ANA - ALEX
07-12-11
3.6.10
AMORE
rmen Y Miguel.

CARLOS GARRIDO FALLA

Protección de datos y acceso a ficheros públicos

El derecho fundamental a la protección de datos de carácter personal

La Constitución Española de 1978 establece en su artículo 18.4 que "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Posteriormente llegaría la Ley 5/1992 de Ordenación y Regulación del Tratamiento Automatizado de Datos, de 29 de octubre (LORTAD) que desarrolla inicialmente la previsión del artículo 18.4 de la Constitución Española, ley que estuvo vigente hasta 1999, al ser derogada por la Ley 15/1999 de Protección de Datos de Carácter Personal (en adelante LOPD), actualmente vigente.

La LOPD, deroga, en consecuencia, a la LORTAD y transpone la Directiva Comunitaria 95/46/CE, siendo objeto de desarrollo reglamentario, a través del Real Decreto 1720/2007, de 21 de diciembre.

El Tribunal Constitucional ha abordado el análisis de los datos desde diferentes perspectivas, partiendo siempre de la premisa básica del respeto a la dignidad de la persona. Una de las primeras Sentencias del Tribunal Constitucional sobre esta materia fue la ST 110/1984; en esta sentencia el Tribunal pone de manifiesto que "el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del

Carlos Garrido Falla
Agencia Española de Protección de Datos
E-mail: cgf@agpd.es

aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad de las personas".

Por otro lado, las sentencias 290/2000 y 292/2000 contribuyen a definir de manera clara y contundente el contenido del derecho fundamental a la protección de datos; así establece: "(...) El contenido del derecho a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso...", y también que "Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular".

Por otro lado, la propia Sentencia reconoce que no se trata de un derecho ilimitado, sino que también expresamente reconoce que "(...) el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los poderes públicos para su determinación como ha hecho con otros derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución. Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE".

En conclusión, estamos hablando de un derecho constitucional, siendo considerado así también por la Constitución Europea aprobada el 18 de junio de 2003.

La Agencia Española de Protección de Datos: naturaleza jurídica

El art. 35 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), establece que "La Agencia de Protección de Datos es 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".

Por su parte, el Real Decreto 428/1993, de 26 de marzo, que aprueba el Estatuto de la Agencia de Protección de Datos (en lo sucesivo EAPD), completa la descripción de la naturaleza jurídica que realiza el citado art. 15 de la LOPD, señalando en su art. 1 que se trata de un ente público de los previstos en el art. 6.5 del Real Decreto Legislativo 1091/1988, de 23 de septiembre, que aprueba el Texto Refundido de la Ley General Presupuestaria.

Del marco normativo señalado en el párrafo anterior, se deduce la primera característica que identifica la naturaleza jurídica de la AEPD. Se trata de un Ente Público que continuará rigiéndose por su legislación específica y, supletoriamente, por la Ley de Organización y Funcionamiento de la Administración General del Estado.

El art. 1.2 del EAPD dispone que la Agencia actúa con plena independencia de las Administraciones Publicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

Régimen jurídico aplicable

En el apartado anterior, que hemos dedicado a delimitar la peculiar naturaleza jurídica de la AEPD, ha quedado especificado que la misma se regirá, con carácter preferente, por su normativa específica.

Pasemos ahora a pormenorizar cuáles son los regímenes jurídicos de los diferentes ámbitos de actuación.

El art. 35 de la LOPD va enumerando los diferentes ámbitos de la siguiente manera:

- En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la LOPD y sus disposiciones de desarrollo, actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- En sus adquisiciones patrimoniales y contratación se regirá por el derecho privado.
- El régimen del personal que presta servicios en la AEPD, será el previsto en la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública y demás disposiciones de desarrollo, cuando se trate de funcionarios públicos, y, cuando se refiera a personal contratado, por el Convenio Único para el personal laboral de la Administración General del Estado, aprobado por Resolución de la Dirección General de Trabajo de 24 de noviembre de 1998.
- Desde el punto de vista del Derecho Presupuestario, la AEPD incorpora su presupuesto dentro de los Presupuestos Generales del Estado.
- La contabilidad de la Agencia se ajusta al Plan General de Contabilidad Pública, aprobado por Orden Ministerial de 6 de mayo de 1994.

