Agencia Española de Protección de Datos (AEPD):
Privacidad e Internet

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

1. Datos e identificación del proyecto

Privacidad e Internet son dos principios incontestables que es necesario concertar, dos paradigmas a conservar y equilibrar.

Internet en sus orígenes se constituyó como un entramado que conectaba a un número reducido de computadoras de una red cerrada. Cuando se popularizó, la red conectó personas con máquinas y con otras personas frente a ordenadores. El siguiente paso evolutivo que se realizó fue la consecución de la movilidad: desde hace pocos años, acceder a Internet desde cualquier sitio es mucho más sencillo gracias a los teléfonos móviles avanzados (smartphones) mediante redes 3G o incluso con teléfonos de satélite, para los que no existan las zonas de cobertura. La red deparará más fronteras que el tiempo traspasará como el denominado Internet de las cosas que permitirá almacenar y recuperar datos sobre objetos que se identifican y pueden interactuar. Por ejemplo enviando mensajes sobre la cercanía de una fecha de caducidad o la inexistencia de un producto que alimentará una lista de la compra virtual.

Todos estos avances, aun siendo inestimables, realizan una descripción incompleta del fenómeno si no se eleva la vista y se constata que lo que ha hecho Internet es redescubrir el mundo o, quizá dicho en palabras más exactas, configurar un nuevo mundo. Y el nuevo diseño se ha hecho en gran parte, poniendo en riesgo a la privacidad.

El Premio Nobel Mario Vargas Llosa ha escrito en El País en enero de 2011 lo siguiente:

> *"Tal vez hablar de "vida pública" sea ya inexacto, pues, para que ella exista debería existir también su contrapartida, la "vida privada", algo que prácticamente ha ido desapareciendo hasta quedar convertido en un concepto vacío y fuera de uso".*

> *"La desaparición de lo privado, el que nadie respete la intimidad ajena, el que ella se haya convertido en un espectáculo que excita el interés general y haya una industria informativa que alimente sin tregua y sin límites ese voyerismo universal es una manifestación de barbarie".*

La dilución de la privacidad en la red es un fenómeno incontestable. Pero también un elemento a combatir. Es una realidad, pero que debe ser reconducida buscando un equilibrio que pondere ambos principios.

La moneda de cambio en la red es la información personal. Nuestros datos pagan la red. Incluso en las redes sociales hay quien dice que el usuario no es el cliente sino el poseedor de la mercancía: sus datos.

Todos dejamos rastro cuando usamos Internet a través de una identificación que no es genérica sino que se perfila al individuo que se identifica en las redes sociales, que deja de integrarse en la masa de manera anónima y que permite conocer los gustos y costumbres del usuario y potencialmente enviar publicidad en base al comportamiento.

Junto a ellos, los espacios de comunidad en Internet se presentan al internauta, y generalmente se perciben por éste, como ámbitos relacionales equivalentes a aquellos de los que dispone en el mundo físico. Ello genera una falsa percepción de privacidad.

Las reglas de juego del entorno no las define el usuario. Se somete a unas reglas fijadas por el proveedor de servicios como un contrato de adhesión generalmente ajustado a las reglas de un país diferente del internauta. Son contratos onerosos en los que se aplican reglas del tipo "pay for privacy" que van a autorizar al proveedor a rastrear y configurar perfiles.

Las relaciones no se dan en un entorno neutro, Internet no es la vía pública. El titular del servicio da soporte técnico, registra las sesiones, accede a perfiles, posee en suma o puede acceder a todo el conocimiento que se va generando por cada usuario que queda vinculado por unas reglas configuradas "por defecto" que no suelen favorecer los intereses del usuario.

El usuario difícilmente puede, aunque debiera, conocer las reglas del juego, adquirir los conocimientos técnicos básicos que le permitan desenvolverse en libertad y mantener un absoluto control sobre su información personal y la de terceros. Raramente lee las políticas de privacidad o las modula en aspectos como la limitación de cookies que controlan su "navegación". Junto a ello, la percepción de los ciudadanos muestra desconfianza ante los retos de Internet

El barómetro del Centro de Investigaciones Sociológicas (CIS) de septiembre de 2009 reflejaba que los usuarios creen que Internet es un lugar en que la seguridad y privacidad de sus datos es deficiente, considerando un 56,6% que es baja o muy baja y más del 70% que su uso favorece la intromisión en la vida privada, citándose como servicios que generan mayor desconfianza, las redes sociales, los servicios de mensajería y los chats. En par-

ticular, la inclusión de fotografías o vídeos propios o de familiares o amigos en Internet ofrece para el 76,7% de los ciudadanos poca o ninguna seguridad.

