LOS MENORES COMO CONSUMIDORES Y LA PROTECCIÓN DE SUS DATOS PERSONALES. UN ANÁLISIS DEL PANORAMA A NIVEL INTERNACIONAL Y EN ESPAÑA[1].

*Mª Belén Andreu Martínez**

SUMARIO: 1. Introducción. 2. La regulación en EUA: la *children´s online privacy protection act*. 3. El tratamiento de los datos personales de los menores en la unión europea. 4. La protección de los datos personales de los menores en España. El artículo 13 del reglamento de protección de datos: 5. Conclusiones.

1. INTRODUCCIÓN

El tratamiento de datos personales de menores de edad y su utilización, entre otros, con fines publicitarios, es cada vez más frecuente y ha generado en los últimos años un gran debate acerca de las medidas que deben adoptarse para aumentar su protección, y sobre el papel que deben jugar los representantes legales (en relación con el consentimiento, acceso a los datos, etc.). A ello hay que añadir el desarrollo de la sociedad de la información y la posibilidad de acceso cada vez más sencilla y frecuente por parte de los menores a las distintas herramientas de Internet y otras tecnologías de última generación[2].

Los riesgos que se derivan de la ingente cantidad de datos que pueden acumularse en la actualidad, tanto por entidades públicas como por empresas privadas, son por todos conocidos. Pero, en el caso de los menores, hay que tener en cuenta una serie de factores que hacen que estos riesgos se incrementen.

En primer lugar, hay que destacar la mayor facilidad para obtener sus datos. La falta de un completo desarrollo y madurez de los menores hace que estos no sean del todo conscientes de los riesgos o de la vulneración que para sus derechos puede suponer el proporcionar información personal. Además, la propia personalidad en la adolescencia, más propensa a asumir riesgos, conlleva que no siempre se pongan reparos a la hora de facilitar datos personales. Por ello, los menores suelen proporcionar datos a terceros sin que esto les preocupe o moleste en especial, como sí sucedería en muchos casos con los adultos.

---

* *Profesora de Derecho civil de la Universidad de Murcia (España).*

[1] Este trabajo se enmarca dentro del proyecto de investigación financiado por el Ministerio de Ciencia e Innovación español: "Los desafíos jurídicos de Internet para la protección de los datos personales: hacia un marco normativo de tercera generación" (ref. DER2009-09157).

[2] Según encuestas del Eurobarómetro de 2008, en Europa el 75% de los niños usan Internet y el número es cada vez mayor entre los más pequeños (6-10 años), que llega al 60% (*vid.* el estudio financiado por la Unión Europea: *EU Kids Online: Final Report, 2009*).

Por otra parte, esta falta de desarrollo o desconocimiento del menor puede ser aprovechado para obtener información no sólo respecto del propio menor, sino sobre terceras personas, en particular sobre la familia (situación económica, religión, etc.). La información tanto del menor como de su familia se suele obtener a cambio de premios, acceso a juegos, etc.

Igualmente, la inmadurez o inexperiencia del menor lo hace más vulnerable frente a la publicidad, en especial, cuando se trata de publicidad engañosa. Los menores no siempre disponen de los elementos necesarios para comprender esa parte de exaltación, a veces exagerada, del producto, o para defenderse frente a una publicidad muchas veces agresiva, y su credulidad puede ser explotada por terceros.

Junto a todo esto, el hecho de disponer de datos de las personas desde edades tempranas abre una gran puerta a la creación de perfiles de personalidad detallados, que pueden ser explotados y ampliados a lo largo de su vida.

En el caso del tratamiento de datos a través de Internet, a los problemas anteriores hay que añadir la brecha generacional en el dominio de las nuevas tecnologías, que hace a los menores mucho más duchos en el manejo de éstas que sus padres, lo que dificulta su tarea de educación, control y protección del menor.

Los problemas específicos en el tratamiento de los datos personales de los menores derivan, como vemos, de su falta de plena capacidad y de tratarse de personas en formación, que precisan, por ello, de una especial protección. No obstante, la legislación en materia de protección de datos no se ha preocupado, hasta fechas recientes, de este sector de la población, aplicándosele sin más las reglas generales sobre protección de datos.

En efecto, las Directivas europeas en la materia (Directiva 95/46/CE, de 24 de octubre; Directiva 2002/58/CE de 12 de julio) no mencionan de manera expresa la protección de datos de los menores de edad. Tampoco lo hace la Ley Orgánica de Protección de Datos Personales española. Ha sido el Reglamento de desarrollo de esta Ley del año 2007 el que ha incluido una regulación con carácter general del tratamiento de los datos personales de los menores de edad en su artículo 13. Pero, evidentemente, la regulación que se contiene en el artículo 13 del Reglamento español no surge de la nada. Este precepto tiene en cuenta los estudios y trabajos previos llevados a cabo sobre todo por los organismos y grupos de trabajo internacionales en materia de protección de datos.

En este artículo analizaremos, en primer lugar, los textos que a nivel internacional han abordado la protección de los datos personales de los menores de edad, principalmente en los

EUA y en la Unión Europea, y que sirven de guía para la regulación de esta materia. Posteriormente, nos centraremos en los requisitos que ha introducido la legislación española para el tratamiento de los datos de los menores, y que son aplicables de cara a su utilización con fines publicitarios.

2. LA REGULACIÓN EN EUA: LA *CHILDREN´S ONLINE PRIVACY PROTECTION ACT*

Los Estados Unidos de Norteamérica promulgaron en 1998 la *Children's Online Privacy Protection Act* (COPPA). Fue una de las primeras normas a nivel internacional dedicadas a la protección de la información personal de los menores de edad, y constituye un modelo de referencia a la hora de abordar la regulación de esta materia.

La COPPA regula el tratamiento por parte de los sitios web de los datos personales de los menores de 13 años de edad, estableciendo una serie de mecanismos para que los padres puedan controlar la información personal que se recaba de sus hijos. Esta Ley tiene su origen en un informe realizado en el año 1996 por la asociación *Center for Media Education* (cuyo título era "Web of Deception: Threats to Children from Online Marketing"), en el que se analizaban las prácticas de recogida de datos de menores en Internet. Como consecuencia de este informe, se inició por parte de la *Federal Trade Commision* (Comisión Federal de Comercio, en adelante, FTC) una campaña de supervisión, que puso de relieve la existencia de numerosos defectos en el tratamiento de datos personales de menores (ausencia de políticas de privacidad, de consentimiento parental, etc.), y que derivó en una petición al Congreso para regular esta materia. En octubre de 1998 se aprobó la COPPA, que se desarrolla mediante unas normas promulgadas por la FTC en noviembre de 1999, y que entran en vigor el 21 de abril de 2000 ("Children's Online Privacy Protection Rule")[3].

