AUTODETERMINACIÓN INFORMATIVA Y DERECHO AL OLVIDO EN LA UNIÓN EUROPEA PARTICULARIDADES RESPECTO DE LOS MENORES DE EDAD

FRANCISCO DURÁN RUIZ
Profesor Contratado Doctor
Departamento de Derecho Administrativo. Universidad de Granada. (España) Email: fduranr@ugr.es

/RESUMEN

Pretendemos en esta ponencia plantear las dificultades que se plantean actualmente a las Administraciones públicas para defender el derecho fundamental a la protección de los datos personales de sus ciudadanos, en un momento en que la determinación del contenido y extensión de la protección de datos personales en la Unión Europea se encuentra en un momento trascendental. Como consecuencia de un contencioso entre Google y la Agencia Española de Protección de datos, por varias resoluciones de este último que obligaba al buscador a suprimir la posibilidad de acceder a datos personales, se ha planteado una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea y se ha provocado un cambio legislativo a nivel de la Unión, adaptando la legislación sobre protección de datos especialmente a internet y a las redes sociales.

Se ha planteado, entre otras cuestiones, si un buscador es responsable del tratamiento de datos personales o no, para que se haga efectivo el "derecho al olvido" en internet, dentro de las peculiaridades que tiene en internet el tratamiento de datos personales, pues sus titulares no pueden eliminarlos cuando quieran y sin condiciones, sino que más bien poseen la facultades de consentimiento, oposición y cancelación al tratamiento de los mismos que son la esencia del derecho a la autodeterminación informativa.

En el caso del ejercicio de este derecho por menores de edad la situación se complica, especialmente cuando tales menores no colaboran en dicha protección, y por el gran valor económico que para el mercado y las empresas que en su seno compiten, tienen sus datos personales.

/PALABRAS CLAVES

Información, derecho, menores, Google, Internet

/ABSTRACT

We aim in this paper raise the difficulties currently faced by the public authorities to defend the fundamental right to protection of personal data of its citizens in a time when determining the content and extent of the protection of personal data in the European Union is at a momentous time. As a result of a dispute between Google and the Spanish Agency for Data Protection, by several resolutions of the latter that forced the search engine to remove the possibility of access to personal data, has raised a preliminary question to the Court of Justice of the Union European and legislative change has led to the Union level, adapting the data protection legislation to the internet and especially social networks.

It has been suggested, among other things, if a search engine is responsible for processing personal or not, information is made effective the "right to be forgotten" on the Internet, within the features you have in internet processing of personal data, as holders may not remove them whenever and unconditionally, but rather have the powers of consent, cancellation and opposition to the processing of them that are the essence of the right to informational self-determination.

For the exercise of this right by children the situation is complicated, especially when such children do not cooperate in such protection, and the great economic value to the market and the companies that compete within it, have your personal data.

/KEY WORDS

Information, rights, children, google, internet

1. DERECHO A LA AUTODETERMINACIÓN INFORMATIVA EN LA UNIÓN EUROPEA

La Entonces Comunidad Europea adoptó la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre sus Estados miembros. Los retos derivados de la protección de los datos personales se han incrementado por la vertiginosa evolución tecnológica. Actualmente la tecnología permite que tanto las administraciones públicas como las empresas privadas utilicen datos personales a una escala anteriormente inimagiblable en el desarrollo de sus actividades, incrementándose exponencialmente la magnitud del intercambio y la recogida de datos (hasta 2003, la humanidad había generado cinco exabytes de datos, cantidad que actualmente se genera cada tres días). Del mismo modo, las personas físicas aumentan diariamente el volumen de información personal que difunden, siendo este un fenómeno global. No se puede negar que tanto la vida social como la económica están siendo actualmente fuertemente transformadas por las TIC.

Por todo lo anterior resulta esencial para el desarrollo económico generar confianza en el entorno digital, de forma que los consumidores no alberguen dudas a la hora de adquirir productos y servicios en internet, y las TIC puedan desarrollar todo su potencial y usos. En este sentido es esencial la adecuada protección de los datos personales, o del derecho a la "autodeterminación informativa" término que expertos como MURILLO DE LA CUEVA o PIÑAR MAÑAS[1] , prefieren al finalmente acuñado de derecho a la protección de datos de carácter personal[2] .

Actualmente debemos partir, en lo relativo a la protección de datos personales y desde un punto de vista jurídico, del artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), sin olvidar que desde el año 2000 tanto la privacidad como la protección de datos personales son derechos reconocidos en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea, y por tanto entran dentro de las competencias de la Unión. La cuestión es ver cómo se conjugan estos derechos con otros igualmente reconocidos en la Carta como la libertad de expresión e información o la libertad de empresa.

Estas cuestiones, y otras como la cuestión prejudicial planteada por la Audiencia Nacional española ante el Tribunal de Justicia de la Unión Europea por la sanción de la Agencia Española de Protección de Datos a Google[3] tras la modificación por esta última de su política de privacidad en 2012[4] han llevado a la Unión Europea a plantearse la necesidad de revisar el acervo comunitario en materia de comunitario en materia de protección de datos. Así pues, la Comisión ha decidido promover la aprobación de un reglamento sustitutivo de la Directiva 95/46 CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, con el fin de hacerla más efectiva[5] .

Entre las cuestiones recogidas en la propuesta de Reglamento, debemos destacar, la exigencia de que los datos recogidos para finalidades determinadas, explícitas y legítimas no puedan ser tratados posteriormente de manera incompatible con esas finalidades. Igualmente, los datos tratados deben serlo de forma limitada y adecuada a la necesidad y finalidad del tratamiento, garantizándose la pertinencia de tal tratamiento. Y en cuanto a la conservación de los datos, esta debe realizarse de manera que permitan la

[1] Este autor considera más expresiva la denominación de "derecho a la autodeterminación informativa" cuando nos referimos al control que ofrece el ordenamiento jurídico a las personas sobre el uso por parte de terceros de información sobre ellas mismas, que la que finalmente se ha impuesto, derecho a la protección de datos de carácter personal; vid. ad.ex, el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (MURILLO DE LA CUEVA 2009, 11-12).

identificación del interesado durante el tiempo que no exceda del necesario para la realización de los fines para los que son recogidos, de tal manera que solo podrán ser conservados durante más tiempo en la medida en que no sean tratados más que a fines de investigación histórica, estadística o científica de acuerdo con una serie de reglas y condiciones establecidas en el reglamento y procediendo a un examen periódico con el fin de valorar la necesidad de continuar conservándolos.

---

[2]. Este nuevo derecho, de última generación, sólo recientemente ha recibido el estatus de derecho fundamental, como es sabido, y salvo en algún caso, como el de Portugal, se ha introducido en los ordenamientos jurídicos bien por el legislador ordinario o comunitario, como el caso de la Carta de Derechos Fundamentales, bien por la jurisprudencia: en España por la STC 292/2000, de 30 de noviembre, y en Europa con las Sentencias del TEDH Amann contra Suiza de 16 de febrero de 2000 o Rotaru contra Rumanía, de 4 de mayo de 2000, todas coetáneas (Ibidem, pp. 13-14).

