# LA PROTECCIÓN DE DATOS EN ESPAÑA. ANÁLISIS DE ACTUALIDAD

Artemi Rallo Lombarte
*Director de la Agencia Española de Protección de Datos*
*Catedrático de Derecho Constitucional*
Universidad Jaume I de Castellón

**Resumen:** La trascendencia social e institucional del derecho a la protección de datos personales se refleja claramente en el papel desempeñado por la Agencia Española de Protección de Datos en una actividad multidisciplinar que va desde la divulgación a través de guías explicativas hasta el incremento sin precedentes del número de denuncias formuladas. Los medios de comunicación han ahondado en esa sensibilización identificando los problemas que preocupan a la sociedad. Pese a ello, grandes interrogantes aquejan aún a la privacidad; debiendo destacarse los relativos a la videovigilancia, la protección de datos en el entorno laboral o los nuevos riesgos derivados del desarrollo de las redes sociales en Internet. El mundo globalizado demanda un compromiso para la consolidación de una cultura de protección de datos que cristalice en la asunción de unos estándares internacionales para la protección de los datos personales y la privacidad que hagan real y efectiva la garantía de este derecho fundamental.

**Palabras clave:** Agencia Española de Protección de Datos, Videovigilancia, Redes Sociales, Internet, Privacidad.

**Abstract:** The social and institutional transcendence of the right to personal data protection is clearly manifested in the role played by the Spanish Data Protection Agency in a multidisciplinary activity that goes from the publication of user guidelines to the unprecedented increase of lodged complaints. Mass media have dwelt on awareness, by identifying issues that concerns to the society. However, there are major questions that still affect privacy; we must stress those related to video surveillance,

data protection in the workplace or new risks arising from the development of social networks on the Internet. This globalized world demands a commitment to build a culture of data protection, which materializes on the assumption of international standards for the protection of privacy and personal data that make real and effective the protection of this fundamental right.

**Keywords:** Spanish Data Protection Agency, Video surveillance, Social Networks, Internet, Privacy

**SUMARIO:** I. INTRODUCCIÓN. II. LA AGENCIA ESPAÑOLA COMO CATALIZADOR DE LA NUEVA SENSIBILIDAD. III. EL PAPEL DE LOS MEDIOS DE COMUNICACION. IV. LA PRIVACIDAD EN RIESGO: LOS GRANDES INTERROGANTES: 1. La videovigilancia: garantías ante un fenómeno omnipresente; 2. Internet vs. privacidad; 3. Especial atención a los menores; 4. Proteger los datos en el entorno laboral. El equilibrio entre obligaciones y derechos; 5. La privacidad en un mundo globalizado e interconectado. V. CONCLUSIONES.

## I. Introducción

Transcurridos treinta años desde que comenzase la andadura democrática, y nueve desde que el Tribunal Constitucional en su sentencia 292/2000 otorgase al derecho a la protección de datos carta de naturaleza propia, apenas resulta concebible un horizonte democrático que no contemple la protección de un derecho que si nació ya fuerte, hoy goza de una expansión mayor.

Este derecho, definido por el Tribunal como "el derecho fundamental que garantiza a toda persona "un 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", se encuentra regulado en la Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999. Cuando se cumple un año desde la entrada en vigor de este último, no cuesta observar una creciente sensibilización de los ciudadanos, poderes públicos y agentes sociales y económicos respecto de la trascen-

dencia social e individual del derecho. La constatación de una conducta más activa de los ciudadanos en la defensa de sus derechos se ha hecho incuestionable a raíz de la inclusión en el barómetro de febrero de 2008 del Centro de Investigaciones Sociológicas (CIS) de un cuestionario dirigido a evaluar la concienciación ciudadana sobre la protección de datos personales.

La encuesta coincidió en el tiempo con el Eurobarómetro realizado en enero y publicado en abril del mismo año, para medir la percepción de los ciudadanos de la Unión Europea sobre la misma materia. La comparación de sus resultados llevaba a una conclusión clara: la concienciación ciudadana en España se sitúa claramente por encima de la media europea. Más de un 70% de los ciudadanos en España se mostraba preocupado por la protección de datos y el uso de información personal por otras personas; cifra superior a la media europea que el Eurobarómetro situaba en el 64%.

Asimismo, el barómetro del CIS reflejaba que el 52,4% de los ciudadanos españoles afirmaba conocer la existencia de una ley que les protege contra posibles abusos que puedan producirse con sus datos personales, y situaba en un 64% el porcentaje de los ciudadanos que aseguraba tener conocimiento de la existencia de la AEPD como organismo encargado de la defensa de sus derechos.

