

## WHAT DO CITIZENS KNOW AND FEEL?

### WHAT ARE CITIZENS FEAR ON NEW TECNOLOGIES?

Señor presidente, queridos colegas:

Enhorabuena queridos colegas italianos (amigo Pizzetti) por la organización de una Conferencia tan espléndida.

What do citizens know and feel? What are they fear on new technologies?

. Nuestro trabajo como Autoridades de de Protección de Datos es muy claro: proteger a los ciudadanos en el ejercicio y garantía de su derecho fundamental a la protección de datos de carácter personal; del cual los ciudadanos son titulares. Para ello se nos atribuyen poderes de investigación, auditoria y enforcement.

Sin embargo, permítanme que formule en voz alta algunas preguntas aparentemente muy sencillas. What do citizens know and feel? What are they fear on new technologies? ¿Qué piensa el ciudadano? ¿Los ciudadanos conocen realmente los riesgos asociados al uso de las tecnologías para su privacidad? ¿Viven, acaso, en un estado de feliz desconocimiento?

Permítanme que comparta con ustedes algunas reflexiones que me han provocado recientes y relevantes encuestas de opinión ciudadana.

Muy recientemente (hace escasamente tres semanas) se hicieron públicos en España los resultados de una relevante encuesta sobre “privacidad, nuevas tecnologías y, singularmente, Internet” preparada por la AEPD y realizada por el principal Centro Español de Investigaciones Sociológicas.

Si pudiéramos resumir los resultados de la encuesta en un breve titular diríamos que “los ciudadanos están bastante preocupados por los riesgos para su privacidad y por la seguridad de sus datos personales generados por las nuevas tecnologías de la información”.

Examinemos los datos obtenidos: casi un 65% dice acceder a Internet todos o casi todos los días:

Los principales usos que obtienen de Internet son:

- el 91% busca información o documentación.
- el 80% manda correos electrónicos.
- casi el 50% descarga archivos musicales, videos o películas (con programas peer to peer).
- el 45% chatea, acceder a foros o usa el Messenger.

Destaquemos algunas cifras muy significativas que evidencian los temores de los ciudadanos:

- Un 70% de los ciudadanos se muestra preocupado por la protección de datos y el uso de información personal por otras personas.
- el 63 % está preocupado por el avance de la ciencia y la tecnología y el 55% por el desarrollo de la comunicación e información a través de Internet.
- Casi un 60% de usuarios considera fiables las páginas de Internet y dicen leer sus políticas de privacidad.
- El 50% sabe que al navegar por Internet deja un rastro de información personal.
- Al 80 % de los ciudadanos les preocupa la difusión de imágenes en Internet.
- A más del 75% no le da seguridad facilitar el número de su tarjeta de crédito por Internet.

Algunas de estas cifras se han visto corroboradas por la encuesta realizada en la Unión Europea por Eurostat con motivo del Safer Internet Day. En ella se evidencia que el uso de Internet alcanza al 60% de los ciudadanos; que existe un

uso generalizado de los sistemas peer to peer para compartir archivos, música o películas (casi el 50%); pero casi un 50% evita usar la banca electrónica.

En ambas encuestas subyace una misma idea: el ciudadano está preocupado por la seguridad de sus datos en Internet.

Queridos amigos y colegas:

Estas cifras nos permiten apuntar algunas conclusiones:

1º) Es muy probable que los ciudadanos no sepan definir con precisión el alcance y naturaleza del derecho fundamental a la protección de datos pero, podemos estar seguros, de que lo intuyen, reconocen e identifican en cuanto éste es amenazado y puesto en riesgo.

Seguramente, los ciudadanos no tendrán una conciencia clara de cómo proteger sus derechos pero su mensaje muy claro: nos preocupa Internet, nos preocupa nuestra privacidad y nos preocupa la seguridad de nuestros datos personales en la Red.

2º) Los ciudadanos dicen conocer la existencia de las políticas de privacidad en Internet. Sin embargo, nuestra experiencia práctica nos ofrece una conclusión bien contraria. El número de accesos a las páginas de las políticas de privacidad es muy bajo, prácticamente marginal: ¿Un 1 por cada 100.000 accesos a Internet?.

Las políticas de privacidad ocupan espacios residuales en los websites y resultan ininteligibles. Por tanto, es evidente que el ciudadano, a pesar de creer lo contrario, desconoce el contenido real y las consecuencias de estas políticas de privacidad. En Internet no puede hablarse de un consentimiento basado en información fiable o confiable.

Formalmente, los proveedores de Internet cumplen con su deber de informar pero la mayor parte de las veces las reglas del juego en Internet es clara y se basa en: "o lo tomas o lo dejas" ("take it or leave it clauses").

3º) Por otro lado, los usuarios intuyen que la navegación por Internet deja rastro. Unos pocos expertos saben que sus perfiles de navegación son susceptibles de explotación comercial. Pero, a pesar de ello, son mayoritariamente indiferentes a este riesgo.

Sin embargo, esta trivialización o indiferencia frente a los rastros invisibles en Internet desaparece cuando existe una conciencia clara de riesgo: por ejemplo, cuando se procesan sin consentimiento imágenes en Internet o cuando existen un fallos de seguridad; en consecuencia, cuando la alarma social es inmediata.

Estas ideas pueden corroborarse desde la experiencia práctica de la Agencia Española de Protección de Datos:

- ▶ La captación ilícita de imágenes y su difusión en Internet han causado conmoción pública y alarma social.