Esta preocupación es mayor respecto de los menores, considerando más del 80% de los ciudadanos que los menores de edad deben tener controles en el acceso a Internet.

La combinación entre privacidad e Internet ha derivado en una panoplia de actuaciones y planteamientos por parte de la Agencia Española de Protección de Datos (AEPD) en tres frentes principalmente que se analizan en el presente caso:

a) **Reactivo. Como consecuencia de las peticiones de los ciudadanos en defensa de sus datos en Internet ejerciendo el denominado derecho al olvido.**
b) **Proactivo. Como Agencia Reguladora delimitando nuevos escenarios y regulaciones.**
c) **Participando en el nuevo debate que plantea Internet entre regulación o autorregulación del sector.**

2. El modelo organizativo

En el marco del sector Administración y Competitividad, la Agencia Española de Protección de Datos y el proyecto de Protección de la privacidad en Internet se encuadran en el grupo denominado *"Administración Digital",* que reúne organizaciones públicas involucradas en procedimientos ligados a la Administración Electrónica y aquellas cuyo objeto sea la producción, tratamiento y difusión digital de información pública de carácter oficial.

Dentro de la *Administración Digital*, la AEPD reviste una singularidad importante: es la única institución independiente creada exclusivamente para la defensa de un derecho fundamental consagrado en la Constitución española (art. 18.4 CE) y a cuyo efecto se le dota de importantes potestades administrativas, como la potestad de inspección y de sanción, entre otras.

Para asegurar la máxima eficacia en la salvaguarda del derecho a la protección de datos, AEPD se constituye como una autoridad independiente —según dispone el artículo 16 del Estatuto de la AEPD aprobado por Real Decreto 428/1993, de 26 de marzo— y especializada.

En tal sentido, desarrolla lo previsto en la Directiva 95/46/CE, del Parlamento 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, que señala en su considerando 62 que "*la creación de una Autoridad de Control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial para la protección del derecho al tratamiento de datos personales".* Asimismo, en el artículo 28 de la Directiva se refiere a que dicha Autoridad de Control deberá tener atribuidos poderes de investigación, de intervención y sancionadores.

La naturaleza y régimen jurídico de la Agencia quedan establecidos en el artículo 35 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), definiéndola como un *ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.* Se relaciona con el Gobierno a través del Ministerio de Justicia.

Tras la Ley 15/1999, de Protección de Datos, el marco de infracciones y sanciones se ha ido ampliando paulatinamente mediante leyes sectoriales posteriores. Así, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) o la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT), atribuyen a la Agencia nuevas competencias para sancionar en el ámbito de esas comunicaciones comerciales, principalmente llamadas telefónicas, fax y correos electrónicos.

Una reciente modificación en 2011 por medio de la Ley de Economía Sostenible ha atenuado el régimen sancionador disminuyendo la cuantía mínima de las sanciones graves (de 60.000 a 40.000 euros) e introduciendo la figura del apercibimiento.

En el ámbito internacional, forma parte desde el inicio del Grupo de Trabajo del artículo 29 creado en la directiva 95/46/CE, que es el órgano consultivo independiente integrado por las Autoridades de Protección de Datos de los Estados Miembros, la Comisión Europea y el Supervisor Europeo de Protección de Datos.

En el ámbito iberoamericano, desarrolla un activo papel desempeñando la Secretaría Permanente de la denominada Red Iberoamericana.

Asimismo, forma parte de los órganos de coordinación a nivel de Director y Subdirector que están compuestos con las tres Agencias autonómicas existentes: Madrid, Cataluña y País Vasco.

3. El papel de la innovación

La Agencia Española de Protección de Datos ha tenido que regular y diseñar una estrategia innovadora partiendo de la existencia de un régimen legal huérfano de previsiones específicas sobre múltiples problemas que crea Internet.

Internet ha desarrollado servicios que son utilizados masivamente por media humanidad. Los prestadores de estos servicios en su actividad inciden en la privacidad de los usuarios a través de dos factores: La fijación unilateral de las condiciones de uso y privacidad y el propio modelo de negocio que los sustenta.