[3]. Asunto C-131/12 Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.

[4]. Google modificó la política de privacidad y las condiciones de uso de la mayoría de sus servicios en marzo de 2012, creando un modelo de tratamiento de datos basado en la transversalidad, posibilitando que la información que una persona facilita para un servicio pueda combinarse con la de otros y utilizarse con cualquier finalidad, y generando un uso de los datos personales que excede ampliamente las expectativas que un usuario podría esperar de la utilización de un servicio. Ante las múltiples dudas suscitadas por esta cuestión, el Grupo de Autoridades Europeas de Protección de Datos (GT29) acordó iniciar una investigación conjunta coordinada por la Autoridad Francesa, la CNIL, que concluyó constatando la incompatibilidad de la nueva política de privacidad con la legislación europea de protección de datos.

En octubre de 2012, las Autoridades de todos los Estados de la Unión Europea enviaron una carta a Google en la que se relacionaban los principales problemas y se hacían recomendaciones para cumplir con el derecho europeo, requiriendo que se adoptaran medidas en un plazo razonable.

Ante la falta de reacción de Google, el Grupo de Autoridades acordó que las autoridades de los Estados iniciarían acciones coercitivas para garantizar el respeto del derecho a la protección de datos.

En abril de 2013 las Autoridades de Protección de Datos de Alemania, España, Francia, Holanda, Italia y Reino Unido iniciaron actuaciones de investigación y procedimientos sancionadores con arreglo a las previsiones de sus ordenamientos nacionales, pero actuando en estrecha coordinación.

Fruto de esta actuación fue la Resolución de la Agencia Española, la primera en la UE en sancionar a Google, por tres infracciones graves de la Ley Orgánica de Protección de Datos (LOPD) española, imponiéndole una sanción de 300.000 euros por cada una de ellas y requiriendo a la compañía para que adoptase a la mayor brevedad las medidas necesarias para cumplir con la legalidad.

La Agencia Española de Protección de Datos (AEPD) consideró que Google recoge y trata ilegítimamente información personal, tanto de los usuarios autenticados (dados de alta en sus servicios) como de los no autenticados, e incluso de quienes son meros "usuarios pasivos" que no han solicitado sus servicios pero acceden a páginas que incluyen elementos gestionados por la compañía sin explicitarlo, y que tal actuación vulnera gravemente el derecho a la protección de los datos personales reconocido a todos los ciudadanos por el artículo 18 de la Constitución Española y regulado en la LOPD.

Según las inspecciones realizadas por la AEPD, Google recopila información personal a través de casi un centenar de servicios y productos que ofrece en España, sin proporcionar en muchos casos una información adecuada sobre qué datos se recogen, para qué fines se utilizan y sin obtener un consentimiento válido de sus titulares. No se informa de forma clara, por ejemplo, a los usuarios de Gmail de que se realiza un filtrado del contenido del correo y de los ficheros anexos para insertar publicidad. Cuando se informa, se utiliza una terminología imprecisa, con expresiones genéricas y poco claras que impiden a los usuarios conocer el significado real de lo que se plantea, utilizando expresiones ambiguas como "mejorar la experiencia del usuario" que originan una política de privacidad indeterminada y poco clara. La falta de información adecuada, particularmente sobre las finalidades específicas que justifican el tratamiento de los datos, impide que pueda considerarse que existe un consentimiento específico e informado y, en consecuencia, válido.

Un segundo problema reside en el hecho de que Google combina la información personal obtenida a través de los diversos servicios o productos para utilizarla con múltiples finalidades que no se determinan con claridad, vulnerando con ello la prohibición de utilizar los datos para fines distintos de aquellos para los que han sido recabados. Esta combinación de los datos que se recogen en un servicio con los obtenidos en otros, y que permite a Google enriquecer la información personal que almacena, excede ampliamente las expectativas razonables del usuario medio, que no es consciente del carácter masivo y transversal del tratamiento de sus datos. Al actuar así, Google se sirve de una tecnología sofisticada que sobrepasa la capacidad de la mayoría de los usuarios para tomar decisiones conscientes sobre el uso de su información personal por lo que, en la práctica, pierden el control sobre la misma que está en la base del derecho a la protección de datos personales o autodeterminación informativa.

Google almacena y conserva datos personales por periodos de tiempo indeterminados o injustificados, contraviniendo con ello el mandato legal de proceder a su cancelación cuando dejan de ser necesarios para la finalidad que determinó su recogida. Tal conservación de los datos por tiempo indefinido y más allá de las exigencias que se derivan de las finalidades pretendidas en el momento de la recogida, constituye un tratamiento ilícito de los mismos.

Un tercer motivo de sanción por parte de la AEPD es que ésta consideró que Google obstaculiza e incluso impide en ocasiones el ejercicio de los derechos de acceso, rectificación, cancelación y oposición que son el núcleo esencial del derecho a la protección de datos personales.

Y esto es así porque el procedimiento que los ciudadanos deben seguir para ejercer sus derechos o gestionar su propia información personal les obliga a recorrer un número indeterminado de páginas, dispersas en varios enlaces, que no están disponibles para todos los tipos de usuarios y, en ocasiones, con denominaciones que no siempre hacen referencia a su objeto. La propia compañía ha reconocido que es necesario ejecutar al menos siete procesos diferentes, reservándose incluso el derecho de no atender las solicitudes que supongan un "esfuerzo desproporcionado" a su parecer.

[5]. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM/2012/09 final), de 25 de enero de 2012, sobre La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI.

2. EL CONSENTIMIENTO DEL INTERESADO EN EL TRATAMIENTO DE LOS DATOS PERSONALES

Teniendo en cuenta la estrecha relación que existe entre los datos personales y el derecho fundamental a la intimidad (y en sentido más amplio, a la dignidad personal), como regla general se exige la obtención previa del consentimiento de una persona para poder proceder al tratamiento de sus datos.

Del derecho reconocido a la autodeterminación informativa (control sobre los propios datos personales), surge también el reconocimiento de la posibilidad de evitar el tratamiento de los datos, especialmente frente a las potenciales agresiones a la dignidad y a la libertad provenientes del uso ilegítimo del tratamiento mecanizado de datos. A este respecto, la legislación de protección de datos ofrece varias alternativas al afectado: revocar el consentimiento, oponerse al tratamiento o ejercitar los derechos de rectificación y cancelación.

Así, la Sentencia 292/2000 del Tribunal Constitucional español que estableció el derecho a la protección de datos personales como un derecho fundamental e independiente del derecho a la intimidad, dice expresamente que el derecho fundamental a la protección de datos persigue garantizar a esa 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. Y que el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone

De acuerdo con la Directiva 95/46 CE, la Ley orgánica de protección de datos española exige que el consentimiento para el tratamiento de los datos referentes a una persona ha de ser libre, inequívoco, específico e informado. Por tanto, no es necesario que tenga carácter expreso en el sentido de que deba haber una declaración al efecto, verbal o escrito; no obstante, la actuación de la que se deduzca que existe un consentimiento tácito debe ser indubitada en este sentido.