Estructura y funciones

Estructura orgánica

La estructura orgánica básica de la AEPD se establece en el art. 11 de su Estatuto, que distingue los siguientes órganos:

- El Director.
- El Consejo Consultivo.
- El Registro General de Protección de Datos.
- La Inspección de Datos.
- La Secretaría General.

Además, para el ejercicio de sus funciones el Director de la AEPD es asistido por una Unidad de Apoyo integrada por el Adjunto al Director y el Gabinete Jurídico.

Haremos una mención sucinta de las funciones del Órgano máximo representante de la Agencia.

El Director de la Agencia

A tenor del art. 36 de la LOPD, dirige y ostenta la representación de la Agencia ejerciendo sus funciones con plena independencia y objetividad. El Director de la AEPD, con rango de Subsecretario, desempeña su cargo con dedicación absoluta, plena independencia y total objetividad. No estará sujeto a instrucción de autoridad alguna. Deberá oír al Consejo Consultivo en aquellas propuestas que este le realice en el ejercicio de sus funciones.

En el EAPD (art. 12), se distinguen las funciones de dirección, en las que el Director dictará las resoluciones e instrucciones que se requieran en relación con las competencias que corresponden a la Agencia. Entre ellas, destacan las siguientes:

- Procedencia o improcedencia de las inscripciones en el RGPD.
- Requerimientos a los responsables de los ficheros de titularidad privada para que subsanen deficiencias de los códigos-tipo.
- Procedencia o improcedencia de la denegación del acceso a algunos ficheros automatizados.
- Autorización o denegación de transferencias internacionales de datos a países con un nivel de protección no adecuado.
- Adopción de medidas cautelares y acuerdos de iniciación en relación con el ejercicio de la potestad sancionadora respecto a responsables de ficheros privados.

- Solicitud de incoación de expedientes disciplinarios contra los responsables de ficheros públicos.
- Autorización de entrada en los locales en que se hallen los ficheros con el fin de proceder a las inspecciones que resulten pertinentes.

Ámbito de aplicación de la LOPD

El artículo 1 de la LOPD señala que "La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

Su artículo 2 delimita que "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado".

En función de lo anterior, esta normativa NO se aplica a:

a) Personas jurídicas:
La Ley se aplica a personas físicas. Ergo, a sensu contrario, no es de aplicación la Ley Orgánica 15/1999 al caso relativo al tratamiento de datos de una empresa o persona jurídica o autónomo o a personal de contacto de la misma, entendiendo por tal las personas que ostentan un cargo directivo que representa a la empresa (Director General, Administrador, Gerente, etc.) y siempre que el dato se utilice en su condición de tal.

b) Datos de fallecidos:
En relación con los datos del fallecido, cabe decir que si el derecho fundamental a la protección de datos es considerado como el derecho del individuo a decidir sobre el poder de disposición y control sobre sus datos, es evidente que dicho derecho desaparece con la muerte que extingue la personalidad jurídica del fallecido. Por ello, los tratamientos de datos de personas fallecidas no están comprendidos dentro del ámbito de aplicación de la LOPD, por lo que, en relación a la posible cesión o tratamiento de los datos del mismo, estos no se encontrarían amparados por la citada Ley Orgánica.

No obstante, la AEPD viene admitiendo que los familiares de los fallecidos ejerciten el derecho de acceso a su historial clínico, de conformidad con lo prevenido en la Ley de Autonomía del Paciente.

Asimismo, el nuevo Reglamento 1720/2007, de 21 de diciembre, permite también que las personas vinculadas familiarmente al fallecido

pueden notificar al responsable del fichero el fallecimiento con la finalidad de perseguir la cancelación de los datos de aquel del fichero, sin que ello suponga un posterior derecho a ser tutelado por la AEPD.

c) Procedimientos de disociación:
Según dispone el artículo 3 apartado f) de la LOPD, se denomina procedimiento de disociación a todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

En este sentido, cuando no es posible determinar la persona física que se encuentra detrás de un determinado conjunto de datos, estos no pueden ser considerados datos personales y, en consecuencia, no se aplica la LOPD.

d) Libros de bautismo:
Siguiendo el criterio marcado por la jurisprudencia del Tribunal Supremo (STS), los Libros de Bautismo no constituyen ficheros en los términos en que se consideran por la Ley Orgánica 15/1999 y, además, tampoco cabe estimar aplicable el art. 4.3 de la citada Ley, relativo a la exactitud y veracidad en cada momento de los datos, motivo por el que se instaba la anotación marginal en los Libros de la Iglesia.

