcha intenta despertar la conciencia sobre el problema en los proveedores de servicios, animándoles a ser más proactivos. Se proponen una serie medidas de carácter técnico y educacional, como pueden ser el incremento del nivel de seguridad en los equipos de los usuarios y en los servidores del propio proveedor, así como el suministro de información y herramientas de seguridad a los usuarios.

En el ámbito de la Unión Europea se ha solicitado ya la colaboración de las autoridades de Alemania y Reino Unido en casos concretos y en cuanto a las relaciones bilaterales con EEUU querría destacar la firma en Washington el pasado mes de febrero (de 2005) de un Acuerdo de Colaboración o MOU (Memorandum of Understanding) entre la AEPD y la FTC (Comisión Federal de Comercio) para luchar contra el spam, sobre todo el remitido desde aquél país, así como, por nuestra parte, para colaborar en la lucha contra el cada vez más numeroso e intenso spam en español.

Por otra parte, y en el ámbito de la Comunidad Iberoamericana, la Agencia promovió el pasado año la celebración del III Encuentro Iberoamericano de Protección de Datos en Colombia, suscribiendo la llamada Declaración de Cartagena de Indias, en la que se dedica una atención destacada a la lucha contra el spam. Entre otras conclusiones, se señala lo siguiente:

> "La intromisión ilegítima que el "spam" realiza en la privacidad, el perjuicio económico que el mismo ocasiona a los ciudadanos y a las empresas, así como el envío a través del mismo de contenidos que en muchos casos resultan engañosos y fraudulentos, hacen que la sociedad exija medidas que combatan la realización de este tipo de prácticas.
>
> Deben adoptarse medidas técnicas que permitan controlar y establecer filtros al envío de "spam". Estas medidas resultan necesarias, aunque no suficientes para contrarrestar el crecimiento de estas prácticas. En este sentido deberían adoptarse medidas legislativas que disciplinen específicamente la lucha contra el "spam", garantizando los derechos de los usuarios y regulando, en lo que sea necesario, la actividad que desarrollan los diferentes agentes implicados en esta actividad. La colaboración internacional en esta materia permitirá establecer un marco homogéneo, que resulta imprescindible para combatir el "spam", dado el ámbito transnacional del propio fenómeno. Es preciso, además, propiciar e impulsar iniciativas de autorregulación sectorial que complementen y faciliten la aplicación del marco regulatorio sobre la materia.
>
> Por último, es imprescindible que se adopten medidas que potencien la concienciación de los usuarios en relación con los perjuicios que la práctica del "spam" les genera. De esta manera, los agentes que

posibilitan la propagación de “spam” verán dificultada su actividad por una mayor formación de los usuarios, lo que contribuirá a prevenir activamente esta problemática que presenta múltiples interdependencias.”

Creo, Señorías, que las anteriores consideraciones resumen muy precisamente las iniciativas que han de tomarse contra el spam y a favor de la sociedad de la Información. La Agencia Española de Protección de Datos está volcada en ello.

En este sentido, acaba de incorporar a su página web una guía contra el Spam dirigida fundamentalmente a los ciudadanos y ha actualizado una guía para usuarios de internet, también disponible en la web. En el año 2000 llevó a cabo un Plan Sectorial de Oficio en el sector del Comercio Electrónico y en el 2002 otro sobre la Banca a Distancia.

En relación con el primero, debe destacarse el gran desarrollo que han experimentado las transacciones comerciales electrónicas, y al mismo tiempo el progresivo incremento en el nivel de cumplimiento de la normativa sobre protección de datos y en particular de seguridad. No olvidemos que una de las causas más importantes de la ralentización en la generalización del comercio electrónico (pieza clave en la sociedad de la información) es la desconfianza de los usuarios, derivada de la percepción que tienen en torno a la falta de seguridad y confidencialidad en el tratamiento de los datos personales. Pudo apreciarse entonces (Plan Sectorial de Oficio en el sector del Comercio Electrónico, de 2000), que no siempre se ofrecía un canal seguro para garantizar la confidencialidad de las transacciones, (incumpliendo en ocasiones lo establecido por el Reglamento de Medidas de Seguridad aprobado por Real Decreto 994/1999). En alguna ocasión se detectó la utilización de vías no seguras para la confirmación al usuario de sus propios datos de registro

(incluida su contraseña o clave de acceso); tal es el caso de la remisión de tales datos por correo electrónico sin aplicación de procedimientos de cifrado.