La fijación unilateral de las condiciones de uso y privacidad afecta a la información que reciben los usuarios —que resulta insuficiente en cuanto a su claridad y accesibilidad—, a las finalidades del tratamiento de los datos y a sus plazos de conservación. Así, la retención de las búsquedas que realiza cada persona en un buscador dependerá de la decisión de

éste de la misma manera que el uso de los ingentes datos vertidos en cada red social puede ser teóricamente utilizado por el titular de la misma.

El modelo de negocio repercute en la privacidad por ser, en términos generales, servicios gratuitos que se financian con ingresos publicitarios. Lo que ha generado estrategias cada vez más desarrolladas para conocer los hábitos de los usuarios, elaborar perfiles de ellos y personalizar la publicidad que se les ofrece.

La actuación de la Agencia se ha desarrollado en un triple ámbito.

a) Reactivo. Como consecuencia de las peticiones de los ciudadanos en defensa de sus datos en internet: derecho al olvido

Los ciudadanos reclaman cada vez con mayor intensidad la posibilidad de ejercer un control sobre sus datos personales en la Red, incluido el derecho a no figurar en ella, conscientes de que, salvo que confluyan derechos prevalentes, cada persona debe poder decidir sobre la información que sobre ella existe en Internet.

El incremento de las consultas sobre cómo desaparecer de Internet y sobre el ejercicio de los derechos de cancelación y oposición —instrumentos de autodefensa que le otorga la LOPD— acredita la intensidad de esta demanda.

El origen de estas reclamaciones se encuentra en la publicación de datos personales en boletines y diarios oficiales, medios de comunicaciones digitales, sentencias y otros sitios web.

Es el ciudadano en todos estos casos el que proactivamente se dirige en defensa de su privacidad, actuando la Agencia únicamente en el supuesto en que, tras considerar su pretensión insatisfecha, reclame su tutela.

Pero la Agencia ha de dar respuesta a varias cuestiones, principalmente ¿A quien deberá dirigirse el ciudadano y, si no se atienden sus pretensiones, la Agencia? ¿al responsable de la página donde se ubica el dato (webmaster) o al buscador solicitando que se cancelen los datos o se evite su indexación por los buscadores (al que coloca el "objeto" en el escaparate o al que mira)?

La Agencia se ha dirigido al buscador o al webmaster en función de lo que haya pedido la persona afectada. Y en ambos casos se han instado actuaciones. Esto es, si el ciudadano se ha dirigido a ambos, se insta al buscador a evitar la captación de la información en decenas de resoluciones que han sido recurridas en vía judicial por Google alegando ausencia de jurisdicción de la AEPD, censura administrativa y que tendría que ser el webmaster el que suprimiera el dato.

Pero también la Agencia tuvo que plantearse qué hacer en el caso de los webmaster: decidir si requerían un tratamiento diferente tres categorías por la concurrencia de otros derechos a sopesar, lo que derivó en tres situaciones distintas:

a) **Hemeroteca o prensa digital** accesible a través de Internet (por ejemplo, noticia de una detención hace años de una persona posteriormente absuelta, matrícula de un coche en una fotografía...) El alcance y relevancia de la libertad de prensa limita el carácter coercitivo de la Agencia, que se limitó a transmitir al medio la conveniencia de reflexionar acerca de si resulta relevante en la actualidad el mantenimiento del dato en la red (recomendación).

b) **Diarios o Boletines Oficiales** (por ejemplo, referencia a indultos, subvenciones o sanciones administrativas con identificación). La obligación de publicidad del Boletín es inalterable, por lo que se insta a que adopten medidas técnicas para evitar que el buscador capte la información (se trata de un Protocolo Standard denominado robots TXT).

c) **Blogs, chats o páginas no vinculadas a libertad de prensa**. Se insta el borrado de la información.

b) Proactivo. Como Agencia Reguladora delimitando nuevos escenarios y regulaciones

La Agencia Española ha actuado a iniciativa propia —simultáneamente— en un triple sentido:

- Generador: impulso de regulación internacional.
- Negociador: coordinación con los principales prestadores de servicios de Internet.
- Reparador: investigación por propia iniciativa de posibles infracciones.

b) 1. Vertiente generadora: Estándares Internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal.