Esta jurisprudencia ha sido ya recogida en la sentencia de la Audiencia Nacional, de 22 de octubre de 2008.

Por todo ello, cabe concluir que la Agencia no es competente para resolver la cuestión relativa a la cancelación de datos de los libros de registro de bautismo, al no resultar de aplicación la Ley Orgánica 15/1999, de protección de datos de carácter personal, en los términos y con los argumentos contenidos en la sentencia del Tribunal Supremo de 19 de septiembre de 2008.

La Agencia Española de Protección de Datos presentó recurso de amparo ante el Tribunal Constitucional, que también ha sido rechazado, por lo que el criterio interpretativo del Tribunal Supremo sigue hoy vigente.

e) Ficheros de juzgados o tribunales:
Tampoco se aplica a actuaciones realizadas por un Juzgado o un Tribunal. En consecuencia, deberán dirigirse las reclamaciones en este sentido al Consejo General del Poder Judicial, que es el Organismo competente para conocer sobre el régimen de protección de datos personales contenidos en ficheros públicos de los juzgados, conforme ha dictaminado el Tribunal Supremo en sentencia de 2 de diciembre de 2011.

Por el contrario, SÍ se aplica a:

a) Datos de menores de edad:
Se plantea la licitud del procedimiento referido a la recogida de datos de personas menores de edad, En este sentido, debe señalarse como regla general que las disposiciones de la Ley serán aplicables por igual, con independencia de la mayoría o minoría de edad de los afectados.

Ello no obstante, deberá analizarse en especial la prestación del consentimiento, exigido por la Ley para que el tratamiento de los datos sea conforme a Derecho, tal y como dispone el artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Este consentimiento habrá de ser, tal y como exige el artículo 3.i) de la propia Ley, libre, específico, inequívoco e informado, siendo necesario el cumplimiento de lo preceptuado por el artículo 5.1:

> "Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
> a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.
> b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
> c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
> d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
> e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

Lo que se ha venido indicando hasta ahora es predicable de cualquier tratamiento consistente en la recogida de datos de carácter personal de cualesquiera personas. Sin embargo, en el supuesto de que las personas de las que se obtienen los datos son menores de edad, será necesario analizar en qué supuestos se considerará que los mismos ostentan pleno discernimiento para prestar ese consentimiento y en cuáles aquel habrá de completarse con el de su representante legal.

Según dispone el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, que desarrolla la LOPD, podrá procederse al tratamiento de los datos de los mayores de 14 años con su consentimiento, salvo para aquellos casos en que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de 14 años se requerirá siempre el consentimiento de los padres o tutores.

En ningún caso podrán recabarse datos del menor que permitan obtener información sobre los demás miembros del grupo familiar o sobre las características

del mismo, como actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

La pérdida de la custodia no implica la de la patria potestad. Los parientes separados siguen teniendo los mismos derechos sobre sus hijos menores.

b) La imagen:

Otra de las cuestiones debatidas es la referida a la consideración de la imagen personal como dato personal. No cabe duda que la imagen, en el aspecto fisiológico, debe ser considerado como un dato personal ya que en todo caso te hace persona identificada o identificable Más aún, la grabación de imágenes por medio de videocámaras de vigilancia, tanto de naturaleza pública como privada se deben considerar como la captación de un dato personal y por lo tanto objeto de protección por la LOPD y normativa de desarrollo.

El artículo 3.a de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos Personales define dato personal como "cualquier información concerniente a persona física identificada o identificable".

Por otro lado, el artículo 3.c define el tratamiento de datos como "Operaciones y procedimientos técnicos de carácter automatizado o no, que permita la recogida, grabación conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones consultas, interconexiones y transferencias".

Además el artículo 1.4 del RD 1322/1994 de 20 de junio considera dato personal "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, tratamiento o transmisión concerniente a una persona física identificada o identificable".