La Propuesta de reglamento comunitario define el consentimiento como manifestación de voluntad libre, específica, voluntaria, informada y explícita, por la que el interesado acepta por una declaración o un acto positivo inequívoco que los datos de carácter personal que le conciernen sean objeto de tratamiento, por lo que no hay cambios en este sentido.

Por lo que se refiere a las actuaciones dirigidas a utilizar publicidad comportamental en el marco de internet, que se realiza mediante la actuación de los proveedores de redes de publicidad, los anunciantes y los editores, exige que previamente se haya obtenido el consentimiento informado de los usuarios[6] .

La información deberá ser clara y precisa, y abarcar la identidad del responsable de instalar las cookies y recoger la información correspondiente, el funcionamiento de las cookies, el tipo de información que se recaba y la finalidad del tratamiento. Dicho consentimiento puede obtenerse a través de los parámetros adecuados del navegador, siempre que el usuario del ordenador reciba la información previa adecuada y suficiente, y que realice una acción expresa para modificar la configuración predeterminada que por defecto rechace la recogida y el tratamiento de la información para permitir así el uso de las cookies.

En determinados casos la Ley de protección de datos no considera necesario el consentimiento del interesado para el tratamiento de su datos. En primer lugar cuando los datos se recojan para el ejercicio de las funciones propias de las adminis-

traciones públicas en el ámbito de sus competencias; en segundo cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; en tercer lugar cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado; o por último cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado (art. 6.2 LOPD).

Por tanto, cabe entender que es suficiente el interés legítimo de quien realiza el tratamiento para que sea posible el mismo sin consentimiento del interesado, no implica que se haya derogado la necesidad del consentimiento como regla general. Se exige, por un lado, que el tratamiento sea necesario para satisfacer el interés legítimo y, por otro, la no vulneración de los derechos fundamentales del titular de los datos como límite. Será necesario como ha establecido el TJUE[7] , para el tratamiento de datos personales sin consentimiento del afectado, además de que exista un interés legítimo por parte del responsable del tratamiento "la ponderación de los derechos e intereses en conflicto, que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los derechos fundamentales de la Unión Europea confieren al interesado" (apartado 40).

En relación con las libertades de expresión y de información, existe la posibilidad de hacer públicos datos personales ajenos sin consentimiento previo del interesado en ejercicio legítimo de tales libertades, fundamentándose tal posibilidad directamente en el artículo 20 de la Constitución española y en la previsión de la propia LOPD, que establece la posibilidad de que excepciones al principio del consentimiento informado si están previstas en una ley.

2.1. LOS DERECHOS DE OPOSICIÓN Y CANCELACIÓN Y LA REVOCACIÓN DEL CONSENTIMIENTO

La LOPD establece en su art. 6.3 que el consentimiento para el tratamiento de datos personales puede ser revocado siempre que exista «causa justificada». No obstante, considerando la relevancia del consentimiento y que la disponibilidad de los datos que, en su caso, lo fundamenta afecta a derechos fundamentales de la persona y que la directiva no dice nada en relación con la revocación, la conclusión es que la revocación del consentimiento ha de ser totalmente libre, al igual que ocurre con la emisión del mismo. En este sentido la propuesta de reglamento comunitario prevé que el consentimiento del interesado pueda retirarse en cualquier momento sin ningún condicionamiento adicional.

El problema surge cuando debe ponderarse la posibilidad de revocación sin justificación con otros derechos o intereses legítimos de terceros, del propio responsable del tratamiento o bien con cuestiones de interés general como el derecho a recibir información, de enseñanza, interés histórico-artístico, etc. En tal caso, y especialmente si existen derechos adquiridos en el marco de una relación contractual, será posible la revocación del consentimiento del contratante que ha cedido los datos, pero esta debe ir precedida y supeditarse a una indemnización de los perjuicios que haya podido sufrir el cesionario contratante por la revocación.

A diferencia de la revocación, la oposición a tratamiento se define como la facultad que la ley reconoce al titular de los datos en los casos en que no es necesario su consentimiento para

[6] El Real decreto ley 13/2012 de 30 de marzo, que desarrolla la Ley de servicios de la sociedad de la información, a incorporado a la normativa española esta exigencia de la UE, derivada de la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (art. 5.3).

[7] Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011.

el tratamiento y siempre que no haya ley que se oponga a ello, y se exige también en este caso por la LOPD (art. 6.4) motivos fundados y legítimos relativos a una situación personal para llevarla a cabo. También se permite cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, bastando en tal supuesto simplemente la solicitud del afectado, y en el caso en que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

A este respecto la Propuesta de reglamento comunitario no modifica sustancialmente lo establecido en la Directiva 46/95 , y prevé que ha de admitirse por razones propias de la situación del interesado al menos en los casos en que el tratamiento sea necesario para atender intereses vitales del mismo, cuando sean recabados para el ejercicio de una misión efectuada en interés general o relevante para el ejercicio de la autoridad pública de que esté investido el responsable o en atención a intereses legítimos perseguidos por el responsable del tratamiento. También se recoge el derecho a oponerse al tratamiento de datos con fines de publicidad.

La cancelación por su parte, se define como el derecho que la ley reconoce al interesado para retirar datos, mediante su bloqueo, cuando el tratamiento no se ajuste a lo dispuesto en la ley. Así el art. 4.5 LOPD establece que los datos personales serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, y no serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en función de los cuales hubiesen sido recabados o registrados.

Se trata de tres facultades o derechos distintos, aunque no existan legislativamente ni en la práctica grandes diferencias entre ellos. Sí son cambian sus condiciones de ejercicio. Así, la revocación y la oposición no implican que haya existido una irregularidad en el tratamiento de los datos, mientras que procederá la cancelación precisamente cuando exista tal irregularidad. Tanto la facultad de oposición, como la de revocación y cancelación pueden ejercitarse frente al responsable del fichero o tratamiento. En el caso de los datos que son objeto de tratamiento, en internet será responsable quien decida o permita tanto la «subida» de los mismos como su difusión en la red, pues en todos estos casos se están determinando efectivamente los fines y medios del tratamiento.

3. EL DERECHO AL OLVIDO DIGITAL O AL OLVIDO EN INTERNET COMO PARTE DEL DERECHO A LA AUTODE TERMINACIÓN INFORMATIVA.

Recientemente se han ido produciendo cada vez con mayor frecuencia casos de ciudadanos afectados por hechos del pasados divulgados vía internet que les persiguen en el presente, ante lo cual ha comenzado a dirigirse a las autoridades en materia de protección de datos demandando la tutela de sus derechos, y la cancelación de sus datos personales.