La COPPA estadounidense se aplica únicamente a los datos personales recabados *online* de los menores por debajo de los 13 años de edad[4]. Respecto al ámbito subjetivo de aplicación, la Ley afecta a los operadores de sitios web dirigidos a menores, así como a webs dirigidas a un

---

[3] Puede consultarse tanto el texto de la Ley como su normativa de desarrollo aprobada por la FTC en http://www.ftc.gov/privacy/privacyinitiatives/childrens_lr.html

[4] También se contienen en la Ley y sus normas de desarrollo (Sec.1302 (8) de la COPPA y § 312.2 de las normas de desarrollo) una definición de "personal information" o datos personales a los efectos de su aplicación. Ésta incluiría: el nombre; dirección; correo electrónico; teléfono; nº. de la Seguridad Social; información que el menor revele sobre sí mismo o su familia y que se asocie a los anteriores datos; cualquier otro dato identificador que, según la FTC, permita contactar (presencial o virtualmente) con una persona y que se recabe vía *online*. Por lo tanto, el elemento clave para considerar que estamos ante un dato personal protegido por la Ley es que permita identificar y con ello contactar con una persona. Se excluye, en cambio, datos (como por ej., una dirección IP) que no estén asociados a información personal.

público en general que tengan un "conocimiento efectivo" de que están tratando datos personales de dichos menores. Ese "conocimiento efectivo" se puede adquirir, por ejemplo, si se recaba la edad o fecha de nacimiento de la persona. En cualquier caso, la COPPA no obliga a estos operadores de webs genéricas a comprobar la edad del usuario que facilita sus datos personales.

Los principios que establece la COPPA para el tratamiento de los datos personales de los menores en los supuestos descritos anteriormente son los siguientes: 1) Es necesario dar publicidad de las políticas de privacidad sobre el tratamiento de datos de los menores; 2) Hay que informar y obtener el previo consentimiento de los padres o representantes legales del menor para el tratamiento de sus datos personales; 3) Se reconoce a los padres el derecho a acceder y conocer los datos personales recabados del menor, solicitar la cancelación de los mismos y rechazar cualquier recogida o tratamiento posterior, debiendo establecerse los mecanismos para ejercitar estos derechos; 4) Se prohíbe condicionar la participación de un menor en un juego, la obtención de un premio o cualquier otra actividad a la comunicación de más datos de los necesarios para tomar parte en dicha actividad; 5) Es necesario adoptar mecanismos de protección de la confidencialidad, seguridad e integridad de los datos personales de los menores.

Tanto la Ley como sus normas de desarrollo hacen especial hincapié en el primero de los principios señalados, esto es, el de la publicidad de las políticas de privacidad sobre el tratamiento de datos de los menores[5]. Se dispone, así, que las políticas de privacidad deben estar redactadas de forma clara y comprensible, el enlace a las mismas debe encontrarse en la página principal y en cada una de las páginas en las que se recaben datos personales de los menores, debiendo ser dicho enlace claro y fácilmente visible en estas páginas (no lo sería, por ej., un enlace en letra muy pequeña), y, además, se establece su contenido mínimo obligatorio (identificación del operador, datos personales que se solicitan y forma en que se recaban, finalidad para la que serán tratados, etc.).

Otro de los elementos fundamentales de la Ley es la información y consentimiento de los representantes legales. El operador del sitio web debe informar a los padres sobre su intención de recabar datos personales del menor, sobre el contenido obligatorio de las políticas de privacidad al que se acaba de hacer referencia, así como de los mecanismos para prestar el

[5] *Vid.* § 312.4 de las normas de desarrollo de la FTC.

consentimiento. También deberá informar de cualquier modificación posterior en las condiciones del tratamiento[6].

Antes de recabar o ceder datos personales del menor, se debe contar con el consentimiento de los representantes legales[7]. Para ello, los operadores de sitios web deben realizar "esfuerzos razonables", teniendo en cuenta la tecnología disponible, para conseguir el consentimiento parental y asegurar que la persona que lo presta es el progenitor del menor[8]. Las vías para conseguir este consentimiento de forma "verificable" es uno de los aspectos más polémicos de la Ley. La FTC ha propuesto una serie de mecanismos que varían según el uso que se pretenda dar a los datos personales de los menores (lo que se ha denominado "sliding scale").

De esta manera, cuando los datos recabados van a utilizarse únicamente para fines internos de la propia empresa (por ej., envío de comunicaciones o publicidad al menor) y no se van a comunicar a terceros, se admite un método sencillo (denominado "email plus"): el consentimiento del progenitor a través de un correo electrónico (conforme a la dirección proporcionada por el propio menor), unido a otros mecanismos adicionales para asegurarse de que ha sido éste quien ha otorgado el consentimiento (ej., solicitando confirmación a través de otro e-mail, carta o llamada telefónica). En cambio, se establecen mecanismos más exigentes si los datos van a ser comunicados a terceros o publicados en una web: entre otros, enviar al progenitor un documento de consentimiento para su firma y posterior remisión por correo o fax; la utilización por el progenitor del número de una tarjeta de crédito en relación con una transacción; mediante una llamada del progenitor a un teléfono gratuito encomendado a personal entrenado al efecto (para distinguir voces o contestaciones adultas); o a través de correo con firma electrónica[9].

---

[6] § 312.4 (c) de las normas de desarrollo de la FTC.

[7] Salvo que concurra alguna de las excepciones previstas por la COPPA al consentimiento parental previo (Sec 1303 (b) (2) de la COPPA; y § 312.5 (c) de las normas de desarrollo de la FTC). Así, por ej., se pueden recabar los datos de nombre y correo electrónico para poder solicitar el consentimiento de los padres; se puede tratar la dirección de correo electrónico del menor para contestar a una única solicitud del mismo, si después se borra la información ("one-time contact exception"); o también cuando dicha solicitud del menor requiere más de una contestación (aunque en este caso es necesario informar a los padres para que puedan oponerse al tratamiento; ej., para enviar un boletín informativo); también se pueden recopilar datos del menor para proteger su seguridad, la del sitio web o para el cumplimiento de obligaciones legales impuestas al sitio web o a petición judicial.

[8] *Vid*. § 312.5 (b) de las normas de desarrollo de la FTC.

[9] Un análisis de los principales aspectos de esta Ley y los problemas de aplicación de los sistemas de verificación de edad y obtención del consentimiento parental, puede consultarse en WARMUND, J., "Can COPPA work? An analysis of the parental consent measures in the Children's Online Privacy Protection Act", *Fordham Intellectual Property, Media and Entertainment Law Journal*, Autum 2000; SKOZA, B./THIERER, A., *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, The Progress & Freedom Foundation, June

Por último, la COPPA recoge unas normas de "puerto seguro" ("safe harbor"), en las que se potencia la autorregulación por parte de la industria. De esta manera, las empresas o grupos de empresas pueden presentar a la FTC para su aprobación códigos autorregulatorios ("Self-regulatory Guidelines") en los que se concreten los criterios para el tratamiento de los datos personales de menores de edad. Una vez aprobado el Código por la FTC, su aplicación por parte de una empresa debe asegurarle el cumplimiento de las obligaciones establecidas en la COPPA.