Por otro lado, los datos personales procedentes de imágenes de individuos deberán formar parte de ficheros conforme a lo definido el artículo 3.b de la LOPD "todo conjunto organizado de datos de carácter personal cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". En consecuencia, los datos personales de grabación de imágenes, tanto si se almacenan durante un periodo de tiempo mediante un sistema de grabación como si es simplemente un circuito cerrado de imágenes en tiempo real serán objeto de regulación por la LOPD. Si bien en el primer caso los datos personales de la imágenes se almacenarán en un fichero y en el segundo al no existir grabación no podrá existir fichero pero sí un tratamiento de datos personales.

En la actualidad, la regulación de la captación de imágenes, consideradas estas como datos personales se encuentra desarrollado por la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el

tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

c) La videovigilancia:

Tal y como marca la Instrucción, las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 5 del Real Decreto 1720/2007, de 21 de diciembre, que considera como dato de carácter personal la información gráfica o fotográfica.

Se excluyen el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar (como la propia vivienda o la propia plaza de garaje).

Aunque nos hallemos ante un supuesto en que existan datos de carácter personal, será necesario que dichos datos se encuentren incorporados a un fichero. Ello supone que en el supuesto en que las imágenes no sean objeto de una organización sistemática, con arreglo a criterios que permitan la búsqueda de las mismas a partir de los datos personales de una determinada persona, el archivo en que se contuvieran no será considerado fichero a los efectos de la Ley. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

La creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

La Instrucción 1/2006 se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras. El tratamiento comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquellas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la Instrucción 1/2006 sin que ello requiera plazos o actividades desproporcionados. Las referencias a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

- Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como

cerrados deberá incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

- Tener a disposición de los interesados impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes solo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

Solo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquellas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Los datos serán cancelados (mediante bloqueo) en el plazo máximo de un mes desde su captación.

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Asimismo, cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas. El responsable deberá informar del deber de secreto a las personas con acceso a los datos.

En consecuencia, y únicamente bajo el aspecto de lo que es protección de datos, la utilización de videocámaras estaría fuera del ámbito de aplicación de la siempre que no pueda procederse a la identificación de las personas que aparecen en las imágenes o, en caso de poderse identificar dichas imágenes no hayan sido incorporadas a un fichero, en los términos definidos.

La videovigilancia en la vía pública está reservada a las Fuerzas y Cuerpos de Seguridad.

d) La dirección IP:

Se plantean diversas cuestiones referentes a la consideración como dato de carácter personal de una dirección IP de acuerdo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y sus implicaciones de cara a la adopción de las medidas de seguridad.

En primer lugar, se plantea si las direcciones IP son consideradas como datos de carácter personal, dado que solo en ese caso será aplicable al caso lo dispuesto en la Ley 15/1999, a tenor de lo establecido en su artículo 2.1.

Respecto a dicha cuestión, debe partirse en todo caso de la definición de dato de carácter personal que establece el artículo 3.a) de la Ley, que lo define como cualquier información concerniente a personas físicas identificadas o identificables.

El TCP/IP se trata de un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. Las redes TCP/IP se basan en la transmisión de paquetes pequeños de información, cada una de los cuales contiene una dirección IP del emisor y del destinatario.

Por otro lado, el DNS (sistema de nombre de dominio) es un mecanismo de asignación de nombres a ordenadores identificados con una dirección IP. Ciertas herramientas existentes en la Red permiten encontrar el enlace entre el nombre de dominio y la empresa o el particular.

A su vez, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. Es mas, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.

En estos casos, ello significa que, con la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre dirección, número de teléfono, etc.), por medios razonables, con lo que no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a del artículo 3 de la Ley 15/1999.

En otros casos, un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones estáticas.

Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación.

Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia Española de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos.

e) La dirección e-mail:
   Con carácter general, respecto de la consideración del e-mail como dato de carácter personal, se debe decir que la dirección electrónica se forma por un conjunto de signos o palabras que la diferencian de las demás, siendo el titular de la misma quien generalmente decide y elige la dirección correspondiente, con el único límite de que no exista otra dirección idéntica correspondiente a otro titular. En la selección de la dirección electrónica se pueden elegir combinaciones que no contengan significado alguno o, incluso, utilizar como combinación el nombre de la persona o algún otro dato identificativo.