Las demandas más habituales se producen ante la negativa de los responsables y administradores de páginas web y redes sociales de cancelar datos personales. La previsión es que estos problemas vayan siendo mayores, a medidas que los datos están más interconectados y que la generación de los denominados "nativos digitales", que procesa públicamente su vida privada compartiendo en tiempo real imágenes, vídeos y comentarios en la redes sociales y a través de aplicaciones para dispositivos electrónicos (teléfonos móviles, tablets, ordenadores...) pueda ver comprometido su futuro, precisamente, por la gran cantidad de datos personales que la red contiene y que pueden constituir un auténtico currículum vitae no deseado que les provoque consecuencias negativas a la hora de contratar productos o servicios (seguros, servicios médicos, etc.) o acceder al mercado laboral.

Ante la gran preocupación que ha surgido en torno a esta cuestión, las autoridades en materia de protección de datos han tenido un papel relevante y proactivo a favor del del reconocimiento del derecho al olvido digital. La AEPD ha afirmado en diversas ocasiones que ningún ciudadano que no sea objeto de un hecho noticiable de relevancia pública tiene que resignarse a que sus datos se difundan en Internet sin poder reaccionar ni corregir su inclusión[8] Por otra parte, ha tratado de clarificar y extender tal derecho al olvido, al entender que los ciudadanos pueden ejercer el derecho de cancelación de los datos que la red conserva cuando estos no se contengan en una fuente accesible al público ni exista una finalidad legítima que proteja la publicación tales como libertades informativas, finalidad cultural e histórica, educativa, etc., y por otra parte, al reconocer igualmente el derecho de oposición frente al tratamiento que los buscadores web realizan de los datos personales. Esto es, además de la cancelación entendida como una desindexación de la información pasada en los motores de búsqueda, se exige que el buscador encuentre medios para que dicha información aparezca de nuevo a posteriori[9] , basándose en el consentimiento y la finalidad de los datos como principios fundamentales del tratamiento legítimo de los datos personales.

Esto se ha reflejado en la Propuesta de reglamento comunitario en materia de datos personales, que finalmente ha recogido este derecho al olvido digital, cuyo significado, pese a lo que hemos apuntado, no está delimitado claramente y arroja aún muchas sombras. Puesto que aún no es un concepto legal asentado no se sabe si cuando se alude a ello se quiere hacer referencia al derecho de eliminar los datos personales con motivo o justificación cuando se requiera, de manera que en realidad se trataría de ejercitar las facultades de revocación, oposición o cancelación, o al derecho absoluto a la autodeterminación informativa. En la mayoría de los casos a lo que se hace referencia como hemos visto es a un derecho a la desindexación de los datos en la red, de tal manera que los buscadores y motores de búsqueda, salvo consentimiento, no permitan acceder a estos aún

[8] Resolución TD/266/2007 de la AEPD.

cuando aparezcan en la página web original, ya que realmente es la indexación lo que facilita la difusión no querida de los datos.

A este respecto, la Propuesta de reglamento dispone en su artículo 17 que el interesado tiene derecho a obtener del responsable del tratamiento la eliminación de los datos que le conciernan, así como su difusión, en especial cuando se trate de datos proporcionados por el interesado si es menor, por alguno de los siguientes motivos:

> /que los datos ya no sean necesarios para los fines para los que han sido recogidos o tratados;
>
> /que el consentimiento haya sido retirado o haya expirado el tiempo autorizado para la conservación y no exista otro motivo legal para esta; ó
>
> /la oposición al tratamiento o que este no sea conforme al reglamento por otros motivos.

En realidad, el pretendido derecho al olvido no es algo tan novedoso ni la eliminación de los datos se configura como facultad distinta de la revocación del consentimiento, la oposición y la cancelación, de tal manera que puede concluirse que no es más que la manera de hacer referencia generalizada al ejercicio de aquellas facultades, con el contenido específico que tiene cada una de ellas.

El ejercicio legítimo del derecho tiene como consecuencia que el responsable ha de proceder inmediatamente a la eliminación de los datos, aunque existen algunas excepciones también en este caso, pues puede autorizarse la conservación posterior por fines de investigación histórica, estadística y científica, por razones de interés público en el ámbito de la salud pública, para el ejercicio del derecho a la libertad de expresión, cuando la legislación lo exija, o en caso de que existan motivos para restringir el tratamiento de los datos en vez de proceder a su supresión (vid. considerando 53 de la Propuesta de reglamento).

4. PROTECCIÓN DE DATOS PERSONALES Y MENORES DE EDAD

En la actualidad los menores, mucho antes de tener madurez suficiente y desde una edad cada vez más temprana, facilitan a lo largo de su infancia y adolescencia sus datos personales de manera indiscriminada y descontrolada a una multitud de empresas, entidades y organizaciones públicas y privadas. Todo ello, como es propio de la edad, sin control alguno ni precaución ante el peligro que entraña la exposición pública de los datos personales, y sin ser plenamente consciente de los efectos negativos que dichas conductas pueden tener sobre la su intimidad personal y familiar o sobre su futuro derecho a la autodeterminación informativa.

Como acertadamente expresa Gómez-Juárez Sidera (2006, 2-3), en la inmensa mayoría de los casos, el menor no sólo ignora por completo su derecho a la protección de sus datos de carácter personal y lo que ello significa, sino que además tampoco se siente especialmente preocupado o molesto a la hora de tener que facilitar sus datos a terceros, como puede suceder en el caso de los adultos, haciéndolo gustoso si a cambio accede al servicio deseado (juegos, aplicaciones, redes sociales...) o existe la promesa de un atractivo premio. Por otro lado, el desconocimiento del menor es el instrumento perfecto para obtener a través de él aquellos datos de sus familiares (padres, hermanos, amigos, familiares, etc.) que en circunstancias normales un adulto probablemente se hubiese negado a facilitar, tales como datos acerca de la situación económica familiar, preferencias, hábitos de consumo, o

[9] Resolución TD/00463/2007 de la AEPD.

incluso ideología, religión o creencias de sus padres. Pensemos, finalmente, en lo valioso que puede ser para una empresa el incorporar a sus ficheros los datos de un menor al cual poder bombardear durante el resto de su vida con ofertas y promociones perfectamente adecuadas a sus gustos y perfil como consumidor, seguido con detenimiento desde su infancia.

Partiendo de estas bases, y considerando las escasas posibilidades de los padres y tutores de los menores de controlar o limitar su libertad de expresión e información por pura lógica generacional , el derecho a la protección de datos personales se convierte en el siglo XXI en uno de los grandes campos de batalla de la guerra entre Estado y Mercado[10] . Sólo con el apoyo de los poderes públicos en la defensa de este derecho fundamental, existe alguna posibilidad de preservar el derecho frente a los cada vez más poderosos gigantes de los mercados del consumo, la tecnología y la información.