De entre los Códigos aprobados por la FTC, destaca el primero de ellos (aprobado en enero de 2001), presentado por la *Children's Advertising Review Unit* (CARU)[10]. Se trata de un código de buenas prácticas impulsado por la industria de la publicidad, y que pretende regular la que se dirige a los menores por cualquier medio[11]. Su última versión es del año 2009. En él se recogen, por un lado, una serie de principios aplicables a la publicidad dirigida a los menores en general, y con los que se pretende evitar que la publicidad explote la inexperiencia o falta de madurez del menor[12]. Además, dispone de una sección específica sobre privacidad online de los menores, en la que se recogen los principios establecidos en la COPPA y se detallan cuestiones como los mecanismos de verificación de edad y los enlaces entre webs. Así, por ejemplo, se establece la obligación de informar de forma clara y detallada en la web sobre los datos que se van a recabar y los mecanismos que se utilizarán para ello (directos o indirectos), las finalidades del tratamiento, si se van a comunicar a terceros, la obligación de obtener el consentimiento de los representantes legales del menor, la prohibición de que se recaben más datos de los necesarios para la actividad de que se trate, etc. Las webs en las que es previsible un número significativo de usuarios menores de edad deberán incorporar pantallas de verificación de edad, establecidas de forma neutral (en cuanto a las preguntas que se realicen[13]), junto con otros medios tecnológicos que aumenten su eficacia (ej. uso de *cookies* que eviten dar marcha atrás para modificar la edad una vez denegado el acceso al menor).

2009; JASPER, M.C., *Privacy and the Internet: Your expectations and rights under the law*, Oxford University Press, New York, 2009, p. 57 y ss.

[10] Actualmente hay aprobados cuatro códigos autorregulatorios. Puede consultarse la información al respecto en http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.

[11] El Código se denomina "Self-Regulatory Guidelines for Children's Advertising" y puede consultarse en http://www.caru.org/guidelines/.

[12] Por ej., se hace mucho hincapié en la forma en que debe presentarse la publicidad para que no induzca a error al menor sobre qué es lo que se presenta y en que la información se adapte a su capacidad de entendimiento, en no animar al menor a que pida a sus padres o terceros la compra de un producto, o en otras medidas de presión para la compra (mediante la utilización de palabras como "cómpralo ya", "cuesta sólo…"), en los requisitos para el uso de personajes famosos en la publicidad a menores, de los "Kid's Club", etc.

[13] Se trata de que las preguntas que se realicen estén destinadas a conocer la edad real del usuario, y no se redacten de tal forma que pretendan evitar la aplicación de la Ley. Por ej., permitiendo que el usuario establezca su edad real, en lugar de poner casillas predeterminadas del estilo "tengo más de 12 años", etc. Se sigue con ello las indicaciones que había dado la FTC sobre el tema.

La CARU realiza además una labor de revisión, evaluando las webs dirigidas a menores, para comprobar que cumplen con la COPPA y su normativa de desarrollo. Si detecta violaciones de la legislación, lo pone en conocimiento del sitio web en cuestión y, en caso de que no se rectifique, lo notifica a la FTC para que se inicien las acciones oportunas de responsabilidad[14].

3. EL TRATAMIENTO DE LOS DATOS PERSONALES DE LOS MENORES EN LA UNIÓN EUROPEA

Como hemos señalado anteriormente, las principales Directivas europeas en materia de protección de datos (Directiva 95/46/CE, de 24 de octubre, de protección de las personas frente al tratamiento de sus datos personales y a la libre circulación de estos; Directiva 2002/58/CE de 12 de julio, sobre privacidad y comunicaciones electrónicas) no contienen una regulación específica del tratamiento de los datos personales de los menores de edad. Pero ello no significa que esta materia no sea objeto de atención. En particular, las autoridades de control en materia de protección de datos de los Estados miembros, a través de diversos grupos de trabajo, han abordado la problemática que plantea el tratamiento de los datos de los menores en distintos ámbitos. Aquí vamos a centrarnos en dos de estos grupos de trabajo: el denominado Grupo de Berlín (*International Working Group on Data Protection in Telecomunications*, en adelante, IWGDPT) y el Grupo de Trabajo del Artículo 29 (en adelante, GdT).

3.1. El Grupo de Berlín

El IWGDPT se creó a instancia de la autoridad de control del Länder de Berlín, donde tiene su sede, por lo que se le conoce también como "Grupo de Berlín". Su objetivo principal es el estudio de las implicaciones que tienen las telecomunicaciones en la intimidad y la protección de los datos personales de los individuos. En marzo de 2002, en el marco del 31º Encuentro del Grupo de Trabajo, se adoptó en Auckland (Nueva Zelanda), el Documento de Trabajo: "La privacidad de los menores en Internet: El papel del consentimiento parental"[15]. Como su nombre

[14] Esto fue, por ej., lo ocurrido en el caso de la empresa UMG Inc., que se saldó con una sanción de $400.000 por incumplimiento de la COPPA. La CARU denunció a esta empresa discográfica que disponía de diversas webs de promoción de sus productos. Alguna de ellas estaba dirigida a menores (por las estrellas del pop y las actividades que contenía), y las webs genéricas recababan el dato de fecha de nacimiento, por lo que tenían un "conocimiento efectivo" de que trataban datos de menores, sin consentimiento previo de sus representantes legales.

[15] Puede consultarse en http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt

indica, en él se analiza cuándo es necesario contar con el consentimiento de los representantes legales del menor para el tratamiento de sus datos personales en el contexto de Internet.

Ante todo, el Grupo de Trabajo reconoce en dicho documento la dificultad de establecer unos estándares sobre consentimiento parental de forma clara y práctica, aplicables internacionalmente. Por un lado, determinar cuándo el consentimiento de los padres es preciso atendiendo a la madurez del menor no es viable en el contexto de Internet, en el que difícilmente se puede analizar dicha circunstancia. Por otro lado, acudir a la edad como criterio objetivo plantea también el problema de su comprobación por este medio. En cualquier caso, se señala que el consentimiento parental sólo debe entrar en juego cuándo sea necesario para representar los intereses más favorables del menor, evitando que se convierta en un mecanismo de control parental en circunstancias donde la intervención de los padres no es necesaria. Igualmente se destacan los problemas que en la práctica plantea el hecho de que el consentimiento parental, cuando éste sea preciso, debe ser verificable. Ahora bien, la dificultad de obtener un consentimiento parental verificable no debe llevar a estándares menos restrictivos que puedan colocar en riesgo a los menores. Se trata de una obligación que debe asumir el responsable del tratamiento si quiere recabar datos de menores.