Del barómetro del CIS se pueden extraer algunas conclusiones adicionales sobre las principales inquietudes de los ciudadanos: así, un 57,8% dice asegurarse de que las páginas de Internet que visita son fiables leyendo sus políticas de privacidad y un 54,1% sabe que al navegar en la red deja un rastro de sus datos personales. Respecto de la actividad publicitaria, el 68,2% ha recibido en alguna ocasión una llamada telefónica o un mensaje SMS en su teléfono móvil con fines publicitarios de entidades a las que no tiene constancia haberle facilitado sus datos personales. Porcentaje que asciende a casi el 80% respecto de los usuarios de Internet que aseguran haber recibido "spam" o correos electrónicos no deseados. Acerca de la seguridad en el tratamiento de sus datos, el 58,8% la valora de manera alta en la Administración Pública y de manera destacada en hospitales (55,6%) y bancos (53,3%). Esta percepción es menor en los comercios (el 31,3% considera que en ellos hay una baja seguridad) y destaca que facilitar datos personales para participar en un concurso ofrece poca o ninguna seguridad al 72% de los encuestados.

Dos elementos se encuentran detrás de la explicación de este incremento en la concienciación ciudadana. En primer lugar, el papel desem-

peñado por la Agencia Española de Protección de Datos. En segundo lugar, la difusión llevada a cabo por los medios de comunicación.

## II. La agencia española de protección de datos como organismo catalizador de la nueva sensibilidad

La Agencia Española de Protección de Datos es la autoridad de control independiente que vela por el cumplimiento sobre la normativa de protección de datos, garantizando y tutelando el derecho fundamental a la protección de datos de carácter personal. Su actividad se aposenta en tres pilares: capacidad de aplicación de la ley, asesoría a través de servicio legal y de atención al ciudadano, y comunicación. La Agencia actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

El nivel de concienciación derivado de la encuesta del CIS puede complementarse con el análisis de la información estadística que proporcionan los servicios internos de la Agencia. Estos servicios revelan que uno de los bloques de consultas más frecuentes al Servicio de Atención al Ciudadano de la agencia es el relacionado con el ejercicio de derechos. En este ámbito, destacan dos preguntas que se repiten de forma recurrente: "¿cómo puedo saber quien tiene mis datos personales y de dónde los han obtenido?" y "¿cómo cancelar los datos de un fichero?". De ellas se pueden obtener dos conclusiones: que los ciudadanos carecen de información o no son conscientes de los datos personales que facilitan y que, cuando son conscientes de que son utilizados por terceros, tratan de impedirlo solicitando su cancelación.

En 2008 los procedimientos para la tutela de derechos iniciados por reclamaciones de los ciudadanos se incrementó en un 88% y las resoluciones dictadas en un 44%. De estas resoluciones, el 70% se refirieron al ejercicio del derecho de cancelación y el 22,5% al derecho de acceso.

Con respecto al ejercicio del derecho de cancelación, se ha registrado un importante volumen de reclamaciones sobre el ejercicio del derecho en Libros-Registro de la Iglesia Católica. Según el criterio de la AEPD sostenido desde 2004, los libros de bautismo eran ficheros en tanto se trata de conjuntos organizados de datos de carácter personal, a los que puede aplicarse el principio de calidad de los datos en relación con la actualización y exactitud de los mismos, pudiéndose ejercer en relación con ellos el derecho de cancelación. Esto no obstante, la Sentencia Tribunal Supremo de 19 de octubre 2008 revocó el criterio de la AN (que daba la

razón a la AEPD), entendiendo que los libros de bautismo no pueden ser considerados como ficheros al ser "una pura acumulación de datos que comporta una difícil búsqueda, acceso e identificación en cuanto no están ordenados ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo". Con ocasión de la sentencia, la AEPD presentó un incidente de nulidad de actuaciones frente al Tribunal Supremo y se dirigió al Fiscal General del Estado y Defensor del Pueblo para que éstos interpusiesen recurso de amparo. Finalmente, la Fiscalía General del Estado y La AEPD han comparecido ante el TC interponiendo sendos recursos de amparo.

En cuanto al derecho de acceso, debe destacarse que las principales materias que han motivado su ejercicio han sido las imágenes de videocámaras en vía pública, las valoraciones de solvencia económica realizadas por entidades financieras, los historiales clínicos, o las imágenes en programas de televisión por parte de personajes públicos.