4.1. LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS MENORES POR LAS ADMINISTRACIONES PÚBLICAS

Las Administraciones públicas, cuyos medios materiales y personales serán siempre menores que los de los operadores privados, deberán guardar especial cuidado en no convertirse en un aliado de los "usurpadores de datos" a los que trata de combatir, y en respetar las especiales exigencias que le impone la ley en el tratamiento de los datos de los ciudadanos de cuyo tratamiento es responsable [11] . En cualquier caso, en esta guerra, siguiendo con el símil, la neutralidad de la Administración no la convierte en aliada sino en enemiga. Las Administraciones públicas, con las Agencias de Protección de Datos y todo el arsenal del Estado de Derecho (Defensores del Pueblo y del Ciudadano), cooperación y colaboración internacional e interadministrativa, colaboración público-privada, etc., son el último bastión encargado de proteger a los ciudadanos, y particularmente a los menores de edad, contra todos y frente a todos. No olvidemos que en este ámbito, inclusive amigos, compañeros o familiares pueden ser también los que faciliten los datos personales de otros e ingenuamente contribuyan a la vulneración de sus derechos. También los propios ciudadanos, y especialmente los menores, contribuyen como se ha apuntado a la vulneración de sus propios derechos, siendo necesario en este caso especialmente llevar hasta sus últimas consecuencias el principio del superior interés del menor reconocido tanto en Convención sobre los Derechos del Niño de la ONU de 1989 como en las normas internacionales y nacionales de protección de menores, entendiendo ese interés superior como el interés objetivo del menor que es independiente de los intereses subjetivos tanto del menor como de sus padres, tutores o guardadores.

Resulta esencial que la Administración constituya en esta tarea protectora un aliado y no el enemigo, puesto que todas las Administraciones territoriales [12] manejan continuamente los datos de los ciudadanos, especialmente en el contexto de la prestación de servicios públicos, y particularmente los que implican contacto con los menores de edad, como los servicios sociales[13] o los centros educativos [14]

Imaginemos, en el ámbito de los servicios sociales, el caso de los menores tutelados cuya guarda se ejerce en la mayoría de los casos en acogimiento residencial cuando se trata de adolescentes que han sido declarados por la Administración en situación de desamparo. En estos casos, y especialmente cuando los menores son mayores de 14 años, pueden surgir conflictos.

10. Como apunta BALLESTEROS MOFFA (1997, 33), la tutela de la información personal "es fruto de la llamada "sociedad de la información" o "del conocimiento", también denominada "sociedad digital" y "sociedad en red", cuyo correlato económico se encuentra en la "nueva economía" o "economía digital", que constituyen un auténtico nuevo modelo u orden social.

11. Cfr., en este sentido, PÉREZ VELASCO, María del Mar, «Los ficheros públicos", en AAVV, Troncoso Reigada, A. (Dir.), Estudios sobre Administraciones públicas y protección de datos personales, Madrid, Thomson-Civitas y Agencia de Protección de Datos de la Comunidad de Madrid, 2006, pp. 117-142.

El interés superior del menor que la Administración tiene la obligación de defender, es decir, la interpretación que de dicho interés haga tal Administración –que tiene ex lege (art. 172 CC) la tutela y ejerce la guarda del menor desamparado–, pueden entrar en conflicto con el interés subjetivo del propio menor, a la hora de que el menor acceda, por ejemplo, a una concreta red social en internet y muestre determinada información personal, coincidente o no con dicho interés superior reconocido como summun principiis de la protección de menores[15] .

Cabe recordar aquí la doctrina sentada por la STC 183/2008, de 22 de diciembre, que establece que a los menores de 16 años tutelados (en este caso extranjeros, pero la fundamentación es aplicable a los menores en general)[16] , debe dárseles audiencia.separadamente, por sí mismos o mediante el representante que designen en los procedimientos administrativos o judiciales que afecten a derechos de su esfera personal (como es el caso de la repatriación de un menor extranjero no acompañado). En el caso de menores de dieciséis años con madurez suficiente, que manifiesten una voluntad contraria a la de quien ostenta su tutela o representación, se establece el nombramiento de un "defensor judicial" ajeno a la Administración tutora para su representación, figura que, como veremos, no se ha contemplado en la legislación de protección de datos personales.

Resulta necesaria una importante labor pedagógica para el conocimiento y el ejercicio del derecho a la protección de datos de carácter personal, hacia los menores y hacia sus familias y responsables legales, especialmente por parte de las instituciones educativas y de la Administración institucional dedicada al apoyo de los jóvenes (Institutos de la Juventud, organismos locales y autonómicos encargados del movimiento asociativo juvenil, etc.) [17]

12. Cfr., en el contexto europeo, Agencia de Protección de Datos de la Comunidad de Madrid, e-PRODAT: Administración electrónica y Protección de Datos en Regiones y Ciudades Europeas, Madrid, 2006 o, en el ámbito local, DEL PESO NAVARRO, Emilio, JOVER PADRÓ, Josep, y DEL PESO RUIZ, Margarita, Los datos de los ciudadanos en los Ayuntamientos, Ediciones Díaz Santos e Informáticos Europeos Expertos, 2004.

13. Cfr., en este sentido, Agencia de Protección de Datos de la Comunidad de Madrid, Protección de datos personales para Servicios Sociales Públicos, Madrid, Thomson-Civitas, 2008.

14. Vid, al respecto, Agencia de Protección de Datos de la Comunidad de Madrid, Protección de datos personales para Centros Educativos Públicos, Madrid, Thomson-Civitas, 2008.

15. Vid. art. 3 de la Convención de los Derechos del Niño aprobada por la Asamblea General de la ONU el 20 de noviembre de 1989, así como el art. 24.2 de la Carta de Derechos Fundamentales de la UE, o en el ámbito doméstico, en el art. 2 de la Ley Orgánica 1/1996, de Protección jurídica del menor y en múltiples artículos del Código Civil, la LEC, LECrim o la LORPM (5/2000), sin olvidar las leyes autonómicas en materia de protección de menores.