La AEPD organizó en 2009 la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, el mayor foro dedicado a la privacidad a nivel mundial y punto de encuentro privilegiado entre autoridades de protección de datos y garantes de la privacidad de todo el planeta, así como de representantes de entidades públicas, privadas y de la sociedad civil.

El mayor logro resultó la consecución de su objetivo prioritario: avanzar hacia la consecución de un instrumento legal, universal y vinculante en materia de privacidad que contribuyera a una mayor protección de los derechos y libertades individuales en un mundo globalizado concitando el más amplio consenso institucional y social.

La Conferencia adoptó, mediante la denominada *"Resolución de Madrid",* el primer gran paso en esta línea: la *"Propuesta conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con Tratamiento de Datos de Carácter*

Personal", que insta a todas las autoridades participantes a implementar y difundir a nivel tanto nacional como internacional.

La Propuesta Conjunta pretende ofrecer un modelo de regulación de la privacidad en Internet que garantice un alto nivel de protección y que, al mismo tiempo, pueda ser asumido en cualquier país con las mínimas adaptaciones necesarias en función de las diversas culturas jurídicas, sociales o económicas propias de cada región. Del mismo modo, la Propuesta buscaba facilitar el flujo de datos personales a nivel internacional —circunstancia inherente a Internet— tratando de mitigar los obstáculos, costes y retrasos existentes, que generan desequilibrios desde el punto de vista de la competencia.

No se trata de un acuerdo internacional ni de una normativa jurídicamente vinculante. No obstante, su valor y relevancia como texto de referencia deriva de la amplia participación de la comunidad internacional de protección de datos y privacidad en su elaboración y génesis y del hecho de que recoge elementos que están presentes en todos los sistemas vigentes de protección de datos actualmente en vigor y, finalmente, de que ha sido respaldada por todas las Autoridades integrantes de la Conferencia Internacional. De este modo, la propuesta se configura no sólo como la base para la futura elaboración de un Convenio universal vinculante, sino como la herramienta de indudable utilidad para el desarrollo normativo e institucional en aquellos países en los que la protección de datos no se encuentre todavía convenientemente implementada.

Una de las prioridades de la AEPD durante los meses siguientes fue la promoción y difusión de este texto entre entidades privadas, expertos y organismos públicos nacionales e internacionales. Esta difusión se ha llevado a cabo a nivel institucional y empresarial y ha conducido, por ejemplo, a que varias empresas multinacionales hayan incluido los Estándares como referente en sus políticas globales de privacidad.

El Congreso de los Diputados y el Senado aprobaron por su parte sendas iniciativas parlamentarias reconociendo la propuesta de estándares como una base adecuada para avanzar hacia un instrumento internacional vinculante e instando al Gobierno a promoverlo en la Unión Europea, la Comunidad Iberoamericana y las organizaciones internacionales más relevantes. A título de ejemplo, la Ley de Protección de Datos de Méjico, aprobada en julio de 2010, menciona específicamente estos Estándares como base para su normativa.

b) 2. Vertiente negociadora: Intercambio periódico de relaciones con los principales prestadores de servicios de Internet.

Intercambio a menudo informal mediante reuniones de clarificación de posturas pero también frecuentemente por medio de comunicaciones formalizadas.

Así, en el mes de abril de 2010 la AEPD, junto con nueve Autoridades de diversas áreas geográficas, dirigieron una carta conjunta a Google Inc. manifestando su preocupación por el olvido de la protección de datos en el despliegue de nuevas aplicaciones tecnológicas.

En particular, destacaban las amenazas para la privacidad de la red social Google Buzz en la que se asignaron automáticamente y sin información previa a los usuarios una red de "seguidores" entre las personas con las que habitualmente mantenían correspondencia electrónica a través de email.

Las Autoridades europeas asimismo reiteraron la necesidad de limitar el período de conservación de las búsquedas en Internet al plazo de seis meses, comunicándolo a Google, Microsoft y Yahoo.

También en 2010 las Autoridades europeas de protección de datos comunicaron a los responsables de Facebook su rechazo a la modificación unilateral llevada a cabo en la configuración de la política de privacidad que ampliaba el acceso a los datos de un usuario por parte de terceros, incluso aunque hubieran elegido una política de privacidad más restringida.