La AEPD se ocupa de garantizar el efectivo y eficaz cumplimiento de la LOPD y de impulsar que los responsables del tratamiento de datos puedan cumplir con la legislación exige multiplicar los esfuerzos que faciliten su conocimiento y dar respuesta a las dudas que puedan plantearse. El Área de Atención al Ciudadano y las consultas al Gabinete Jurídico de la Agencia han sido los canales tradicionales para hacer frente a esta exigencia. Sin embargo, el año 2008 ha supuesto un punto de inflexión en este ámbito, fruto de una decidida política dirigida a ampliar la oferta de información a los responsables del tratamiento. Un instrumento particularmente eficaz para ello es la edición de guías que difunden con un lenguaje claro, sencillo y fácilmente comprensible para cualquier responsable, los aspectos básicos de protección de datos.

Con este objetivo se publicó la "Guía de Protección de Datos para responsables de ficheros" abordando con una perspectiva general las exigencias de la LOPD. No obstante, las crecientes demandas de información sobre las medidas de seguridad que han de implantar los responsables de ficheros, especialmente tras la aprobación del Reglamento de Desarrollo de la LOPD (RLOPD), han hecho necesario editar "la Guía de seguridad de datos" para facilitar su implantación. La Guía incluye, además, un cuestionario de autoevaluación que permite conocer el grado de seguridad aplicado y su adecuación a la normativa vigente.

La publicación del RLOPD multiplicó en 2008 los requerimientos a la AEPD para conocer su criterio sobre el mismo. Para dar respuesta a esta demanda la Agencia ha adoptado una nueva iniciativa informativa

poniendo en marcha las "Sesiones Anuales abiertas de la AEPD". Ya la "I Sesión Anual" (a la que asistieron 2.000 participantes representativos de grandes corporaciones, consultores, Pymes, agentes sociales y Administraciones Públicas), supuso un cambio cuantitativo y cualitativo en la política de servicio público de la Agencia para facilitar el conocimiento de la LOPD. Su enfoque, como lo sería el de la segunda Sesión, fue esencialmente práctico, dirigido a contestar las preguntas previamente presentadas por los asistentes.

Estas iniciativas informativas dirigidas a facilitar el cumplimiento de la LOPD han venido a completar las tradicionales políticas preventivas de la AEPD basadas en las inspecciones sectoriales de oficio, que han tratado de atender algunas de las principales preocupaciones de los ciudadanos, como son las inspecciones sectoriales de oficio sobre llamadas telefónicas comerciales y sobre mensajes cortos a telefonía móvil. A ellas se ha añadido la realización de informes o declaraciones sobre nuevos retos en materia de protección de datos, especialmente respecto de los servicios en Internet.

Facilitar el cumplimiento de la LOPD es un objetivo que se complementa con la actividad dirigida a conseguir una mejor sistemática en las regulaciones sectoriales que puedan incidir en la protección de datos personales. El principal instrumento para lograrlo son los informes jurídicos previos y preceptivos sobre las disposiciones de carácter general que afectan a esta materia.

En 2008 fueron informadas 79 disposiciones de carácter general, entre las que cabe hacer referencia al Proyecto de Real Decreto por el que se regula el sistema de registros administrativos del Ministerio de Justicia de apoyo a la actividad judicial. En el ámbito de la seguridad y la garantía de derechos, debe destacarse el Anteproyecto de Ley de Control de Precursores de Drogas, el Anteproyecto de Ley por el que se modifica el Texto Articulado de tráfico y seguridad vial, o el proyecto de Real Decreto por el que se establecen medidas para garantizar la intimidad, la confidencialidad y la equidad en la prestación de la interrupción voluntaria del embarazo.

La mayor visibilidad que la AEPD tiene entre los ciudadanos se ha traducido en un fuerte crecimiento de las denuncias. Las actuaciones inspectoras previas a la iniciación de procedimientos sancionadores se incrementaron en un 45,4% y las resoluciones de los procedimientos iniciados casi se duplicaron (Δ 94,1%). Los sectores en los que se han realizado más inspecciones han seguido siendo los de telecomunicacio-

nes, entidades financieras y videovigilancia, que supone, en conjunto, el 50,9% de todas las realizadas. Por el contrario, las resoluciones sancionadoras disminuyeron en sectores como publicidad y prospección comercial, suministro de gas, electricidad y agua y enseñanza. Debe recordarse también que las resoluciones declarativas de infracción de la LOPD por las Administraciones públicas crecieron un 19,7% en su conjunto.