En el documento se establecen una serie de recomendaciones para el tratamiento *online* de los datos personales de los menores de edad. Es importante destacar que en dicho documento se entiende por menor el individuo por debajo de los 16 años de edad. En relación con estos menores se establecen, entre otras, las siguientes recomendaciones: obtención del consentimiento verificable de los representantes legales del menor, tanto para el tratamiento, como para la cesión o difusión pública de sus datos; la información o publicidad dirigida a los menores no debe explotar su falta de experiencia o credulidad; no debe incitarse a los menores a que divulguen sus datos personales a cambio de regalos o similares; no debe utilizarse al menor para obtener información de terceros (ej. padres); los menores puede dejar sin efecto el consentimiento prestado por sus representantes legales una vez alcancen la madurez suficiente para decidir por sí mismos[16].

3.2. El Grupo de Trabajo del Artículo 29

Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE, describiéndose sus funciones en el artículo 30. Se trata de un organismo de la UE, con carácter consultivo e

[16] Un análisis del documento puede consultarse en GÓMEZ-JUÁREZ SIDERA, I., "La protección de los datos del menor como e-consumidor", en COTINO HUESO, L. (coord.), *Consumidores y usuarios ante las nuevas tecnologías,* Tirant lo Blanch, Valencia, 2008, p. 729 y ss.

independiente, para la protección de la intimidad y los datos personales de los ciudadanos, formado, entre otros, por las autoridades de control en materia de protección de datos de los Estados miembros. A pesar de su carácter meramente consultivo, goza de gran autoridad y reconocimiento en esta materia. De ahí que sus documentos de trabajo marquen las pautas de actuación en las principales cuestiones que afectan a la protección de datos.

El GdT ha abordado tangencialmente el tema de los menores en distintos documentos de trabajo[17]. Así, principalmente, el Dictamen 3/2003, relativo al Código de conducta europeo de la FEDME sobre comercialización directa; el Dictamen 5/2005, sobre geolocalización; el Dictamen 3/2007, sobre visados y biometría; o el Dictamen 5/2009, acerca de las redes sociales.

Pero, además, ha elaborado un documento específico en el que se analiza con carácter general el tratamiento de los datos personales de los menores: el Documento de trabajo 1/08, de 18 de febrero (WP 147), sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios). Vamos a analizar a continuación las ideas básicas contenidas en algunos de estos documentos.

3.2.1. EL CÓDIGO DE CONDUCTA EUROPEO SOBRE LA COMERCIALIZACIÓN DIRECTA

Consideramos de especial trascendencia este Código en la medida en que recoge un conjunto de buenas prácticas a nivel europeo en el tratamiento de datos personales para la industria del marketing directo. Este Código fue analizado en el Dictamen 3/2003, de 13 de junio (WP 77), en el que se destaca la importancia de la protección de los menores en cuanto consumidores, y se considera que las medidas incorporadas al Código para su protección ofrecen suficiente valor añadido. No obstante, aconseja el GdT seguir desarrollando estas medidas para el contexto de la recogida de datos en línea, en donde la protección de los menores es fundamental, y para ello señala como modelo el de la COPPA estadounidense.

Este desarrollo se llevó a cabo a través de un Anexo, que fue objeto de revisión por el GdT a través del Dictamen 4/2010, de 13 de julio (WP 174). En el apartado sexto de este Anexo se recogen una serie de medidas para la protección de los menores. Entre ellas, se señalan algunas básicas, como la obligación de contar con el consentimiento de los representantes legales del menor para el tratamiento de sus datos (cuando éste no tenga capacidad para prestar dicho consentimiento de conformidad con la legislación nacional aplicable), o la prohibición de obtener datos de otros miembros de la familia o de terceros a través del menor (salvo los datos de los representantes legales con la finalidad de obtener el consentimiento parental). Pero

[17] Pueden consultarse en http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

además, destacan otras, como la de considerar ilícito solicitar al menor la revelación de datos sensibles (tales como origen racial, étnico, religión, opiniones políticas, datos de salud, vida sexual, o situación financiara del propio menor o de terceros) sin previo consentimiento parental; o incentivar al menor para que proporcione datos personales con fines publicitarios a cambio de premios o de participar en juegos, sorteos, etc.

En cualquier caso, el propio Anexo remarca que corresponde al responsable del tratamiento adoptar las medidas que garanticen de modo efectivo, usando esfuerzos razonables, la edad del menor y la autenticidad del consentimiento prestado por los representantes legales, eso sí, teniendo en cuenta que no existe a día de hoy un método fácilmente accesible y aceptado universalmente de verificación de edad en Internet.

3.2.2. La geolocalización de menores

Este tema se aborda en el Dictamen 5/2005, de 25 de noviembre (WP 115), sobre el uso de los datos de localización con vistas a prestar servicios de valor añadido. En él se dedica un apartado específico al tema de la localización de menores como servicio que se puede ofrecer a los padres a través, por ej., del uso de los teléfonos móviles. El GdT destaca la necesidad de mantener en este tema un equilibrio entre los distintos intereses y derechos en juego, de manera que el deseo de los proveedores de servicio de posicionarse en un mercado en expansión no ponga en riesgo principios básicos en materia de protección de menores, como "el interés superior del niño" o su derecho a la intimidad. Y es que, como señala el GdT, con este tipo de servicios se corre el riesgo de perturbar las relaciones normales de confianza mutua entre padres e hijos, además del peligro de acostumbrar a las personas desde edades muy tempranas a estar permanentemente controlados, de manera que cuando sean adultas ya no lo perciban como una intromisión en sus derechos. De ahí que el documento aborde el tema del consentimiento del menor a ser objeto de localización, así como la necesidad de garantizar la identificación y restringir el servicio a los padres.

En cualquier caso, es de alabar que el documento avise ya sobre la necesidad de controlar el uso de estas herramientas tecnológicas que afectan de forma importante a la intimidad y autonomía, por lo que a nosotros interesa, de los menores.

3.2.3. Redes Sociales

El Dictamen 5/2009, de 12 de junio (WP 163) aborda el tema de las redes sociales en línea, de enorme actualidad y que está planteando grandes retos para la protección de la privacidad de las personas. En el documento se recogen medidas que intentan garantizar el

cumplimiento del Derecho comunitario por parte de los proveedores de SRS (servicio de red social), en la medida en que son responsables de tratamientos de datos. En este sentido, se establecen una serie de obligaciones para los SRS, como la de informar a los usuarios sobre su identidad, vías de captación de datos personales y finalidades del tratamiento, establecimiento de parámetros de confidencialidad por defecto respetuosos con la intimidad, recomendar a los usuarios no introducir información o imágenes de terceros sin su consentimiento, no tratar datos sensibles sin consentimiento expreso, suprimir los datos personales con la actualización o supresión de la cuenta y establecer períodos máximos de conservación para las cuentas inactivas, etc.

Pero, además, en la medida en que los menores constituyen un importante número de usuarios de estos servicios, deben adoptarse acciones específicas para su protección, con el fin de limitar los riesgos que para su intimidad conlleva el uso de estas herramientas. No hay que olvidar que el principio rector del "interés superior del menor" está igualmente presente en el ámbito de las redes sociales.