Las citadas autoridades se dirigieron, además, a los responsables de otras redes sociales insistiendo en que el acceso a los perfiles informativos y los contactos de cada usuario debe limitarse a los que selecciona y que otros accesos más amplios deben ser una opción explícita del usuario.

b) 3. Vertiente reparadora: Investigación de posibles infracciones

La AEPD inició de oficio un procedimiento sancionador a Google Inc y Google Spain por la captación y almacenamiento de datos de localización de redes inalámbricas abiertas (redes Wi-Fi) y de datos de tráfico transferidos a través de ellas por los vehículos utilizados para obtener imágenes de la vía pública para el servicio Street View.

El procedimiento imputó a Google Inc. la presunta comisión de dos infracciones de la LOPD, como responsable del servicio y del diseño del software de recogida de los datos y a Google Spain como responsable de su captación y almacenamiento en España y su transferencia a los Estados Unidos de Norteamérica.

También se han realizado actuaciones de inspección en la red social Facebook y en My Space solicitando información sobre si se han visto afectados usuarios en España en la transmisión de datos tales como los nombres de los usuarios y de sus amigos por parte de algunas de las aplicaciones más populares programadas sobre tales plataformas a anunciantes y otras empresas.

c) Participando en el nuevo debate que plantea Internet entre regulación y autorregulación

Se puede decir que, en ocasiones, los empresarios de Internet —ante un marco todavía pendiente de consolidación— se encuentran ante un dilema que deben despejar: ¿pedir perdón o pedir permiso?

Los emprendedores en Internet no pueden ni deben dejar de aprovechar las oportunidades que les ofrece el nuevo mundo de la Tecnología en la Red. Es evidente que el progreso en la Red únicamente tiene lugar a golpe de iniciativa, de impulso personal y empresarial. Pero también es cierto que tales iniciativas se encuentran abocadas a "navegar" en un entorno de relativa desregularización en la que, a pesar de ello, sus decisiones no pueden encallar.

Mark Zuckerberg —CEO de Facebook— en una reunión del G-8 debatía sobre el poder transformador de Internet y la necesidad de evitar la regulación sobre un Internet sin restricciones. No únicamente por la situación en la que se encuentra Internet, sino como consecuencia de su percepción de qué es lo que la sociedad necesita para fomentar el espíritu emprendedor, el crecimiento y la innovación. Ya existen, según planteaba, muchos mecanismos de autorregulación para construir y mantener la confianza en Internet (eBay, Amazon y Wikipedia son buenos ejemplos) lo que la convierte en una alternativa real para avanzar. El vicepresidente de la unidad publicitaria de Microsoft completaría el argumento lanzando un serio aviso, "si no nos autorregulamos, alguien lo regulará por nosotros".

Frente a esta tesis, el presidente Sarkozy planteó en la misma sede la necesidad de avanzar hacia un marco regulador eficaz.

Detrás de este dilema se encuentran algunas consideraciones que en ocasiones subyacen en el imaginario de la comunidad de Internet:

- Las TIC van muy por delante del Derecho: nunca va poderse regular Internet. Los intentos que se hagan llegarán tarde y colisionarán con una realidad tecnológica obcecada que desbordará una norma que devendrá en inaplicable en aspectos como privacidad o propiedad intelectual.

- El usuario "ha consentido". Otorga al navegar en Internet su consentimiento tácito para el uso de sus datos que a veces es expreso al confirmar con un clic las condiciones de privacidad que le presenta el prestador de servicios.

- El mercado "necesita procesar información libremente", por lo que los datos personales deberían tender a fluir libremente.

- Es imposible ponerle puertas al campo...

- El Derecho regula "relaciones sociales" y debe tender a adaptarse a Internet, no viceversa. En Internet es el programador el que regula y el usuario el que elegirá en función de los servicios que se le presenten en un régimen de competencia perfecta en el que sobrevivirán únicamente aquellos que mayor confianza inspiren.

- Internet es la nueva democracia y cualquier restricción que se implemente supondría una práctica asimilable a la censura. El Derecho adquiere un claro perfil trasnacional. En su ausencia, y siendo previsible que transcurran años hasta la existencia de un régimen internacional consolidado, consensuado y vigente, no cabe sino la autorregulación.

En este entorno incierto, en línea con lo afirmado por el Presidente Sarkozy, son varias las iniciativas normativas que intentan regular el fenómeno.

Pero lo cierto es que la realidad tecnológica resulta huérfana de una legislación específica que prevea cada situación, por lo que resulta plenamente vigente el reto de la empresa tecnológica de decidir como actuar en cada momento. Supuestos en que la tecnología abre nuevos mundos en el nuevo mundo sin regulación expresa y explícita.