El concepto de dato personal, según la definición de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), comprende cualquier información concerniente a persona física identificada o identificable, de donde se requiere la concurrencia de un doble elemento: por una parte la existencia de una información o dato y de otra, que dicho dato pueda vincularse a una persona física identificada o identificable. En el supuesto de direcciones electrónicas la información está constituida por un conjunto de signos que cuando permiten la vinculación directa o indirecta con una persona física la convierte en un dato de carácter personal.

f) Los datos biométricos:
   En primer lugar, hay que señalar que son datos biométricos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean

para tales fines la recogida de datos referentes a las huellas dactilares al iris del ojo, o a la voz.

Por su parte, el artículo 3.a de la LOPD, define los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". En este sentido, debe indicarse que, si bien el tratamiento de los datos biométricos no revela nuevas características referentes al comportamiento de las personas, sí permite, lógicamente, su identificación, por lo que resulta evidente que, en caso de procederse a su tratamiento, dicho tratamiento deberá ajustarse a los preceptos de la citada Ley Orgánica.

Según el artículo 4.1 de la LOPD, "Los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". El problema se planteará entonces en determinar si el tratamiento de la huella digital puede ser considerado excesivo para el fin que motiva dicho tratamiento.

Así, tratándose del tratamiento de la huella digital, la información contenida en dicho dato no contiene ningún aspecto concreto de la personalidad y tan solo cuando dicha información se vincula a la identidad de una persona es posible identificarla con toda certeza, de modo que los datos que se recaban no pueden considerarse de mayor trascendencia que los relativos a un número personal de identificación que coincide con el número asignado al empleado.

Por otra parte, en cuanto a la necesidad de que el interesado preste su consentimiento (o pueda oponerse) al tratamiento de su huella digital, debe indicarse que si bien el artículo 6.1 de la LOPD exige el consentimiento del interesado para el tratamiento automatizado de los datos de carácter personal, el artículo 6.2 prevé que no será preciso el consentimiento cuando los datos "se refieran a las partes de un contrato o precontrato de una relación de negocio laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

En este caso se debe asegurar el debido cumplimiento de las obligaciones derivadas de la relación administrativa o laboral que vincula al funcionario o personal laboral con la empresa, lo que unido a lo hasta ahora señalado permite implementar dicho tratamiento de datos.

Acceso a archivos de la Administracion General del Estado

Como punto de partida, el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso recuerda el derecho de los ciudadanos de acceso a los archivos

y registros públicos, consagrado en el artículo 106 de la Constitución, al disponer que "Los documentos conservados en los archivos incluidos en el ámbito de aplicación de esta norma serán de libre acceso salvo cuando les afecten las limitaciones previstas en la Constitución y en las Leyes".

Esta norma pretende, como indica su exposición de motivos, facilitar el ejercicio del derecho de acceso de los ciudadanos a los archivos y documentos administrativos, mediante la clarificación de los criterios fijados en la muy diversa legislación aplicable y con la introducción de un procedimiento común, muy simplificado, de solicitud de acceso. En la regulación del procedimiento, que pretende suprimir incertidumbres y eliminar cualquier ocasión de arbitrariedad, está muy presente la necesidad de proteger intereses públicos y privados en los términos reconocidos en la Constitución y las Leyes, que justifican la existencia de especiales requisitos y condiciones para el acceso a documentos que no son de libre consulta y requieren autorización.

En especial, esta regulación es respetuosa del delicado equilibrio que debe mantenerse entre la salvaguarda del derecho fundamental a la protección de datos personales -de acuerdo con la regulación contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal- y el derecho de acceso a documentos y archivos. Con el fin de proceder a una ponderación lo más ajustada posible, la norma distingue una variedad supuestos en relación con el acceso a documentos que contienen datos personales y gradúa, atendiendo al tipo de datos, la edad del documento, las circunstancias del caso y la finalidad del acceso, las condiciones y requisitos que se han de reunir para levantar las restricciones al acceso.

El régimen previsto –requisitos de la solicitud para el ejercicio del derecho de acceso, regulación de la tramitación y resolución, derecho a la obtención de copias– es conforme con lo previsto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que en su artículo 37 dispone que «los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud», al tiempo que menciona una variedad de materias que se rigen por su regulación específica.

Regla general:

- Libre acceso (Art. 106 C.E.) a ficheros públicos o privados sostenidos con fondos públicos.