En cuanto a las sanciones declaradas, se ha constatado un aumento de las correspondientes a infracciones graves (551 frente a 350), manteniéndose estables las impuestas por infracciones muy graves y leves.

## III. EL PAPEL DE LOS MEDIOS DE COMUNICACION

El segundo motivo que, como se recordará, podemos considerar que está detrás de la nueva sensibilidad ciudadana sobre la protección de datos no es otro que el papel desarrollado por los medios de comunicación. Es ésta una causa que en cierta forma se encuentra imbricada con la anterior, pues si una de las principales funciones de la AEPD consiste en conseguir que los ciudadanos conozcan los derechos de los que son titulares, ello se ha conseguido en parte gracias a una muy activa política de medios de la agencia. Así, por ejemplo, sólo en 2008 la Oficina de Prensa de la AEPD atendió más de ochocientas demandas de entrevistas o de información, y emitió 78 comunicados de prensa. Ésta ha impulsado y facilitado que los medios de comunicación, generalistas o especializados, colaboren activamente en la difusión de las implicaciones que la protección de datos personales tiene en la esfera cotidiana de los ciudadanos y, especialmente, en las nuevas realidades vinculadas a los servicios de la sociedad de la información. Lo cierto es que sin la sensibilidad de los medios y sin su capacidad de difusión de los riesgos y alternativas de los ciudadanos para abordarlos, la eficacia de la AEPD en el desempeño de sus funciones quedaría severamente limitada.

La proximidad con los medios de comunicación se ha traducido no sólo en la difusión de los problemas puntuales sobre el uso de datos personales que generan inquietud a los ciudadanos, sino, también, en el desarrollo de proyectos de colaboración para el establecimiento de espacios informativos permanentes dedicados a la difusión del derecho a la protección de datos personales. Pero la implicación de los medios de comunicación, además de promover el conocimiento de los ciudadanos sobre sus derechos, ha tenido una virtualidad adicional: la sensibilidad de los medios de comunicación sobre la protección de datos personales ha

multiplicado su papel como agentes que han denunciado públicamente situaciones y conductas que pudieran vulnerar la LOPD, fruto de la actividad informativa sobre irregularidades que les corresponde de manera principal en una sociedad democrática. De este modo, gran parte de las investigaciones de oficio que ha llevado a cabo la AEPD tienen su origen en informaciones de medios de comunicación que, por su trascendencia social, han exigido la actuación de la Agencia.

Como principal ejemplo, podemos citar que durante el año pasado se iniciaron diversas inspecciones de oficio que traían causa de informaciones publicadas en medios de comunicación, sobre la aparición de documentos con información personal en la vía pública. En particular, cabe destacar, por su especial trascendencia, las inspecciones relativas al hallazgo en la vía pública de Valencia, Madrid, Barcelona, Sevilla y A Coruña de documentación judicial. No debe pasarse por alto la negligencia que supone dejar a disposición de cualquiera informaciones personales que hubieran debido ser destruidas o mantenerse confidenciales y que, en ocasiones, afectan a datos sensibles o especialmente protegidos, ya que ello pone de manifiesto, no ya una patente ignorancia de la entidad del problema, sino una verdadera desidia ante los derechos de los ciudadanos.

Por otra parte, la información difundida por los medios de comunicación ha constituido una referencia cualificada para focalizar las cuestiones relacionadas con la protección de datos personales que pueden ser más importantes para el público. Y así, hay que destacar como cuestiones que han suscitado mayor interés por parte de los medios de comunicación, la videovigilancia y la incidencia de las nuevas tecnologías en la privacidad de los ciudadanos (en particular, la filtración de datos sensibles a través de redes P2P, como e-mule, o el fenómeno de las redes sociales).

## IV. LA PRIVACIDAD EN RIESGO: LOS GRANDES INTERROGANTES

En España nos encontramos hoy sometidos a importantes retos que traen causa principalmente del trepidante ritmo de la revolución tecnológica, y de las exigencias de la actividad económica.

### 1. La videovigilancia: garantías ante un fenómeno omnipresente

Todos los datos disponibles apuntan a la conclusión de que la videovigilancia es un hecho imparable. La instalación de cámaras de videovigi-

lancia por razones de seguridad se está incrementando de manera exponencial en los últimos años. Así, los ficheros de videovigilancia inscritos en el RGPD en 2008 han duplicado a los de 2007, alcanzando una cifra total de 15.510. El 98,1% de ellos son de titularidad privada y sólo el 1,9% de titularidad pública.