Ante las dificultades para la comprobación de la edad y la prueba del consentimiento parental, el GdT propone adoptar una estrategia pluridimensional para abordar la protección de los datos de los menores en este ámbito. Esta estrategia incluiría iniciativas de sensibilización (a través de los distintos agentes implicados en el ámbito escolar), tecnologías que mejoren la protección de la intimidad (parámetros por defecto respetuosos con la intimidad, programas informáticos de verificación de edad…), autorregulación por la propia industria (a través de Códigos de buenas prácticas que incluyan medidas de ejecución eficaces y sanciones disciplinarias), y medidas legislativas *ad hoc* que desalienten prácticas desleales y fraudulentas. En particular, se considera como tratamiento justo y legal contar con el consentimiento previo de los padres antes del registro o no pedir datos sensibles. Pero son especialmente interesantes dos de las medidas propuestas: el establecer grados de separación adecuados entre las comunidades de de niños y adultos[18], y el no realizar comercialización directa destinada específicamente a menores[19].

---

[18] Con lo que se pretende conseguir una mayor seguridad de los primeros, reduciendo en la medida de lo posible los contactos "peligrosos", pero sin eliminar la relación con los adultos necesaria para su formación.

[19] Además de este dictamen, en el ámbito de las redes sociales es importante tener en cuenta los "Principios de la Unión Europea para Redes Sociales más seguras", promovidos por la Comisión Europea a modo de Código autorregulatorio, y que han sido adoptadas en el año 2009 por veinte de las principales redes sociales que operan en Europa. En él se contienen siete principios básicos, que tienen como finalidad aumentar la seguridad de los menores en el uso de las redes sociales. Adicionalmente, la Comisión ha promovido una evaluación por expertos independientes sobre la implementación de estos principios por los operadores firmantes. Las conclusiones de esta evaluación se hicieron públicas en febrero de 2010, y han dado lugar a ciertas modificaciones por parte de las redes sociales para adecuarse a los defectos de cumplimiento señalados en el informe. Puede consultarse la documentación

3.2.4. DIRECTRICES GENERALES EN EL TRATAMIENTO DE LOS DATOS DE LOS MENORES Y EN EL ÁMBITO ESCOLAR

Como se ha señalado anteriormente, el GdT adoptó un documento en el año 2008 en el que se analiza con carácter general el tratamiento de los datos personales de los menores y su aplicación al ámbito escolar. Se trata del Documento de trabajo 1/08, de 18 de febrero (WP 147), sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios)[20]. Con él se pretende reforzar el derecho fundamental de los niños a la protección de sus datos personales, y recoge de una manera estructurada los principios fundamentales para la protección de los datos de los menores, para posteriormente aplicarlos específicamente al ámbito escolar.

En el documento se señalan, por un lado, los principios fundamentales que rigen en materia de protección de menores, y que se contienen en los principales instrumentos internacionales sobre la materia (entre otros, el Convenio de la ONU sobre los derechos del niño de 1989) y, por otro, su aplicación al ámbito de la protección de datos, a la vista de los principios básicos en la materia que se contienen en la Directiva 95/46/CE. Por último, se ilustra con referencias al ámbito escolar[21].

Por lo que se refiere a los principios fundamentales para la protección de los menores, incorporados actualmente a la mayor parte de las legislaciones nacionales, destaca el "interés superior del niño" como principio rector en la materia. Además, se señalan la necesidad de una mayor "protección y cuidado", al tratarse de personas en formación; la titularidad en cuanto seres humanos de los derechos fundamentales, entre ellos, del derecho a la intimidad; la "representación legal" para el ejercicio de sus derechos, representación que debe estar adaptada al grado de madurez del menor, de manera que vaya adquiriendo una mayor capacidad conforme aumente su desarrollo físico y psicológico; y el "derecho a ser oído" en las cuestiones que le afecten. Como señala el propio documento, estos principios se aplican igualmente en el ejercicio de los derechos a la protección de datos. Se ponen como ejemplos, entre otros, el relativo al consentimiento, que dará lugar a distintas soluciones atendiendo al grado de madurez del menor (desde la mera consulta, al consentimiento paralelo de representante y menor, y el consentimiento único del menor cuando sea maduro para el acto de que se trate). Además, una

---

al respecto en la siguiente dirección: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm

[20] Que posteriormente da lugar al Dictamen 2/2009, de 11 de febrero (WP160), sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas).

[21] Un amplio análisis de este documento puede consultarse en PÉREZ LUÑO, A.E., "La protección de los datos personales del menor en Internet", *Revista Española de Protección de Datos,* nº 5, julio-diciembre 2008, p. 44 y ss.

vez que ha alcanzado la mayoría de edad, podrá dejar sin efecto el consentimiento prestado por su representante para el tratamiento de sus datos. También destaca el documento el posible conflicto entre el derecho a la intimidad y el interés superior del menor, que en ciertos casos puede implicar que el primero ceda ante el segundo (ej., respecto a datos médicos, cuando un servicio de bienestar juvenil necesite información de un menor en caso de abusos; o la información proporcionada por un profesor a un trabajador social par proteger al niño física o psicológicamente).

En cuanto a los principios en materia de protección de datos recogidos en la Directiva 95/46/CE y su coordinación con los anteriores, analiza el documento el de calidad de los datos, legitimidad, seguridad y los derechos del interesado en esta materia. Así, por ejemplo, en relación con la calidad de los datos y atendiendo al desarrollo constante de los niños, se hace hincapié en la obligación de mantener los datos actualizados, o en el "derecho al olvido", con la correspondiente cancelación de la información, que cobra especial relevancia cuando se trata de menores. En relación con la legitimidad, deben tenerse presentes los principios del interés superior del niño y la representación. La actuación del representante legal a la hora de otorgar el consentimiento debe estar guiada en todo momento por el interés superior del menor. No obstante, en determinados casos el menor puede ser lo suficientemente maduro como para decidir por sí mismo y, en consonancia, permitir el tratamiento de sus datos (ej. en un contexto médico). Por otra parte, son de especial trascendencia el derecho a la información y el derecho de acceso. El documento señala que la información que se preste a los menores deberá estar adaptada a sus capacidades de comprensión, expresándose en un lenguaje sencillo y conciso, y presentada en el lugar y momento correctos (ej., en un entorno *online*, en pantalla antes de recabar la información). En cuanto al derecho de acceso a los datos personales, se analiza el aspecto especialmente problemático de quién puede ejercitarlo. Normalmente serán los representantes legales, aunque dependiendo del grado de madurez, puede ejercitarse junto con el menor o éste por sí solo. En determinados contextos (ej. ámbito médico o datos sexuales), puede plantearse la posibilidad de que los menores se opongan al acceso por parte de sus representantes legales. En la solución habrá que tener en cuenta los distintos intereses de las partes implicadas y, en especial, el interés superior del niño.