Excepciones:

- Documentos que contengan datos de carácter personal.
- Secretos oficiales.
- Riesgos para la defensa nacional

Así, dispone el Real Decreto que "Los documentos que por disposición expresa de la Ley no deban ser públicamente conocidos se considerarán de acceso restringido. En particular, los documentos clasificados según lo dispuesto en la normativa sobre secretos oficiales, los documentos que contengan información cuya difusión pudiera entrañar riesgos para la seguridad y la defensa del Estado o interferir en la averiguación de los delitos, y aquellos que contengan datos personales cuyo conocimiento por terceros pudiera afectar a la seguridad, el honor, o la intimidad de las personas a las que se refieren". Respecto de tales documentos, el artículo 5.3 especifica las reglas de acceso, al establecer que "El acceso a los documentos previstos en los apartados anteriores queda condicionado, con las excepciones y especialidades previstas en la Ley, a la obtención de autorización previa. En el caso de los documentos que contienen datos personales, ausentes otras razones de limitación del acceso, el consentimiento del afectado será suficiente para levantar la restricción".

En este sentido el artículo 37.1 de la Ley 30/1992 establece el principio general de que "los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud".

A nuestro juicio, el acceso solicitado, en cuanto se refiera a datos de carácter personal contenidos en ficheros, a los efectos definidos en la meritada Ley Orgánica, constituirá una auténtica cesión de datos, dado que el artículo 3.i) de la Ley Orgánica 15/1999 define la cesión o comunicación de datos como "toda revelación de datos realizada a una persona distinta del interesado", lo que sucederá en el presente caso si se concede el acceso solicitado a ficheros que contengan datos de carácter personal de personas distintas del propio interesado.

Pues bien, respecto de la cesión de datos de carácter personal, el artículo 11 de la Ley Orgánica 15/1999 establece, como regla general aplicable al caso, que "los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". Esta regla general se verá únicamente exceptuada en los supuestos a que se refiere el artículo 11.2, a cuyo tenor "el consentimiento exigido en el apartado anterior no será preciso:

1. Cuando la cesión está autorizada en una Ley.
2. Cuando se trate de datos recogidos de fuentes accesibles al público.
3. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación solo será legítima en cuanto se limite a la finalidad que la justifique.
4. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
5. Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
6. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica".

Por otra parte, dado que el acceso se solicita de archivos y registros de la administración pública (y sin entrar ahora a valorar los supuestos en que los ficheros de los colegios profesionales habrán de ser considerados de naturaleza pública o privada, cuestión esta relacionada con la naturaleza de las potestades ejercitadas por la Corporación y que se estudia con mayor detalle en el informe solicitado por el propio Consejo General, obrante en el expediente administrativo), será de aplicación al supuesto lo establecido en el artículo 21.3 de la Ley Orgánica 15/1999, que establece taxativamente que "no obstante lo establecido en el artículo 11.2 b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa".

En consecuencia, a la vista de las disposiciones estudiadas, y tomando como único referente la normativa reguladora de la protección de datos de carácter personal, solo será posible conceder el acceso solicitado en aquellos supuestos en que el interesado haya manifestado su consentimiento libre, inequívoco, específico e informado a ello o cuando una norma con rango de Ley habilite la cesión de los datos[1].

Por otra parte, y como se señaló anteriormente, el artículo 37.7 de la Ley 30/1992 establece un regla específica relativa al acceso a los datos de carácter personal al acreditarse la existencia de un interés "histórico, científico o cultural relevante", lo que exige tomar igualmente en consideración el criterio sustentado por esta Agencia en relación con el acceso a datos de carácter personal con fines históricos, científicos o estadísticos, en los términos establecidos por la Ley Orgánica 15/1999.

En este punto existen numerosos informes de la Agencia[2] en que se analiza, por una parte, el ámbito de aplicación de la normativa de protección de datos cuando se trate de informaciones referidas a personas fallecidas y, por otra, la incidencia que en materia de protección de datos tienen las disposiciones relacionadas con el acceso al patrimonio histórico documental, contenidas en la Legislación reguladora del Patrimonio Histórico Español.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real decreto 1720/2007, de 21 de diciembre, es claro al establecer que "este Reglamento no será de aplicación a los datos referidos a personas fallecidas", añadiendo que "no obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de este con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".