El comercio ha pasado a ocupar el primer lugar de los sectores que han declarado ficheros de videovigilancia, seguido del turismo y la hostelería y de las comunidades de propietarios, que se alzan a la tercera posición, desplazando a la cuarta a los ficheros relacionados con la sanidad. Debe llamarse la atención sobre el importante crecimiento de ficheros de videovigilancia del sector educativo que se han incrementado en un 270%. Asimismo, las actuaciones previas de inspección en videovigilancia suponen el 15,5% del total de las realizadas, situándose en el tercer lugar de los sectores inspeccionados y las resoluciones de procedimientos sancionadores en este ámbito se han incrementado en un 633,3%.

Respecto de la percepción de los ciudadanos sobre el fenómeno de la videovigilancia, la encuesta del CIS que al principio citábamos, sugiere las siguientes reflexiones:

En cuanto a las cámaras de videovigilancia, el 73% se muestra a favor de su colocación. De ellos, el 71,1% la apoyan porque proporciona más seguridad, el 18,6% porque permite la identificación de los delincuentes y el 11,6% porque evita delitos. En contra de la instalación de cámaras se posiciona el 9,5%. El motivo fundamental para posicionarse en contra es la pérdida de intimidad con un 78,7%.

El lugar donde parece mal (28,7%) o muy mal (9,6%) la instalación de cámaras es el lugar de trabajo, pero le parece bien al 30,7% y muy bien al 15,4%. El 45,6% ve muy bien y el 49,4% ve bien la instalación de cámaras en bancos. La instalación de cámaras en guarderías y colegios le parece bien al 51,5% y muy bien al 29,3%. Le parece mal o muy mal al 8,5% y al 2,1% respectivamente. El 46,6% afirma saber que es obligatorio solicitar autorización para la instalación de estas cámaras. El 4,5% dice que no es obligatorio y el 48,7% "no sabe" si es obligatorio solicitar esa autorización.

El 73,2% se muestra a favor de que se controle la difusión de imágenes grabadas por cámaras de videovigilancia que se emiten por televisión o Internet. El 14,2% se muestra en contra. Los casos de difusión de imágenes por Internet o televisión en los que se ha vulnerado el derecho a la intimidad le parece preocupante al 76%, bastante preocupante al 44,1% y le preocupa mucho al 32,1%.

Se ha planteado así la necesidad de cohabitar en un entorno de videovigilancia en el que las garantías de la normativa de protección de datos personales se conviertan en la clave de bóveda que permite equilibrar la tutela de este derecho fundamental con las crecientes demandas de seguridad que fomentan la videovigilancia, lo que ha conducido a exigir a las empresas que ostentan legitimación para actuar en este ámbito una diligencia especifica en la difusión y cumplimiento de la LOPD acorde con la cualificación profesional que la Ley les reconoce. Ello además ha obligado a la AEPD a impulsar iniciativas apropiadas para facilitar el conocimiento de las garantías que han de respetarse, de forma clara y adaptada a los diversos entornos en que se realiza videovigilancia por razones de seguridad. En esa línea, debe destacarse la publicación de la Instrucción 1/2006 de 8 de noviembre para adecuar los principios y garantías de la LOPD a estas actividades, y la organización y celebración de las II Jornadas Abiertas centradas específicamente en el tema de la videovigilancia.

## 2. Internet vs. privacidad

La evolución de la web 2.0 ha multiplicado la oferta de nuevos servicios que están teniendo una acogida masiva entre los usuarios de Internet (buscadores, redes sociales, ...). Estos servicios se interrelacionan entre sí de forma que las posibilidades de obtener y tratar información personal ha crecido de forma vertiginosa. La AEPD ha sido pionera a la hora de ofrecer a los usuarios garantías para su privacidad en nuevos entornos tecnológicos.

Precisamente en relación con la videovigilancia que acabamos de citar, la Agencia inició de oficio actuaciones previas de inspección sobre la captación de imágenes a través de cámaras de vídeo de personas identificables en la calle Montera de Madrid y su posterior difusión en el portal de vídeos "YouTube", con el ánimo de mostrar la peligrosidad de la zona. También se iniciaron actuaciones de oficio sobre la emisión en dicho portal de imágenes de una persona discapacitada sin su consentimiento. De las resoluciones de ambos procedimientos se desprendieron varias conclusiones: la primera, que la imagen de personas identificables constituye un dato personal protegido por la LOPD. La segunda, que la captación y difusión de imágenes de terceros a través de portales de vídeo en Internet requiere, como regla general, el consentimiento de las personas. La tercera, que de no respetarse este requisito, puede ser sancionado por infracción grave de la LOPD aquel usuario que "cuelgue" las imágenes

en el portal provocando su difusión pública. La responsabilidad de esta infracción podría atribuírsele al titular de la línea telefónica que tenía asignada la dirección IP desde la que se "subieron" las imágenes o desde la que se creó la cuenta de usuario utilizada para publicar las imágenes.