16. Esta Sentencia se refiere a un caso de repatriación, denominada reagrupación familiar por la Ley de Extranjería (LO 4/2000, de 11 de enero) de un menor marroquí tutelado por la Comunidad de Madrid. El interés subjetivo del menor de permanecer en España no estaba representado pues chocaba contra el interés de su tutor legal, perteneciente a los servicios de protección de menores de la Comunidad Autónoma, que habían asumido la representación legal del menor tras haber declarado la situación legal de "desamparo" del mismo según el artículo 172 del Código Civil y la legislación autonómica aplicable. Este tutor legal avalaba la repatriación pretendida por la misma Administración a la que pertenecía dicho tutor, impidiéndose a un tiempo la existencia de otra persona o entidad que defendiese al menor ante la repatriación y negándole a éste la posibilidad de recurrir la resolución administrativa. Se estimaba, en aplicación del art. 18 de la Ley de Jurisdicción Contencioso-administrativa, en conexión con el art. 69.b), que el menor necesitaría para ello la asistencia de la persona que ejerce la patria potestad, esto es, de la Administración tutelante, y que esto determinaba la inadmisión formal de su recurso contencioso-administrativo sin entrar en el fondo del mismo. Este caso llegó finalmente hasta el Tribunal Constitucional español, que declaró, en sendas Sentencias, las número 183 y 184, de 22 de diciembre de 2008, que este proceder provocaba la indefensión del menor y vulneraba el artículo 24 a la Constitución, es decir, el derecho a la tutela judicial efectiva (en este caso frente a las decisiones de la Administración) en su vertiente del acceso a la jurisdicción. A raíz de estas dos Sentencias, el artículo 35 de la Ley Orgánica 4/2000, Ley de Extranjería española, fue modificada en este aspecto por la Ley Orgánica 2/2009, estableciendo que debía darse separadamente audiencia por sí mismos o mediante el representante que designen a los extranjeros menores de dieciocho años y mayores de dieciséis años en los procedimientos administrativos o judiciales relativos a su repatriación. En el caso de menores de dieciséis años con madurez suficiente, que manifiesten una voluntad contraria a la de quien ostenta su tutela o representación, se establece el nombramiento de un "defensor judicial" ajeno a la Administración tutora para su representación. Sobre el tema, in extenso, excúsese la remisión a DURÁN RUIZ, F.J., «Los derechos de los MENA, el despertar a su eficacia real a través de la jurisprudencia», en AAVV, LÁZARO GONZÁLEZ, I., en AA.VV., LÁZARO GONZÁLEZ, I y MOROY ARAMBARRY, B. (Coords.), Menores extranjeros no acompañados, Madrid, Tecnos, 2010, pp. 229-261.

17 Muchos son los proyectos que han desarrollando tanto el Estado y la Agencia de Protección de Datos Personales, como las CCAA y sus respectivas agencias. Destacamos, en este sentido, el proyecto CLI-Promoteo, auspiciado por la Comisión de Libertades e Informática, una Asociación que trabaja para la defensa del derecho fundamental a la protección de datos personales con el objetivo de concienciar a ciudadanos, empresas y Administraciones de la importancia que tiene cumplir la normativa vigente en esta materia. El proyecto cuenta con el patrocinio de la Agencia Española de Protección de Datos, junto con sus homólogas de Cataluña, País Vasco y Madrid, con el apoyo institucional del Ministerio de Educación y Ciencia, así como de las Consejerías de Educación de las Comunidades Autónomas en las que se desarrolla (Cataluña, Madrid, Euskadi, Extremadura y Andalucía). Tiene dos objetivos principales: 1- Concienciar a la comunidad educativa sobre la importancia de la protección de datos de carácter personal (conocimiento y tratamiento de los datos) y de los derechos que les asisten como ciudadanos (acceso, rectificación, cancelación y oposición); y 2-Fomentar el uso adecuado de las Tecnologías de la Información por los alumnos, reduciendo los riesgos que conlleven su mala práctica. Para lograrlos el proyecto realiza un estudio de la realidad actual mediante una encuesta por muestreo y el análisis de los resultados con vistas a la elaboración de un informe y de un manual práctico para la Protección de Datos de Carácter Personal dirigido a la Comunidad Educativa Cfr. a este respecto, la web del proyecto, http://www.asociacioncli.es/?q=node/26 y FARRIOLS SOLÁ, A., "Los menores y adolescentes ante el uso de las Tecnologías de la Información y la Protección de los Datos de Carácter Personal", Revista Base Informática, nº 44, 2009, pp. 44-46.

5. EL DERECHO DE LOS MENORES DE EDAD A LA PROTECCIÓN DE SUS DATOS PERSONALES EN LA LEGISLACIÓN ESTATAL ESPAÑOLA

5.1 LOS MENORES DE EDAD Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), cuenta únicamente en su articulado con dos breves referencias y de carácter accesorio a la protección de los datos personales de

La primera referencia a los menores de edad en la LOPD se realiza en el artículo 7, en el contexto de los denominados "datos especialmente protegidos"). El apartado 6 de dicho artículo, alude a los sujetos que no tienen capacidad jurídica suficiente para prestar su consentimiento, entre los que están menores, aunque no de forma absoluta en aplicación del principio de capacidad progresiva que en su día refirió Tolivar Alas (1991)[19] , y los incapacitados. El consentimiento se requiere expreso cuando se autoriza el tratamiento de dichos datos especialmente protegido[20] , pero el artículo 7.6 LOPD establece que no será necesario el consentimiento expreso cuando el mismo «sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento».

El segundo artículo de la LOPD que se refiere a los menores de edad es el 22.4, de forma aún más tangencial, ya que, al referirse a los ficheros policiales, dispone que «los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento» y que, a tales efectos, «se considerará especialmente la edad del afectado y el carácter de los datos almacenados».

Son muchas más las dudas que suscita la cuestión de la protección de datos de los menores de las que puedan resolver estas breves referencias, en especial su capacidad para consentir en el tratamiento de sus datos, las necesidades de especial protección o de formación específica en relación con su derecho a la intimidad, las especialidades relativas a los datos biométricos o genéticos, o la posibilidad de reclamar el derecho a la protección de datos cuando la vulneración de los mismos se produce en países ajenos a la Carta de Derechos Fundamentales y la CEDH aplicables en el contexto comunitario y europeo.

Los datos personales, en el caso de los menores de edad, gozan desde hace tiempo de protección penal, mientras que no se encontraban amparados de forma explícita por la legislación administrativa de carácter sancionador, puesto que no se incluían medidas de protección específicas para los datos de los menores de edad en el derogado Real Decreto 994/1999, de 11 de junio, Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Esto puede tener diversas lecturas y dar lugar a diversas reflexiones. Lo que resulta indiscutible es el hecho de que el legis-

lador considera tan relevante la protección de los datos personales, que otorga a este derecho la máxima protección frente a su vulneración, castigando penalmente la misma, y prácticamente ante cualquier injerencia, de mayor o menor intensidad. Así, el Título X del Código Penal «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», concretamente en su artículo 197, castiga expresamente determinadas conductas vinculadas a la vulneración del derecho a la protección de datos de carácter personal, agravando la pena cuando los afectados son menores de edad o incapaces[21].

5.2 LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS MENORES Y EL REGLAMENTO DE LA LOPD DE 2007

Tras la aprobación del Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se reguló la cuestión de la prestación por parte de los menores del consentimiento para el tratamiento de sus datos personales.

El artículo 13 de dicho Reglamento establece las reglas para que los menores puedan consentir el tratamiento de sus datos personales. El reglamento ha considerado los catorce años como la edad frontera a la que los menores pueden prestar por sí mismos el consentimiento para el tratamiento de sus datos personales, con excepción de aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela[21] . El consentimiento de padres o tutores para el tratamiento de los datos personales de los menores se exige en todo caso cuando estos tienen menos de catorce años.