El primer inciso reproducido no es sino la manifestación en la norma reglamentaria de la posición tradicionalmente mantenida por esta Agencia. Así la cuestión referente a la aplicabilidad de las normas de protección de datos a las personas fallecidas ha sido objeto de estudio reiterado por parte de esta Agencia en diversos informes y resoluciones en que se ha manifestado en la práctica totalidad de los supuestos en el sentido de considerar excluidos de la aplicación de la Ley Orgánica 15/1999 los datos referidos a quienes hubieran fallecido.

Quiere todo ello decir que la problemática planteada por la presente consulta, en lo que a la garantía del derecho fundamental a la protección de datos se refiere, únicamente resulta relevante cuando se esté haciendo referencia a datos relativos a personas que no hubieran fallecido, dado que en caso de fallecimiento no son aplicables las previsiones de la Ley Orgánica 15/1999 y su normativa de desarrollo, salvo en lo previsto en el inciso segundo del artículo 2.4 del Reglamento y la posible solicitud de la cancelación de los datos, si ello fuera procedente, por las personas enumeradas en dicho precepto.

A sensu contrario, la información concerniente a personas físicas identificadas o identificables que no hubieran fallecido sí se encontraría dentro del ámbito de aplicación de las normas reguladoras del derecho fundamental a la protección de datos, siendo entonces aplicable lo dispuesto en la Ley Orgánica 15/1999 y sus disposiciones de desarrollo.

Este mismo criterio aparece recogido en el informe emitido por esta Agencia, de 24 de octubre de 2008, emitido en relación con la consulta remitida por el Ministerio de la Presidencia y relativa a la creación de un mapa integrado sobre las fosas en las que hayan sido enterradas las víctimas, conforme a lo previsto en el artículo 12.2 de la Ley 52/2007, de 26 de diciembre, por la que se reconocen y amplían derechos y se establecen medidas a favor de quienes padecieron persecución o violencia durante la guerra civil y la dictadura, y en su informe de

25 de mayo de 2010, en que se planteaba por el Ministerio de Cultura si resultaba conforme a lo dispuesto en la Ley Orgánica 15/1999 y su Reglamento de desarrollo la difusión pública en Internet de datos personales referidos a las víctimas de la Guerra Civil y represaliados del franquismo, con especial referencia a los datos referidos a expedientes respecto de los que no hubieran transcurrido más de cincuenta años y más en concreto a los sumarios generados por los Juzgados y Tribunales de Orden Público, que teniendo en cuenta la fecha de creación de dichos órganos tendrían siempre una antigüedad inferior a la mencionada, respecto de los que se señalaba lo siguiente:

> "(…) solo será posible la publicación en el portal al que se refiere la consulta de los datos relativos a las personas que tengan la condición de víctimas de la Guerra Civil o represaliados del franquismo, y en particular, los vinculados con los sumarios tramitados por los Juzgados y Tribunales de Orden Público si se cumplen las siguientes condiciones:
> 1. Que se trate de personas fallecidas, debiendo contrastarse los datos que obren en poder de la consultante con los resultantes de otros registros que permitan acreditar esta circunstancia cuando sea necesario.
> 2. Tratándose de personas no fallecidas, que se haya obtenido el consentimiento de los interesados para que sus datos sean incluidos en el portal, debiendo informarse al interesado de todos los extremos relacionados con ese tratamiento en los términos previstos por el artículo 5 de la Ley Orgánica 15/1999.
> 3. En caso de no contarse con el consentimiento, la información que conste en el portal en relación con las personas que no lo hubieran prestado deberá constar de forma disociada, de forma que no resulte posible identificar directa o indirectamente al interesado".