Sobre la posibilidad de acceder a imágenes de personas a través de Internet, la Agencia ha detectado además nuevas prácticas como el visionado abierto y en tiempo real de personas identificadas o identificables por medio de cámaras accesibles a través de la red, por lo que ha iniciado una inspección sectorial de oficio.

Entre los servicios de la web 2.0, las redes sociales ocupan un papel muy destacado por el volumen de usuarios y de intercambios de información, así como por la variedad de información que se trata en ellas y, en particular, por los perfiles que ofrecen quienes las utilizan. Las redes sociales on line son servicios que permiten a los usuarios generar un perfil público en el que plasmar datos personales de uno mismo, con la posibilidad de interactuar con el resto de usuarios afines o no al perfil publicado. Su crecimiento se basa en un "proceso viral" en el que un número inicial de participantes ofrece a sus conocidos la posibilidad de unirse a la red, mediante invitaciones enviadas por correo electrónico. Se convierten así, en potentes canales de comunicación e interacción posibilitando que los usuarios actúen como grupos segmentados (profesionales, ocio, etc.).

Los riesgos que estas redes generan motivaron en 2008 un estudio conjunto de la AEPD con INTECO, en el que se constató que la información sobre la política de privacidad y las condiciones de uso de la red social suele ser poco clara y accesible, de forma que los usuarios desconocen qué uso se hará de su información personal. Pudo advertirse también la ausencia de aplicaciones que permitan controlar la edad de los menores que intentan acceder al servicio, y la facilidad con la que terceros, distintos de las personas catalogadas como "amigos" o "contactos directos" por el usuario puedan acceder a su perfil. Esta situación es consecuencia de que en muchas ocasiones la red social configura por defecto el mayor grado de visibilidad del perfil del usuario, de forma que si el usuario no toma la iniciativa para acotarlas, las posibilidades de acceso serán más amplias.

Asimismo, el estudio reveló un aumento en la publicidad hipercontextualizada basada en el análisis de los perfiles y preferencias de los usuarios, y otra serie de problemas entre los que figuraban los siguientes:

- Dificultades para eliminar la información y dar de baja su perfil a iniciativa del usuario, o cuando ha transcurrido un tiempo prudencial sin que haya accedido en la red social.

- Dificultades también en la determinación de la legislación aplicable a entidades ubicadas en terceros países, que condiciona la posibilidad de que las autoridades nacionales intervengan para garantizar los derechos de los usuarios residentes en su país.

- Riesgos asociados que afectan a aspectos distintos de la protección de datos personales como son los relativos a los derechos de propiedad intelectual, la defensa de los consumidores, la protección del honor o la comisión de delitos ("phising", "pharming", pederastia, secuestros, etc.).

Tras la información recabada en la investigación, se formularon una serie de recomendaciones a todos los agentes intervinientes para aumentar el grado de protección de los usuarios, entre las que se pueden contar:

- mejorar la información legal disponible.

- potenciar la formación de los usuarios.

- controlar de la indexación y almacenamiento de perfiles.

- implementar de sistemas de identificación de edad de los usuarios.

- establecer sistemas de identificación remota de los usuarios a través de firma electrónica.

Dos de esas redes sociales han adquirido una singular relevancia en la actualidad: Facebook y Tuenti. Con respecto a la primera de ellas, la AEPD, como parte de la ronda de contactos con los responsables de las principales plataformas de redes sociales, se reunió con sus resposables para requerir la puesta en marcha de una mejora en la política informativa de la plataforma, ofreciendo una información clara, accesible y comprensible, así como la utilización del establecimiento por defecto del grado máximo de privacidad de los usuarios en las opciones de configuración de privacidad del perfil, aprestándose Facebook a poner en práctica las medidas sugeridas. En cuanto a Tuenti, la AEPD también logró un compromiso de implantación de sistemas de verificación de edad de los usuarios, comprometiéndose Tuenti a la cancelación de los contenidos cuando el usuario solicite la baja de su cuenta.