Así ocurre con el *cloud computing* o "informática en la nube", cuyas aplicaciones se utilizan sin estar instaladas en el ordenador del usuario y cuyos archivos también se almacenan en la red. Documentos albergados en la red de rápido acceso sin necesidad de guardarlos en el ordenador.

Lo mismo ocurre con relación al denominado *"Internet de las cosas"*. Se trata de colocar sensores y sistemas de transmisión de la información en todo tipo de objetos con los que interactuamos en la vida cotidiana. Las cosas pueden así identificarse, comunicarse entre ellas, o enviar información o datos con propósitos muy diversos.

Todo ello ha derivado en la eclosión de conceptos empresariales que complementarán un marco normativo incapaz de dar en tiempo real todas las respuestas que el empresario demanda.

Es el caso del *privacy by design* o *"privacidad por diseño",* caracterizado por la necesidad de que la empresa acometa medidas proactivas en vez de reactivas, que anticipe y prevenga eventos de invasión de privacidad antes de que ocurran. *PbD* no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron: su finalidad es prevenir que ocurran.

Privacidad por Diseño pretende llegar antes del suceso, no después, y significa que cuando haga uso de un producto el consumidor debe encontrarlo preconfigurado con los máximos estándares de privacidad. Hoy, muchas veces tiene que cambiar las preferencias si desea más privacidad, y a veces es muy complicado. Se daría la vuelta al planteamiento: quien quiera revelar más información sobre uno mismo tendrá que cambiar a propósito las preferencias. El ciudadano debe tener derecho a decidir cuan visible quiere ser y esa decisión no debe impedir que accedan a determinados servicios.

Se crea, por tanto, una estructura conceptual que focaliza en el empresario su tarea de analizar los riesgos sobre la privacidad. Es un concepto parecido al principio que, en paralelo y en la misma línea, se introduce en el mundo anglosajón conocido como *"accountability",* que podría traducirse aunque inexactamente como "rendición de cuentas".

En definitiva, como afirmó el CEO de Vodafone ante el dilema planteado entre regulación y autorregulación: ¿y si tienen razón ambos?

4. La cultura corporativa

El contexto que determina la cultura organizativa en la que nace y actúa la AEPD es la protección constitucional de los derechos fundamentales. Su misión marca así la forma de organizarse y funcionar y la orientación de los proyectos que desarrolla la Agencia.

La Constitución Española, en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos.

La intuición del Constituyente se ha confirmado. El progresivo desarrollo de las técnicas de recolección, almacenamiento y acceso a datos ha expuesto la privacidad, en efecto, a una amenaza potencial antes desconocida.

Surge el concepto de privacidad que es más amplio que el de intimidad: La intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí por medios informáticos, arrojan como precipitado un retrato de la personalidad del individuo que tiene derecho a mantener reservado.

Era preciso, pues, delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada e indiscriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, lo que se conoce como privacidad.

El derecho a la protección de datos comparte con el derecho a la intimidad el objetivo de ofrecer una eficaz protección de la vida privada personal y familiar.

No obstante, las principales diferencias se centran en dos aspectos Por una parte, el derecho a la intimidad sólo comprende dentro de su ámbito los datos de la vida íntima. El objeto del derecho a la protección de datos abarca, no sólo a los llamados datos íntimos de la persona, sino también a cualquier otro tipo de dato personal, sea o no íntimo, esto es, sea público o privado, que pueda ser conocido o empleado por terceros.

En segundo lugar, se encuentra el contenido. El derecho a la intimidad supone conferir a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido; mientras que el derecho a la protección de datos, por su parte, supone la atribución a su titular de un conjunto de facultades que no se contienen en el derecho fundamental a la intimidad, que puede ejercitar frente a todo tercero que posea datos públicos o privados

suyos, y que sirven para garantizar a la persona un poder de control sobre sus datos personales. Tales facultades se materializan en lo que se conoce como los derechos "A.R.C.O." los derechos de acceso, rectificación, cancelación y oposición, derechos que deberán poder ser ejercidos de un modo gratuito por todo titular de datos personales.

De todo lo dicho, podemos concluir que el contenido del Derecho Fundamental a la Protección de Datos consiste en el poder que tiene toda persona física de disponer y controlar sus datos personales —cuenta corriente, numero de teléfono, domicilio, imagen...— lo cual le faculta para decidir cuáles proporcionar a un tercero, 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 salvo justificación legal.