Por último, el documento estudia de forma especial el tema de la protección de los datos de los menores en el ámbito escolar. En concreto, se recogen los principios aplicables a los ficheros de alumnos, señalándose, entre otras cuestiones, los límites a la publicación de los resultados escolares. También se analizan distintas cuestiones sobre protección de datos relacionadas con la vida escolar. Así, por ejemplo, la utilización de datos biométricos para el control de accesos (que, en determinadas situaciones, puede considerarse desproporcionada,

debiendo tener los padres un método sencillo para oponerse al tratamiento); el uso de videovigilancia con fines de seguridad (que deberá responder de manera especial al principio de proporcionalidad, de manera que sólo deben instalarse cuando el objetivo no se pueda conseguir con un método menos intrusivo, y deberá hacerse en lugares o momentos que menos afecten al derecho a la intimidad -ej., en las entradas o salidas del colegio, en horarios no lectivos, etc.-); la utilización de fotografías de los menores (que deberá contar con su consentimiento o el de sus representantes legales); o el uso de los teléfonos móviles (advirtiendo a los alumnos sobre las infracciones que para el derecho a la intimidad de terceros pueden suponer las grabaciones de vídeo, audio o fotografías).

En conclusión, el documento destaca cómo la protección eficaz de los datos personales de los menores implica la aplicación de la legislación sobre protección de datos a la vista del "interés superior del menor" y el resto de principios contenidos en los Convenios internacionales de protección de menores. El documento hace especial hincapié en el ámbito escolar, no sólo como el primer nivel en el que el GdT ha querido analizar la protección de los datos de los menores, sino también como el primer ámbito en el que los menores deben aprender la importancia de la intimidad y la protección de sus datos. Para el GdT, esta materia debería incluirse en los planes de estudio, de manera que en el futuro les permitiera adoptar decisiones informadas sobre qué datos desean o no divulgar, a quién y en qué condiciones. También se destaca un aspecto que consideramos decisivo en la sociedad actual, y es la necesidad de equilibrio entre la intimidad de los menores y su seguridad. Debe evitarse un control excesivo de los menores que limite su autonomía.

4. LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS MENORES EN ESPAÑA. EL ARTÍCULO 13 DEL REGLAMENTO DE PROTECCIÓN DE DATOS.

En España, la Ley Orgánica de Protección de Datos Personales de 1999 (Ley Orgánica 15/1999, de 13 de diciembre, en adelante, LOPD) no dedicó ningún artículo a regular específicamente la protección de los datos personales de los menores de edad, por lo que les eran aplicables las reglas generales recogidas en la legislación sobre protección de datos[22].

[22] Sobre la necesidad de establecer una protección reforzada para el tratamiento de los datos personales de los menores de edad (por ej., a través de un consentimiento expreso para el tratamiento de sus datos personales, o por medio del régimen de infracciones y sanciones), vid. GÓMEZ-JUÁREZ SIDERA, I., "Reflexiones sobre el derecho a

Paralelamente, este sector de la población se ha ido convirtiendo en un importante nicho de mercado para empresas y entidades, lo cual se ha acrecentado con la generalización del uso de las nuevas tecnologías[23]. En efecto, junto a los aspectos positivos que para el desarrollo del menor puedan tener las TIC's, no se puede obviar los importantes riesgos que conllevan para su derecho a la intimidad e incluso su seguridad[24]. De ahí que sea habitual observar cómo el menor facilita sus datos personales a multitud de empresas u organizaciones a veces de manera inconsciente y, en cualquier caso, de forma poco controlada.

Hay que esperar hasta la promulgación del Reglamento de desarrollo de la LOPD en el año 2007 (Real Decreto 1720/2007, de 21 de diciembre, en adelante Reglamento), para encontrar la primera norma que regula con pretensiones de generalidad el tratamiento de los datos personales de los menores de edad. Se trata del artículo 13 del Reglamento, que establece básicamente las condiciones para la prestación del consentimiento por parte de los menores para el tratamiento de sus datos personales. Esta norma no solo recoge algunos de los criterios asentados en los textos internacionales que han sido objeto de estudio en los apartados anteriores, sino que incorpora la doctrina que al respecto había ido creando la Agencia Española de Protección de Datos (en adelante, AEPD) en sus informes y resoluciones[25].

En este apartado analizaremos las principales cuestiones reguladas en el artículo 13 del Reglamento español, en particular, el deber de información y la capacidad del menor para consentir el tratamiento de sus datos[26]. El análisis del artículo 13 será completado con la referencia a una norma de carácter autorregulatorio, como es el Código Tipo "Confianza Online", en el que se concreta el tratamiento de datos de los menores en el ámbito de la publicidad y el comercio electrónico.

---

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*, nº 11, 2006, p. 73 y ss.

[23] Sobre las prácticas publicitarias de las empresas con los menores, *vid.* STEEVES, V., "It's not child's play: The online invasion of children's privacy", University of Ottawa Law & Technology Journal, 169, 2006.

[24] Señala PEREZ LUÑO, A.E., *ob. cit.*, p. 36 y ss., cómo la revolución tecnológica comunicativa ha redimensionado las relaciones del menor con su espacio vital (aumentando su visión del mundo), con los demás (enriqueciendo sus relaciones sociales) y consigo mismo (permitiéndole un mayor conocimiento de sí mismo).

[25] Junto a ello, tanto la AEPD como las Agencias de las Comunidades Autónomas, han creado diverso material de carácter formativo y orientador sobre la protección de su intimidad y datos personales, dirigido a los propios menores, padres, profesores, etc. Así, por ejemplo, la AEPD ha elaborado guías para el tratamiento de datos de los datos de los menores de edad y para los usuarios de Internet (incluido menores). También las Agencias autonómicas, junto con la Comisión de Libertades e Informática han creado guías para el uso de las TIC's por edades (hasta los 11 años, de 12 a 14 y de 15 a 17 años). Pueden consultarse en las webs de las distintas Agencias: http://www.agpd.es, http://www.apdcat.net, http://www.avpd.euskadi.net, http://www.apdcm.org.

[26] No entraremos a analizar otras cuestiones que plantean también importantes problemas, como los derechos ARCO en materia de protección de datos (acceso, rectificación, cancelación y oposición), y cuándo pueden ejercitarse por el menor o cuándo por los representantes legales. Esta cuestión no está regulada en el art. 13 del Reglamento, haciéndose únicamente una referencia general en el art. 23. Sobre el tema pueden consultarse los informes de la AEPD 409/2004, 466/2004, 227/2006, 114/2008, sobre acceso por los padres a los datos sanitarios y escolares de sus hijos.

4.1. El consentimiento del menor para el tratamiento de sus datos personales

4.1.1. LA CAPACIDAD PARA CONSENTIR

Un tema que ha suscitado mucho debate, incluso antes de la entrada en vigor de la LOPD, ha sido el de la posibilidad de que los menores presten por sí solos el consentimiento para el tratamiento de sus datos personales. El artículo 13 del Reglamento entra de lleno en esta cuestión estableciendo en su apartado 1º que "*podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento*". Con ello, se establece en principio la barrera de los 14 años en relación con el ejercicio del derecho fundamental a la protección de datos.