Una de las posibilidades de acceso al perfil de terceros de las que antes hablábamos incluye la indexación por buscadores en Internet; es ésta una búsqueda que deriva con facilidad en las ediciones digitales de los diarios y boletines oficiales, cuya puesta en práctica ha multiplicado universalmente la posibilidad de conocer los datos personales publicados, y

el riesgo de agresiones a la privacidad, ya que entre los datos personales publicados en los boletines oficiales, algunos de ellos son especialmente sensibles. Ha comenzado a ser habitual, por lo tanto, la presentación de tutelas ante la AEPD al no haber atendido el buscador a la solicitud de oposición al tratamiento instada por los ciudadanos. Analizada esta cuestión por la AEPD, ha considerado que respuesta al problema debe obtenerse por la vía de la revisión de criterios de incorporación de datos personales a las publicaciones oficiales por parte de los órganos e instituciones.

3. Especial atención a los menores

El tratamiento de la información personal de niños y adolescentes constituye uno de los retos al que se enfrenta nuestra sociedad, y en relación con él, no basta con aprobar un marco regulador. Se requiere en cambio una actuación decidida de los poderes públicos articulada de planes específicos de protección de los menores, lo que implica hacer lo posible por evitar que los datos personales de menores puedan ser utilizados sin el consentimiento de sus padres o tutores. Pese a ello se constata que, con frecuencia, no se han desarrollado procedimientos que permitan conocer de manera efectiva la edad de los menores, especialmente, en productos o servicios accesibles en Internet. Advirtiendo de la necesidad de impulsar un acuerdo con los operadores y prestadores de servicios de telecomunicaciones y de la sociedad de la información de ámbito nacional para la implantación de mecanismos efectivos de comprobación de la edad, la Agencia Española de Protección de Datos ha dedicado distintos esfuerzos a promover la conciencia social sobre este problema. En primer lugar, con motivo del Día de Internet elaboró y presentó la Guía sobre "derechos de niños y niñas y deberes de padres y madres". Este documento incorpora recomendaciones básicas para concienciar sobre la importancia de la protección de datos en el entorno de la familia y la escuela. La Guía obtuvo una muy buena acogida tanto entre su público objetivo como por los medios de comunicación, proporcionando un fuerte impulso a las políticas de concienciación de la Agencia.

Las redes sociales antes citadas han puesto sobre la mesa hasta que punto Internet constituye la piedra de toque de la protección de los datos personales de los menores. En la 30ª Conferencia Internacional de Autoridades de Protección de datos pudo ya constatarse que la formación en el uso básico de las herramientas informáticas, con sus riesgos y ventajas es insuficiente, ya que nuestros hijos nacen a la sociedad como niños digi-

tales. La telefonía móvil, la televisión digital, las PDA, los juegos digitales, o Internet son su medio natural y social, pero no por ello aprenden a protegerse. En cualquier caso debe abordarse un reto urgente: desarrollar herramientas eficaces para conocer si los usuarios de servicios en Internet son menores, debiendo contar con la asistencia de sus padres.

En esta línea, el Reglamento de la Ley 15/1999 ya ha establecido un deber de diligencia que implica articular procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por padres, tutores o representantes legales. La AEPD, por su parte, ha resuelto un primer caso de tratamiento ilícito de datos de un menor sin verificación previa de su edad que culminó con la imposición de una sanción ante la falta de diligencia en la comprobación de la edad.

## 4. Proteger los datos en el entorno laboral. El equilibrio entre obligaciones y derechos

En el ámbito laboral, la normativa vigente legitima al empleador para tratar los datos personales de sus trabajadores en un amplio abanico de finalidades (art. 20 Estatuto de los Trabajadores). Pero esta legitimación está condicionada por el respecto a los derechos de los empleados. Las denuncias presentadas a la AEPD son indicativas del amplio espectro de problemas que se plantean:

- Utilización de datos biométricos para el control horario de los trabajadores.

- Instalación de sistemas de videocámaras y grabación de voz por razones de seguridad.

- Utilización del correo electrónico del trabajador.

- Acceso indebido y comunicación de información médica de los trabajadores sin las debidas garantías.

- Uso de certificados de vida laboral sin justificar procedencia de la información.