Para garantizar su respeto, la AEPD desarrolla numerosas funciones recogidas en la LOPD.

- Genérica de salvaguarda y tutela, consistente en velar por el cumplimiento de la legislación de protección de datos.
- Informe de disposiciones que pueden incidir sobre la privacidad.
- Informativa, dando publicidad a los ficheros inscritos en el Registro General de Protección de Datos e informando a los particulares acerca de sus derechos en el campo de protección de datos.
- De Cooperación Internacional.
- Inspectora, que le permite recabar de los responsables de los ficheros cuanta información considere necesaria. El artículo 40 de la LOPD configura expresamente una potestad de inspección sobre los ficheros contemplados en la Ley.
- Represiva, mediante el ejercicio de la potestad sancionadora.

En los primeros años de actividad de la Agencia Española de Protección de Datos, las actividades de inspección e instrucción se basaron de forma exclusiva en el ámbito normativo delimitado por la LOPD y sus normas de desarrollo.

Posteriormente, dos leyes: la LSSI y la LGT, establecen nuevas competencias a asumir por la AEPD, centradas en la competencia sancionadora en el ámbito de las comunicaciones comerciales en formato electrónico.

5. Configuración Organizativa

La AEPD es un órgano independiente constituido como un Ente de Derecho Público que se rige por el Real Decreto 428/1993, de 26 de marzo, que aprueba su Estatuto. Como prevé la LOFAGE en su disposición adicional décima, se regirá por su legislación específica (Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal) y supletoriamente por la LOFAGE. El régimen jurídico propio de la Agencia no establece, sin embargo, una independencia funcional o una especial autonomía respecto de la Administración General del Estado, rigiéndose por su normativa específica en los aspectos precisos para hacer plenamente efectiva dicha independencia o autonomía.

A tal efecto, el Estatuto de la Agencia, en su artículo 14, señala que el Director de la Agencia gozará de los mismos honores y tratamiento que los Subsecretarios, teniendo su mandato una duración prevista de 4 años. Su nombramiento corresponde al Gobierno, a propuesta del Ministro de Justicia. El Director no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna, y su cese se realiza por el Gobierno, previa constatación del cumplimiento de una serie de causas tasadas y la instrucción del correspondiente expediente. El cargo de Director de la Agencia Española de Protección de Datos está sujeto a las incompatibilidades que para los altos cargos prevé la Ley 25/1983, de 26 de diciembre.

En la **estructura orgánica** básica de la AEPD se distinguen los siguientes órganos:

- El Director

- El Consejo Consultivo encargado de asesorar al Director y compuesto por un Diputado, un Senador, un experto nombrado por el Consejo Superior de Universidades y un representante de la Administración Central, Administración Local, Real Academia de Historia, usuarios y consumidores, de cada Comunidad Autónoma que haya creado Agencia de Protección de Datos y del sector de ficheros privados.

- Tres unidades con rango de subdirección general: El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia.

El Presupuesto de la Agencia para 2011 asciende a 14.437.970 millones de euros y sus efectivos a 156 personas en plantilla.

6. Estrategia

La Misión de la AEPD cabe conjugarla bajo los siguientes objetivos:

Generar un diálogo permanente con la Sociedad.

Uno de los aspectos más relevantes para la Agencia Española de Protección de Datos es la necesidad de extender y consolidar en la sociedad la cultura de protección de los datos personales como un objetivo estratégico.

La consecución de este objetivo implica necesariamente un diálogo constante con la sociedad en el que pueden 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 comprende un abanico de objetivos entre los que necesariamente se incluyen los de promover un mayor conocimiento de sus derechos por parte de los ciudadanos, incre-

mentar la seguridad jurídica para los sujetos obligados, simplificar y facilitar el cumplimiento de la normativa de protección de datos y alcanzar una sociedad más informada.

Este diálogo se articula, fundamentalmente, a través de consultas, de la emisión de informes que den respuesta a las consultas planteadas por los responsables del tratamiento y de reuniones bilaterales dirigidas a anticipar los criterios que posibiliten un desarrollo lícito de sus actividades.