El criterio recogido en este precepto sigue las líneas de actuación marcadas por las normas que regulan la capacidad del menor de edad. Como ya se ha señalado, en la actualidad el principio comúnmente aceptado en relación con la capacidad de obrar de los menores es el de su adquisición progresiva conforme al desarrollo físico y mental.

En el Derecho español, este principio se recoge con carácter general en el artículo 162.2.1º del Código Civil, que excluye de la representación legal de los padres "los actos relativos a derechos de la personalidad u otros que el hijo, de acuerdo con las Leyes y con sus condiciones de madurez, pueda realizar por sí mismo". Para los derechos de la personalidad, este mismo criterio se establece en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil de los derechos al honor, intimidad y propia imagen, que remite a las "condiciones de madurez del menor" a la hora de permitir que éste pueda prestar el consentimiento para la intromisión legítima en estos derechos (art. 3). La Ley Orgánica 1/1996, de protección jurídica del menor se inserta también en esta tendencia de reconocer una progresiva capacidad de obrar al menor de acuerdo con su proceso evolutivo. Así, en su artículo 2, se establece un principio general de interpretación restrictiva de las limitaciones a la capacidad de obrar de los menores.

Por tanto, el criterio a tener en cuenta para determinar la capacidad del menor a la hora de ejercitar por sí mismo un determinado derecho es el de las "condiciones de madurez", condiciones que no se alcanzan con carácter general a una edad específica, sino que para determinarlas habrá que atender al acto de que se trate y a la edad del menor. Lo que sí encontramos en el Derecho español son normas dispersas que establecen para determinados actos una edad concreta en la que se adquiere capacidad. Edad que varía de unos supuestos a otros, aunque suele estar en el arco de los 12 a los 16 años. Por citar algunos casos, a partir de los 12 años el menor debe consentir su acogimiento o adopción (art. 173 y 177 Código Civil), o puede otorgar consentimiento matrimonial a partir de los 14 con dispensa judicial (art. 46.1

Código Civil). En el ámbito sanitario, se establece con carácter general que a los 16 años el menor puede consentir por sí sólo un acto clínico, pero antes de esa edad también podría hacerlo por sí mismo si "es capaz de comprender intelectual y emocionalmente el carácter de la intervención" (art. 9.3 Ley 41/2002, básica reguladora de la autonomía del paciente).

En este contexto, el artículo 13 del Reglamento de protección de datos establece una presunción general de madurez a los 14 años, recogiendo así el criterio mantenido por la AEPD[27]. Con ello, se pretende otorgar una mayor seguridad jurídica, evitando los problemas de tener que comprobar caso por caso las condiciones de madurez del menor, lo que resultaría muy complicado en entornos como Internet[28]. Ahora bien, ¿eso significa que por debajo de los 14 años prestan siempre el consentimiento los representantes legales del menor? A pesar de que la AEPD había acudido en estos casos al criterio de la madurez (siguiendo con ello las reglas generales arriba señaladas)[29], el artículo 13 del Reglamento es tajante cuando establece que en el caso de menores de 14 años "*se requerirá el consentimiento de los padres o tutores*". Por lo que se deja claro que la capacidad para consentir el tratamiento de los datos personales no se adquiere antes de los 14 años[30].

En sentido contrario, podemos también preguntarnos si a partir de los 14 años siempre prestan el consentimiento los propios menores. En este caso, el Reglamento no es tan tajante, ya que exceptúa de la regla general "*aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela*". De ello se deduce que habrá que atender al acto de que se trate para comprobar si el menor tiene o no capacidad para prestar el consentimiento por sí solo. Esto ocurrirá, por ejemplo, en el ámbito médico, en el que según hemos señalado el menor adquiere con carácter general la mayoría de edad sanitaria a los 16

---

[27] La AEPD ya analizó esta cuestión en su memoria anual del año 2000. En ella, la Agencia parte del criterio general sentado en el artículo 162 Código Civil (en el que se exceptúan de la representación legal de los padres los actos que el menor pueda realizar por sí mismo conforme a las leyes y sus condiciones de madurez), para analizar a partir de cuándo un menor tendría suficiente madurez para consentir el tratamiento de sus datos personales. Pues bien, a la vista de otras normas presentes en el ordenamiento jurídico español, que reconocen capacidad a los mayores de 14 años para determinados actos de la vida civil (ej. adquisición de la nacionalidad española por derecho de opción o residencia, capacidad para testar, etc.), la AEPD traslada este criterio al ámbito de la protección de datos. Puede consultarse este documento en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf

[28] En este sentido, PUENTE ESCOBAR, A., "Consentimiento del afectado y deber de información", en MARTÍNEZ MARTÍNEZ, R. (coord.), *Protección de datos. Comentarios al Reglamento de desarrollo de la LOPD*, Tirant lo Blanch, Valencia, 2009, p. 43.

[29] En la Memoria de la AEPD del año 2000 citada anteriormente, se señala que para los restantes menores, es decir, los que estén por debajo de 14 años, "no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162.1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez".

[30] Así lo dice expresamente la AEPD en su informe jurídico 308/2008, para el caso de SMS recibidos por una menor en su teléfono móvil. Los informes de la AEPD pueden consultarse en su web en la siguiente dirección: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/index-ides-idphp.php

años. Si se considera que el menor no es capaz para consentir un determinado acto médico (ej. una intervención quirúrgica), tampoco podrá consentir por sí solo el tratamiento de los datos médicos derivados de dicha actuación[31]. Igualmente, esto suele darse en el ámbito contractual en el que, con carácter general, el Código Civil excluye la capacidad para contratar de los menores de edad no emancipados (art. 1263.1º).

La AEPD ha resuelto algunos casos de tratamiento de datos de menores de edad sin el correspondiente consentimiento parental. Así, por ej., la Resolución de 11 de noviembre de 2008, en la que se sancionó a la empresa Telefónica Móviles España al quedar acreditada la adquisición de un pack telefónico y la emisión de una factura a una menor de 13 años sin que constara el consentimiento de sus representantes legales[32].

Una última cuestión que es importante destacar en relación con este tema es que el consentimiento del menor es válido únicamente para el tratamiento de los datos que le conciernen (art. 13.2 Reglamento). Aunque esto se deduce de los principios generales en materia de protección de datos, el Reglamento quiere dejar claro que no se puede utilizar al menor para obtener información de su núcleo familiar, salvo que se trate de los datos de identidad y dirección del representante legal y con la única finalidad de recabar su consentimiento para el tratamiento de los datos del menor.