Una característica común de las denuncias se basa en la falta de información previa y suficiente a los trabajadores. Omisión que choca con una de las garantías básicas exigidas por la jurisprudencia del Tribunal Supremo: establecer previamente las reglas de uso de los medios e informar a los trabajadores. También debe reiterarse la gravedad de la falta de medidas de seguridad que conduce a la divulgación en Internet de ficheros

sensibles de la empresa cuando los empleados utilizan los instrumentos de trabajo para realizar descargas, normalmente utilizando el programa e-mule.

A ello se añade la implantación de mecanismos de denuncia interna ("whistleblowing") que inciden sobre el derecho a la protección de datos de denunciantes y denunciados. Los datos sobre ficheros inscritos en el RGPD apuntan dos tendencias respecto de estos ficheros:

La primera, su incremento progresivo habiéndose alcanzado la cifra de 32 ficheros de los que son titulares, en su mayor parte, grupos multinacionales.

La segunda, la variedad de sectores de actividad en los que se implantan mecanismos de denuncia interna. Entre ellos cabe citar los sectores financiero, de alimentación, transporte, energético, publicidad, turismo y hostelería e industria química y farmacéutica.

Las tecnologías disponibles han incidido también en el ejercicio de derechos tan consolidados como el de la libertad sindical al hacer posible nuevas modalidades de comunicación con los trabajadores en el desarrollo de la acción sindical (intranets corporativas, páginas web abiertas, comunicaciones a través de correo electrónico...).

## 5. La privacidad en un mundo globalizado e interconectado

España no puede ser ajena a la realidad del mundo actual, en el que el crecimiento de los flujos internacionales de información ha multiplicado las solicitudes de autorización de transferencias internacionales de datos. Estos flujos se han acompañado de iniciativas para conseguir fórmulas más flexibles que los faciliten. Así, la prestación de servicios de la sociedad de la información en un mundo globalizado ha hecho preciso reflexionar sobre la necesidad de impulsar estándares internacionales mínimos que permitan garantizar los derechos de los ciudadanos cualquiera que sea el lugar donde residen. Con este motivo, la autoridad española de protección de datos consideró que era el momento de superar la etapa de constatación de las carencias actuales y de poner en marcha iniciativas que permitieran obtener avances tangibles en el logro de esa normatividad internacional. Ello llevó a la presentación en la 30ª Conferencia Internacional de Protección de Datos y Privacidad de los principales parámetros de su propuesta sobre estos estándares. La finalidad última será la de que el texto que se presente a la próxima Conferencia de Madrid pueda ser adoptado por un amplio consenso y sirva de base para, supera-

dos los trámites que resulten necesarios, convertirse en un instrumento internacional de protección de la privacidad y de los datos personales.

## V. CONCLUSIONES

El derecho a la autodeterminación informativa surge como respuesta a la posibilidad de un tratamiento masivo de datos propiciado por la mejora de las tecnologías y la comunicación, factores ambos que han multiplicado la velocidad de ese tratamiento, la capacidad de almacenamiento, y la transmisión de un enorme flujo de información. La legislación española surgida con la intención de afianzar este derecho ha gozado desde el principio de un perfil notablemente garantista, y no ha eludido las exigencias de responsabilidad civil cuando se producen vulneraciones de derechos de los afectados. El camino recorrido hasta el momento por España para robustecer este derecho ha sido, por tanto, el correcto, pero debemos recordar que aún no ha terminado, y que el grado de cumplimiento del derecho aún puede y debe mejorarse sin dejar de considerar a los ciudadanos como la principal prioridad. Ello supone la necesidad de que éstos conozcan los derechos de los que son titulares y estén informados sobre las dudas que se les planteen para el ejercicio de tales derechos, pudiendo hacer uso de los instrumentos preventivos y coercitivos que garanticen su eficacia.

En este sentido, corresponde a los poderes públicos y a la autoridad de protección adquirir el compromiso necesario para la consolidación de la cultura de protección de datos, promoviendo como objetivo estratégico las precisas iniciativas y actuaciones para fomentar la efectiva garantía del derecho fundamental a la protección de datos en ámbitos concretos que merecen atención singular o específica.

La consecución de estos objetivos implica necesariamente un diálogo constante con la sociedad, en cuya interlocución podrán distinguirse dos colectivos específicos: los ciudadanos y los responsables del tratamiento de datos, tanto públicos como privados, como sujetos obligados a actuar conforme al sistema de garantías que establece la normativa de protección de datos personales. Este diálogo deberá ayudar no sólo a incrementar la seguridad jurídica, sino también a alcanzar una mayor simplificación y facilidad del cumplimiento de la normativa de protección de datos para lograr así una sociedad más informada.