Para ello, es necesario mantener contactos con las empresas y asociaciones del sector de las telecomunicaciones y servicios de la sociedad de la información; el sector financiero, donde merece una mención específica el desarrollo de nuevos servicios que faciliten a los ciudadanos la protección frente al fraude; el sector asegurador y el de publicidad y marketing directo, además de otros sectores como el de la automoción, o los nuevos servicios que se están desarrollando en el aseguramiento sanitario privado vinculados a la historia clínica electrónica.

Junto a ello, debe destacarse la importancia de una ambiciosa política de comunicación en la AEPD, dirigida a conseguir una mayor proximidad con los medios de comunicación, posibilitando la difusión de temas de actualidad.

La defensa del derecho.

Impulsar el diálogo con la sociedad no excluye, sino que tiene su complemento en el restablecimiento o sanción por el cumplimiento de la norma en caso de infracción. El restablecimiento del derecho se posibilita tutelando el incorrecto ejercicio de los derechos de acceso, cancelación, rectificación u oposición tras solicitud del afectado. La sanción tiene su amparo en uno de los regímenes de infracciones y sanciones más severos del ámbito comparado —a pesar de la reciente atenuación— ampliado con las modificaciones normativas sectoriales que han conferido a la Agencia competencia en materia de comunicaciones comerciales.

La prevención como elemento clave.

La AEPD ha desarrollado una intensa actividad preventiva basada, fundamentalmente, en la realización de inspecciones sectoriales de oficio a través de las cuales se han auditado diversos sectores de actividad en el tratamiento de datos personales, tanto privados como públicos.

La proyección internacional del derecho a la protección de datos.

La AEPD encuentra en Internet un nuevo espacio no territorial en el que debe desarrollar una intensa actividad. Para ello actúa en varias dimensiones: concibe o participa en la generación de un nuevo marco normativo, lidera proyectos dirigidos a países hoy incorporados

a la Unión Europea para colaborar en su adecuación al acervo comunitario e impulsa la actividad en Iberoamérica de Protección de Datos.

7. Conclusiones

El análisis de la actuación de la AEPD en Internet en aras a la protección de la privacidad permite obtener algunas conclusiones especialmente relevantes en el ámbito de la competitividad.

Uno de los elementos relevantes es que la protección de los datos y la privacidad no puede esperar a que entre en vigor una hipotética y futurible regulación internacional que incluya respuestas exhaustivas y uniformes a cada problema. La Agencia debe defender los derechos de los ciudadanos combinando actividades de regulación con otras de interpretación del régimen legal vigente.

Al mismo tiempo, el empresario no debe sacrificar iniciativa en aras de privacidad o viceversa. Las organizaciones deberán crear sistemas que desde su inicio garanticen ambas y las equilibren.

Esto, en definitiva, constituye al sector empresarial en corresponsable en la definición de la actuación en el marco de Internet cuya implementación se convierte en una suerte de cogestión público-privada que supera los rígidos esquemas de obediencia debida de la normativa existente.

También Internet, en consecuencia, ha descubierto un nuevo mundo en las formas de relación entre el sector público y el sector privado, que deben colaborar en la configuración de sus reglas de funcionamiento y cooperar en la definición de mecanismos y fórmulas que garanticen la privacidad. La empresa debe complementar, por lo tanto, un ejercicio de autoridad pública de la Administración que queda de esta forma relativizado.

8. Clave de éxito del proyecto

La clave del éxito del proyecto de la AEPD en Internet se basa en varios factores:

- Proactividad en las decisiones y valentía política.
- Sensibilidad social por el problema y correspondiente repercusión en los medios de comunicación.
- Pedagogía de las resoluciones de la Agencia, sean sancionadoras o no.

La misión de la Agencia de defender los derechos de los ciudadanos ha encontrado una complejidad adicional con la aparición de nuevos desafíos como consecuencia de las nuevas tecnologías y en especial Internet. Cuestiones como el denominado *"derecho al olvido"* adquieren crecientes cotas de sensibilidad social por el mero hecho de que todo ciu-

dadano es un afectado real o potencial al ver algún contenido de su vida indexado tras introducir su nombre en un buscador y verse condenado a vagar permanentemente en la *Red.*

Internet es irrenunciable. Pero también la privacidad es irrenunciable. Y es del reto que supone la necesidad de combinar ambos axiomas y de la firmeza de las reacciones de la Agencia —en gran parte sostenido en un firme régimen sancionador— de donde ha derivado el éxito del proyecto.