En resumidas cuentas, del estudio de la normativa a la que se ha venido haciendo referencia y de la interpretación efectuada por esta Agencia en los distintos informes que se han referido a la misma, cabría diferenciar una serie de supuestos y reglas de aplicación para el acceso a los datos contenidos en los archivos y registros regulados por el artículo 37 de la Ley 30/1992, teniendo en cuenta la naturaleza de los datos accedidos, la finalidad que justifica el acceso y la antigüedad de los mencionados datos:

1. Las normas de protección de datos de carácter personal no serán de aplicación en los supuestos en los que la información facilitada como consecuencia del acceso a los archivos o registros no contenga datos de carácter personal, bien por no incluirlos los documentos respecto de los que se solicita el acceso, bien al haberse producido un previo procedimiento de disociación.
2. Del mismo modo, las normas de protección de datos tampoco serán aplicables a las informaciones referidas a personas fallecidas que sean objeto del acceso, sin perjuicio de las especialidades que, en su caso, pudieran establecerse en las normas reguladoras del Patrimonio Histórico Español o en otras normas especiales.

3. Cuando el acceso se solicite por el propio interesado cuyos datos figuren en los documentos a los que dicho acceso se refiere no existirá una cesión de datos sino una solicitud por el interesado de ejercicio del derecho de acceso, que podrá tramitarse conforme a lo establecido en la Ley Orgánica 15/1999, sin perjuicio de la posible existencia de disposiciones específicas reguladoras de dicho acceso cuando se trate de archivos o registros sometidos a normas especiales, tal y como dispone el artículo 25.8 del Reglamento de desarrollo de la Ley Orgánica 15/1999.
4. El acceso a los documentos que contengan datos especialmente protegidos de los interesados distintos de quien solicita el acceso a los mismos requerirá el consentimiento del interesado, que deberá reunir los requisitos establecidos en el artículo 7 de la Ley Orgánica 15/1999 o, tratándose de datos relacionados con la salud, el origen racial o la vida sexual de los interesados, que exista una norma con rango de Ley que así lo habilite por razones de interés público.
5. Del mismo modo, también sería preciso el consentimiento de los interesados cuando se trate de documentos que afecten a la intimidad de las personas, dado que en caso contrario el acceso queda únicamente limitado a ellas, conforme a lo previsto en el artículo 37.2 de la Ley 30/1992.
6. El acceso a documentos de "carácter nominativo", que no contengan otros datos que afecten a la intimidad de las personas será posible, además de cuando el interesado haya prestado su consentimiento para ello, en los supuestos en los que el solicitante acredite la existencia de un interés legítimo y directo, tal y como dispone el artículo 37.3 de la Ley 30/1992, en conexión con el artículo 11.2 a) de la Ley Orgánica 15/1999, entendiéndose que dicho interés puede deberse a que "en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos".
7. De la regla anterior, no obstante, quedarán exceptuados los documentos referidos a los procedimientos sancionadores.
8. Finalmente, se podrá autorizar el acceso directo a los documentos en los supuestos en que el investigador solicitante acredite un interés histórico, científico o cultural relevante, "siempre que quede garantizada debidamente la intimidad de las personas". A tal efecto, deberán tenerse en cuenta las reglas establecidas en las propias normas reguladoras del derecho de acceso a archivos y registros y las que establecen el régimen del patrimonio histórico español. De este modo, el acceso sería posible:
    - Con las limitaciones que se han expuesto en caso de documentos con una antigüedad inferior a cincuenta años.
    - Sin dichas limitaciones en caso de documentos con una antigüedad superior a cincuenta años si no consta el fallecimiento del afectado o la fecha del mismo.

Finalmente, hay que tener en cuenta lo dispuesto en el artículo 11.6 de la Ley Orgánica 15/1999, según el cual "si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores"; es decir, la comunicación no deberá fundarse en el consentimiento o en otra de las causas específicas legitimadoras del tratamiento establecidas en el mencionado precepto.

El artículo 3.f) de la Ley Orgánica 15/1999 define el procedimiento de disociación como "todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable". Del mismo modo, es dato disociado, según el artículo 5.1.e) del Reglamento "aquél que no permite la identificación de un afectado o interesado".

A la luz de las definiciones que se han reproducido anteriormente, si la cesión de los documentos se lleva a cabo de forma que no sea posible conocer los datos personales que los mismos contengan lo que existirá en todo caso será un procedimiento de disociación. Por su parte, la excepción a las reglas especiales que impongan una determinada legitimación para el tratamiento de los datos de carácter personal debería operar no cuando la disociación sea posible, sino cuando la misma tenga efectivamente lugar.

Notas

[1] Informe 437971/2011, de la AEPD, de fecha 24 octubre 2011.

[2] Informe de esta Agencia de 19 de abril de 2011.