- ▶ Los ciudadanos, de forma progresiva, demandan su derecho al olvido en Internet ejerciendo sus derechos de cancelación y oposición..

- ▶ El mal uso por los ciudadanos del software “peer to peer” de intercambio de archivos en Internet está poniendo en gravísimo riesgo y peligro la seguridad de los datos personales. La AEPD ha investigado y sancionado numerosos casos en los que datos personales (incluso especialmente protegidos) han sido volcados a Internet; miles de datos personales de historias clínicas (incluso aborto), de clientes de abogados o de miles de trabajadores de participantes en actividades de sindicatos.

Estamos ante un gravísimo problema de desconocimiento e ignorancia en el uso de estas tecnologías de Internet. Y la “letra pequeña” de las ilegibles cláusulas generales de contratación para la instalación de software contribuye significativamente a este problema. ¿Cuántos datos están ahora mismo esperando en Internet a que alguien busque y encuentre en un peer to peer los archivos en que se encuentran dichos datos personales?

- ▶ Por otro lado, la privacidad de los ciudadanos padece reiterados ataques en foros públicos de Internet y en blogs.

► Emergen las denuncias contra las prácticas en Internet consistentes en cribar de forma automatizada los contenidos de los correos electrónicos para anexarles publicidad personalizada: estamos ante un potencial riesgo de obtención de perfiles de personalidad.

Queridos colegas:

Como todos ustedes saben, la Ley de Gordon Moore afirma que el número de transistores en un chip se multiplica por dos cada 18 meses a igual coste, y con él las capacidades de proceso y almacenamiento de información. Así las cosas, el ciudadano conoce inmediatamente cualquier nueva tecnología, para él ya no son nuevas. El individuo intuye con bastante claridad los riesgos, está preocupado y exige nuestra actuación.

Estamos ante un ciudadano-red en una sociedad-red. Pero los perfiles de la sociedad-red son difusos. Las comunidades en Internet pueden abarcar ámbitos tan reducidos como el grupo de los compañeros de colegio, o tan amplios como el conjunto de profesionales de todo el planeta.

Cuando las tecnologías de la información alcanzan el mercado, el ciudadano-red está obligado a negociar y defender su privacidad en condiciones de franca desigualdad y desequilibrio. La negociación en el “mercado de la privacy” favorece y coloca en posición dominante a quien presta un servicio “aparentemente libre” en Internet a cambio de la privacy.

Frente a ello, ¿qué reglas debemos aplicar?, ¿el modelo europeo?, ¿debe confiarse en la autorregulación de los proveedores de servicios de Internet?, ¿ha llegado la hora del gobierno del código de la privacidad en Internet?.

En nuestro modelo europeo, el ciudadano, titular de sus datos personales cuenta con un estándar de protección y ejerce unos derechos que le proporcionan un verdadero control sobre sus datos personales.

Pero, la protección de los datos personales preocupa a la sociedad global, en el mundo entero. Asistimos, al nacimiento de iniciativas en organizaciones internacionales, regionales o especializadas. Se defiende la necesidad de proponer de estándares compartidos. Incluso, se plantea la necesidad de organismos internacionales de alcance planetario a los que atribuir una universal función protectora de la privacidad (y no sólo en Internet o en el ámbito específico de las nuevas tecnologías).

Todo ello, nos aboca a un reto singular: el de la juridicidad de cualquiera de estos compromisos internacionales.

Desde una posición meramente reactiva, las Autoridades de Protección de Datos nos enfrentamos en este punto a una paradoja: la ilustrada por el ilustre filósofo griego presocrático, Zenón en su fábula sobre “la carrera de Aquiles y la Tortuga”. Al vertiginoso ritmo marcado por la Ley de Moore, la garantía reactiva de la privacidad frente cada nueva tecnología emergente siempre llegará tarde. Como Aquiles, al terminar de recorrer la mitad del camino, la tortuga ya no estará allí. Siempre habrá una nueva tecnología, siempre nos quedará la mitad del camino por recorrer y así hasta el infinito. ¡Siempre llegaremos tarde si sólo buscamos reaccionar frente a los riesgos ya consolidados!

Sin embargo, permítanme una pregunta: ¿Acaso quienes diseñan e implantan las nuevas tecnologías desconocen los principios de protección de datos personales? ¿no son conscientes de los estándares de seguridad necesarios? ¿Agreden nuestra privacidad de modo consciente?

Queridos amigos;

Con el tiempo, los matemáticos demostraron que la aporía de Zenón era un sofisma. Que bastaba con cambiar de paradigma para demostrar su falsedad. Seguramente, la cuestión no es qué capacidad tenemos para regular una nueva tecnología sino qué criterios jurídicos deben regir el diseño de tecnologías invasivas de la privacidad.

La dificultad estriba en la globalidad y muestra la necesidad de alcanzar estándares jurídicos universales. Se trata de obtener un complejo equilibrio. La normatividad internacional no debe frenar el impulso creativo, la innovación y el desarrollo económico que deriva de las nuevas tecnologías. Sin embargo, sí debería fijar principios cuyo respeto constituya un mínimo común denominador de obligada atención en el diseño tecnológico. Resulta esencial alcanzar acuerdos que respeten la cultura de la privacy en cada país y en cada región del mundo pero que garanticen un ejercicio efectivo de los derechos de los ciudadanos.

Las autoridades de protección de datos nos enfrentamos cada día a riesgos actuales, reales y no teóricos; pero, podemos y debemos anticipar el futuro: “YES ... WE CAN!.

Muchas gracias por vuestra atención.