Como apuntábamos, a menudo se utiliza a los menores para recabar datos del resto de miembros de su familia o sobre las características y hábitos familiares, especialmente aquellos que puedan ser utilizados para ofrecer productos o servicios que cubran las demandas de la unidad familiar. El apartado 2 del artículo 13 proscribe esta práctica, disponiendo que "en ningún caso podrán recabarse del menor" estos datos del núcleo familiar sin el consentimiento de los titulares de tales datos. El propio precepto pone como ejemplo de tales datos los relativos a la actividad profesional de los progenitores, información económica, datos sociológicos "o cualesquiera otros". Excepciona únicamente los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización por su parte cuando los menores tengan menos de catorce años o la ley así lo exija.

[18] Por razones de espacio, dejo para mejor ocasión el análisis de la legislación autonómica: la Ley 8/2001 (CAM), de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, y la Ley 5/2002 de 19 de abril, de la Agencia Catalana de Protección de Datos, sin olvidar algún reciente Decreto en ámbitos concretos como el Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica en la Comunidad autónoma de Galicia.

[19] Ya hace algunos años se refería TOLIVAR ALAS (1991, 39-40), a la «relevancia jurídica del escalonamiento en la menor edad», explicando desde la casuística legal cómo el niño, desde que comienza a poseer capacidad jurídica –a las veinticuatro horas del alumbramiento–, hasta que cumple los dieciocho años es progresivamente facultado por el Ordenamiento para el desempeño de funciones, con estimación de su voluntad, en conductas que, paulatinamente, van haciendo operativa y relevante para el Derecho la capacidad inherente a la personalidad. Este escalonamiento, según el mismo autor «obedece a un tratamiento lógico de la evolución humana, en la que el juicio y la capacidad de discernimiento van formándose gradualmente durante la niñez y la adolescencia».

[20] El artículo 7.2 de la Ley Orgánica 15/1999 dispone que "sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias", prohibiendo el artículo 7.4 "los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual". Cfr., sobre datos especialmente

No hay que olvidar, como bien apuntaba ante el Congreso de los Diputados[23] el Director de la Agencia Española de Protección de Datos (Rallo Lombarte), que "la oferta de servicios en Internet se basa con carácter general en un modelo de negocio que permite el acceso gratuito de los usuarios, financiado con ingresos de publicidad. Sin publicidad no existiría Internet, tal y como hoy lo conocemos. Las consecuencias de este modelo de negocio son obvias. Por una parte, los servicios de Internet persiguen obtener un conocimiento cada vez más profundo de los hábitos de los usuarios, con el fin de personalizar y hacer más eficaces sus mensajes publicitarios. Esto es, conocer el alma del usuario es la prioridad de los servicios de Internet y su principal activo económico. Ante esta estrategia los legisladores, las autoridades de protección de datos y los propios ciudadanos han de asumir el reto de proteger la privacidad, reaccionando con prontitud ante nuevos desafíos que evolucionan a ritmo vertiginoso" .[24]

Otras garantías adicionales del Reglamento de protección de datos respecto al tratamiento de los datos de menores reside en la exigencia de que la información dirigida a ellos se exprese en un lenguaje que puedan comprender fácilmente, y que explique las condiciones para prestar su consentimiento. Son los responsables de los ficheros o del tratamiento de los datos los obligados por la ley a 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 los padres, tutores o representantes legales.

En este sentido las redes sociales han constituido un auténtico "agujero negro" para la protección de datos personales de los menores, que sólo ha podido ser solucionado mediante la autorregulación, fruto de la responsabilidad de algunos operadores y de instrumentos de colaboración público-privada entre empresas y administraciones[25] . Es necesario darse cuenta que en este campo, el Estado va muy por detrás de las multinacionales que prestan los servicios, y que puede conseguir mejor protección de los derechos de los ciudadanos (y de los menores) con instrumentos de colaboración que con los sancionadores. De ello dan muestras tanto las diversas Agencias de Protección de datos, que están publicando guías y recomendaciones para ayudar a los menores en la protección de este Derecho[26] , como los Defensores del Pueblo estatal y autonómicos, que han publicado diversos informes sobre esta cuestión, ante el crecimiento de las denuncias por vulneraciones de derechos en general, y de la protección de datos en particular.

Instrumentos como el DNI electrónico o la firma electrónica pueden resultar muy útiles para evitar fraudes (muy comunes por otra parte) de los menores para acceder a redes sociales antes de los catorce años sin consentimiento de sus representantes legales. Internet y las redes sociales se han convertido en un instrumento básico para el desarrollo social de los más jóvenes, puesto que les proporcionan un medio gratuito para incentivar y reforzar sus lazos sociales y de pertenencia a un grupo.

Protegidos, TRONCOSO REIGADA, Antonio (Dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Cizur Menor, Thomson-Civitas, 2010, pp. 577-736, que comentan distintos aspectos de los datos especialmente protegidos, en particular su origen y fundamentación, los problemas relativos a los datos de entidades religiosas o partidos políticos, los datos de salud como datos especialmente protegidos, considerando especialmente los datos genéticos y derivados de la investigación biomédica, y las especialidades de la prestación del consentimiento para el tratamiento de los datos relativos a la salud.

[21] El artículo 197 se ubica en el capítulo I "Del descubrimiento y revelación de secretos", del Título X del vigente Código Penal de 1995. En su apartado 2, establece penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses para el que "(...) sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero". Los apartados 3 a 8 del mismo artículo contienen los tipos agravados para estos delitos. Las penas se imponen en su mitad superior si los hechos se producen en relación con datos personales de los que la LOPD cataloga como "especialmente sensibles" (los que revelan la ideología, religión, creencias, salud, origen racial o vida sexual de la persona), y también en aquellos casos en que "la víctima fuere un menor de edad o un incapaz" (apdo. 6). La pena de prisión es de 2 a 5 años si se difunden, revelan o ceden a terceros los datos descubiertos (apdo. 4), y de uno a tres años y multa de doce a veinticuatro meses a los que realizasen estas conductas sin haber tomado parte en el descubrimiento de los datos y conociendo el origen ilícito de los mismos. Se agrava aún más la pena si los autores son las personas encargadas o responsables de la gestión de los datos (apdo. 5). Si la finalidad del delito es lucrativa se imponen las penas en su mitad superior, y si a ello se suma que los datos son de carácter sensible, o de menores o incapacitados, la pena a imponer será de prisión entre cuatro y siete años. Por último, si el delito se comete en el seno de una organización criminal, se aplican las penas superiores en grado. Para un análisis en profundidad de estos delitos, véase, por todos, DE RIASCOS GÓMEZ, L.O., "El derecho a la intimidad, la visión iusinformática y el delito de datos personales", Tesis Doctoral dirigida por Antonio Luis Monreal Ferrer. Universidad de Lérida. 2007.