En el segundo semestre del año 2003 la Inspección de Datos acometió un intenso análisis (hasta 170 páginas web) de los denominados portales de empleo y, en general, de aquellas entidades que, a través de Internet, recaban datos de carácter personal de los demandantes de empleo: entidades públicas (Administración Local, Cámaras de Comercio, Universidades), privadas de interés general (fundaciones, organizaciones profesionales), y otras entidades (empresas de trabajo temporal, empresas de selección de personal, consultoras de RRHH, grandes compañías). En breve la Agencia hará públicas las recomendaciones correspondientes. Pero puede ya adelantarse que hemos apreciado un notable incremento en la implantación de medidas de seguridad.

En cualquier caso, nunca está de más recordar la cautela que ha de asumir el propio usuario al operar en Internet. Cautelas que requieren por su parte un especial cuidado al facilitar sus datos sin las debidas garantías.

Por otra parte, la AEPD forma parte del Comité de Coordinación para la implantación del DNI electrónico y de la Comisión Técnica de apoyo al citado Comité. El DNI electrónico va a ser, sin duda, una de las piezas más importantes en la implantación de la sociedad de la información. Como saben SS.SS. los artículos 15 y 16 de la Ley 59/2003, de Firma Electrónica regulan el DNI electrónico, que se define (art. 15) como “el documento nacional de identidad qu acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos”. El mismo artículo 15 dispone que todas las personas físicas o jurídicas, públicas o privadas, habrán de reconocer la validez del DNI-e para certificar la identidad y demás datos personales del titular y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

La Ley 59/2003 no hace mención expresa de los datos que ha de contener el DNI-e, pero el artículo 17 se remite a lo contemplado en la LOPD y señala que no se incluirán datos de los previstos en el artículo 7º de la misma (datos especialmente protegidos). La creación del DNI-e deberá hacerse, pues, con pleno respeto de los principios configuradores del derecho fundamental a la protección de datos: finalidad, calidad, información, y en particular, principio de seguridad, lo que exigirá adoptar las medidas de seguridad adecuadas en el proceso de implantación del DNI-e y, por supuesto, en el propio documento.

Asimismo, hemos iniciado una línea de colaboración en la implantación y desarrollo del Plan Conecta y debemos informar cuantos proyectos normativos afecten a la protección de datos personales, lo que vale decir cualquier proyecto que tenga que ver con la implantación de la sociedad de la Información. Ella misma ha puesto en práctica el compromiso de transparencia y respeto a la protección de datos que exige la sociedad de la información mediante la aprobación de la Instrucción 1/2004 sobre publicación de sus resoluciones, al objeto de transparentar más su actividad y acercarla a todos los ciudadanos y responsables de tratamientos de datos personales.

Para ello la AEPD cuenta con una plantilla de personal funcionario de altísima cualificación profesional que cumple con rigor sus funciones, pero que sin duda es muy reducida. La relación de puestos de trabajo es de algo más de 100 personas, claramente insuficiente, en efecto, para el correcto desarrollo de sus funciones, como entidad que debe garantizar el derecho fundamental a la protección de datos. Su presupuesto también es extraordinariamente modesto: 7 millones de euros para el presente ejercicio. El más bajo de todas las administraciones independientes del Estado, y menor al correspondiente a otras autoridades europeas de protección de datos semejantes a la Agencia. Tenemos un grave problema en cuanto a la sede que ocupamos, claramente

insuficiente pues está pensada para una plantilla de 60 personas, que además debemos resolver ineludiblemente antes de finalizar el presente ejercicio.

Señorías, desde mi responsabilidad al frente de la Agencia y el servicio público que ha de prestarse a los ciudadanos debo resaltar el papel central que juega la AEPD en la implantación efectiva de la sociedad de la información, y con pleno respeto a los derechos de los ciudadanos, entre ellos el derecho a la protección de datos y a la intimidad. Porque tales derechos, como señalaba al principio de mi intervención guardan directa relación con la dignidad de la persona. La protección de datos, como ha señalado con acierto quien ha sido hasta hace unas semanas Garante de la Privacidad en Italia, y fue Presidente del Grupo del artículo 29 de la Directiva 95/46/CE, Profesor Stefano Rodotà, es pieza capital no sólo en la sociedad de la información, sino también en la sociedad del pluralismo y de la democracia; en la sociedad de la dignidad.

La Agencia, abierta a la total y leal colaboración con el resto de entidades que han de liderar la consolidación de la sociedad de la información, desde el cumplimiento riguroso y sensato de sus funciones y competencias, hará todo lo que esté en sus manos para mejorar la vida de los ciudadanos y la calidad de los servicios públicos. Por eso, Señorías, agradezco de nuevo la ocasión que me han dado para comparecer ante esta Comisión y quedo a su entera disposición para cuantas cuestiones deseen formular y cuantos requerimientos de información consideren oportunos.

Muchas gracias Señorías, muchas gracias Señor Presidente.