La normativa no ha sido totalmente ajena a estas cuestiones, aunque difícilmente pueda adaptarse a tiempo a los nuevos retos y a los vertiginosos avances de las TIC, cumpliendo a un tiempo escrupulosamente con las necesarias garantías legales. En este sentido, la normativa española sobre protección de datos, incorporando a su vez la comunitaria, incluyó en el art. 32 un instrumento esencial para esta esencial colaboración público-privada en defensa del derecho a la protección de datos, los denominados "Códigos tipo". Por suerte o por desgracia, y por la posición dominante de la industria, no pasan hoy de ser "soft law", como el propio precepto reconoce expresamente[27], puesto al definirlos como "códigos deontológicos o de buena práctica profesional", que se ven revestidos de un barniz público mediante su inclusión en un Registro administrativo como es el Registro General de Protección de datos. En relación con los menores y los códigos tipo, el artículo 74 del Reglamento, incita a ampliar los compromisos asumidos en estos por las empresas, estableciendo que tales códigos "podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos" (apdo. 1) y que "además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras en algunas materias sensibles, en particular, la protección de menores o de determinados colectivos de afectados" (apdo. 2).

---

[23] Vid. Diario de Sesiones del Congreso, año 2010, IX Legislatura, núm. 668, pp. 22-24. Comparecencia del Director de la AEPD para informar sobre la memoria de la Agencia Española de Protección de Datos correspondiente al año 2009.

[24] Para tratar de adaptarse a estos cambios, desde la UE se han introducido modificaciones en la Directiva noviembre de 2009 se modificó la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, autodenominada "Directiva sobre la privacidad y las comunicaciones electrónicas". Se han ampliado las garantías de los usuarios frente a al la denominada "publicidad basada en el comportamiento" de los internautas, concretando los casos en que resulta legítimo o adecuado usar los "chivatos" o "cookies" , y se ha introducido el deber de comunicar a las autoridades, a los abonados y particulares afectados las quiebras de seguridad.

[25] La la verificación de la edad de los menores en los redes sociales continúa siendo una asignatura pendiente. Dado que las condiciones de uso de los servicios en Internet suelen establecerse unilateralmente por las corporaciones multinacionales que los prestan, la política reactiva ante los incumplimientos resulta insuficiente y como afirma el Director de la AEPD en su informe al Congreso citado supra "Es preciso primar las políticas activas con los proveedores de servicios para que en su diseño y en sus condiciones de uso ofrezcan garantías adecuadas para la protección de la información personal". La Unión Europea ha impuesto a las redes sociales que operan en territorio de sus Estados miembros la incorporación en sus webs de un "botón para reportar abusos", de fácil acceso para los menores. La Agencia ha mantenido contactos con las redes sociales Tuenti y Facebook (las dos principales redes sociales a las que se adscriben los menores en España) para mejorar sus políticas de privacidad e impedir el acceso de menores de 14 años. Para evitar registros por debajo de esa edad. Tuenti ha implantado y está desarrollando medidas que deberían permitir revisar unos 300.000 perfiles anuales, implantando además un sistema de verificación de la edad, lo que da una idea de la magnitud del problema. También Facebook a requerimiento de la agencia ha establecido como edad mínima para poder registrarse desde España la de 14 años, adecuándose a la normativa española. Otros espacios en internet también pueden suponer ciertos riesgos para los jóvenes, destacando especialmente los portales de contactos en los que los adolescentes publican sus imágenes, en ocasiones provocativas, para someterlas a votación y hacer comentarios.

Vid. AEPD, Derechos de niños y niñas y deberes de los padres y madres. Recomendaciones, 2008. Disponible en la web de la Agencia Española de Protección de Datos, www.agpd.es.
«Artículo 32. Códigos tipo.1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo. 2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

[3] Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia Española de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas».

/CONCLUSIONES

El derecho fundamental a la protección de datos es uno de los que están más asediados y sometidos a continuas vulneraciones, ante el empuje del mercado y la importancia que en términos económicos tienen estos datos para las empresas en su búsqueda del máximo beneficio. En el caso de los menores, la amenaza crece de forma inversamente proporcional a la disminución de la percepción del riesgo de no utilizar el derecho a la "autodeterminación informativa" de forma adecuada y responsable.

Las Administraciones en este ámbito juegan con desventaja y en posición de inferioridad respeto a los grandes operadores, y cuentan con menos recursos. Pese a ello, si somos justos, hay que reconocer que no han permanecido impasibles, tienen conciencia de la magnitud del problema y sus logros no deben minusvalorarse. La respuesta penal no resulta adecuada puesto que no evita las vulneraciones del derecho, y lo mismo cabe decir de la respuesta sancionadora de las AAPP. Hasta el momento ambas se muestran insuficientes, por lo que la colaboración público-privada, la regulación desde instancias internacionales (o al menos de la UE) o la autorregulación son los únicos medios que pueden vincular de forma efectiva a las empresas y conseguir una protección efectiva del Derecho. La labor educativa de las AAPP respecto de los menores y sus familias, así como la facilitación de mecanismos ágiles de respuesta ante las vulneraciones resultan también imprescindibles.

En cuanto a las mejoras legislativas, es necesario un reconocimiento y delimitación clara del denominado derecho al olvido y una simplificación de su ejercicio, especialmente en relación con los buscadores y los datos indexados por los mismos. Por otra parte, además de la mejora de los mecanismos para comprobar el cumplimiento de los límites de edad establecidos para consentir el tratamiento de los datos personales y la normalización de la figura del defensor judicial para apoyar a los menores en la autodefensa de sus derechos, sería importante, a nivel legislativo, que los datos personales relativos a menores pasasen a considerarse como datos de los calificados como "sensibles", en la legislación, con el plus de protección que ello proporciona.

/REFERENCIAS

/Ballesteros Moffa, L. Á. (1997). La privacidad electrónica. Internet en el centro de proteccion. Valencia: Tirant lo Blanch y Agencia de Protección de Datos.

/De Riascos Gómez, L. O. (2007). El derecho a la intimidad, la visión iusinformática y el delito de datos personales. Tesis Doctoral dirigida por Antonio Luis Monreal Ferrer, Universidad de Lérida.

/Farriols Solá , A. (2009). Los menores y adolescentes ante el uso de las Tecnologías de la Información y la Protección de los Datos de Carácter Personal. Revista Base Informática, No. 44.

/Gómez-Juárez Sidera, I. (2006). Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la Legislación Española. Revista Aranzadi de Derecho y Nuevas Tecnologías (11).

/Murillo de la Cueva, P., & Piñar Mañas, J. (2009). El derecho a la autodeterminación informativa. Madrid: Fundación Coloquio Jurídico Europeo.

/Pérez Velasco, M. d. (s.f.). Los ficheros públicos. en AAVV, Troncoso Reigada, A. (Dir.), Estudios sobre Administraciones públicas y protección de datos personales, P. 117-142.

/Tolivar Alas, L. (Enero-Abril de 1991). Aspectos jurídico-administrativos de la protección de menores. RAP (No. 124).