4.1.2. LOS MECANISMOS DE PRUEBA DE LA EDAD Y CONSENTIMIENTO DE LOS REPRESENTANTES LEGALES

Una vez determinado que la capacidad para consentir el tratamiento de datos se adquiere, con carácter general, a los 14 años, la siguiente cuestión que se plantea es la relativa a la comprobación de la edad y, en su caso, la autenticidad de la autorización de los representantes legales. Se trata de una de las cuestiones clave para el funcionamiento del sistema y, desde luego, la que plantea mayores dificultades en el ámbito de Internet.

---

[31] Sobre el tema, *vid.* TRONCOSO REIGADA, A., "La protección de los datos sanitarios del menor", en LÁZARO GONZÁLEZ, I.E./MAYORAL NARROS, I.V. (coord.), *Nuevos retos que plantean los menores al Derecho. III Jornadas sobre Derecho de los menores*, Publicaciones de la Universidad Pontificia de Comillas, Madrid, 2004, p. 213 y ss., y en AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID, *Protección de datos personales para servicios sanitarios públicos*, Thomson-Civitas, Madrid, 2008, p. 102 y ss.

[32] Además, la empresa había incluido a la menor por el impago de la factura de unos 150 € en los conocidos como "ficheros de morosos". En total, se le impuso una sanción por infracción de los arts. 6 y 4.3 LOPD de 70.000 € (Procedimiento nº PS/00315/2008; Resolución R/01349/2008). Otras resoluciones sobre el tema son la 905 y 914 de 2008 (PS/00499/2007 y AP/00003/2008), en las que se sanciona la cesión de los datos de los alumnos por parte de una escuela primaria a una editorial para realizar una publicación, sin que se hubiera solicitado el consentimiento de algunos representantes legales. También la Resolución R/02285/2009 (PS/00010/2009), en la que se sanciona a una federación deportiva por publicar en su web los resultados de competiciones de menores sin consentimiento de los padres. Pueden consultarse los procedimientos sancionadores en la web de la AEPD en la siguiente dirección: https://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/index-ides-idphp.php

Siguiendo los criterios internacionales ya vistos en apartados anteriores, el artículo 13.4 del Reglamento atribuye al responsable del fichero o tratamiento la obligación de articular los procedimientos que garanticen que se ha comprobado de modo efectivo tanto la edad del sujeto, como la autenticidad del consentimiento prestado por los padres en el caso de que éste sea preciso.

El problema se encuentra en determinar qué debe entenderse por "modo efectivo". Desde luego no exige una comprobación absoluta, pero sí algún mecanismo dotado de cierta fiabilidad[33]. Así, por ejemplo, parece un método poco fiable de comprobación la mera pregunta de la edad en un formulario web en el caso además de que las contestaciones estén ya establecidas por defecto (ej., cuando sólo puede ponerse que se es mayor de 14 años para poder continuar), o cuando se incorporan cláusulas por las que el usuario declara ser mayor de edad (sin darle la opción de introducir su verdadera edad), o haber obtenido el consentimiento parental en el caso de ser menor de 14 años. En este sentido, pueden servir de guía los criterios establecidos en la COPPA estadounidense[34].

La AEPD ya ha tenido alguna ocasión de pronunciarse sobre el tema. En su Resolución de 14 de marzo de 2008[35] analizó el caso en el que un menor recibió en su domicilio una promoción comercial de un banco para la contratación de una tarjeta de crédito. La entidad bancaria había contratado con una empresa la realización de la campaña publicitaria. Los

---

[33] En este sentido, PUENTE ESCOBAR, A., *ob. cit.*, p. 44. Señala este autor que la comprobación normalmente se hará exigiendo determinados datos o mediante "preguntas de control" que en principio sólo puede contestar razonablemente un menor. ZABÍA DE LA MATA, J., "Artículo 13. Consentimiento para el tratamiento de datos de menores de edad", en AAVV, *Protección de datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008, p. 189 y ss., diferencia según el contexto en el que se soliciten los datos. En el ámbito de Internet, dada la complejidad para comprobar de manera efectiva la edad, bastaría con una declaración formal de que se es mayor de 14 años por parte de la persona que facilita los datos. En el caso de cupones-respuesta a promociones, podría distinguirse entre aquellos casos en que se solicite datos identificativos para fines sin especial transcendencia, bastando entonces con la firma del representante legal en el cupón si se trata de un menor de 14 años, de aquéllos otros en que se trate datos de mayor trascendencia o se formalice una relación contractual, en cuyo caso sería necesario un documento acreditativo de la edad del menor o el documento de identificación del representante legal para comprobar la firma. Cuando se recaben datos de forma presencial, podría entregarse al menor un documento de autorización para que se firme por el representante legal, acompañado de un documento acreditativo de su identidad, para verificar la firma.

En cualquier caso, existen ya, aunque no estén muy extendidas, herramientas tecnológicas de verificación online de identidad o edad, ofrecidas por diversas empresas (ej. Integrity o Idology), incluso utilizando elementos biométricos, como la densidad de los huesos de la mano (ej. Verificage), al margen de los documentos de identificación electrónica. Un sistema utilizado, por ej., por las redes sociales, es el del análisis semántico de las palabras utilizadas en los perfiles, para detectar usuarios menores de edad.

[34] Tuenti, una de las redes sociales más populares entre los jóvenes españoles, no permite en el registro seleccionar fechas de nacimiento de las que se derive una edad inferior a los 14 años. Facebook solicita la fecha de nacimiento, impidiendo el registro si se es menor de la edad mínima señalada en las condiciones de uso. Utiliza además cookies para impedir un nuevo registro cambiando simplemente la fecha, si bien una vez eliminada la cookie es posible el registro (*vid.* LOBE, B. & STAKSRUD, E. (ed.), *Evaluation of the implementation of the Safer Social Networking Principles for the UE. Part II: Testing of 20 Social Networking Services in Europe*, European Commission Safer Internet Programme, Luxembourg, 2010, p. 20 y ss., 102).

[35] Procedimiento nº PS/00281/2007, Resolución R/00284/2008.

ficheros de datos que dicha empresa manejaba se nutrían, entre otros, de los datos facilitados por los usuarios de un determinado sitio web. En el formulario de inscripción del sitio web se solicitaban una serie de datos personales (entre ellos, la fecha de nacimiento), debiéndose marcar las áreas de interés del usuario (automóviles, juegos, informática, etc.) para recibir promociones comerciales. Una vez registrado, el usuario podía acceder a diversos servicios, entre ellos, trucos en el uso de videojuegos. Además, en los términos y condiciones de uso del servicio se señalaba expresamente que su uso no estaba permitido a los menores de edad.

Pues bien, a pesar de que se solicitara la fecha de nacimiento y el programa impidiera continuar en el caso de tratarse de un menor, el interesado consiguió registrarse en la web, ya que, al parecer, al no completar correctamente los campos solicitados, el sistema lo identificó como mayor de edad[36]. La AEPD rechazó los argumentos presentados por las empresas acerca de la capacidad del menor para consentir el tratamiento de datos (es decir, que el menor tenía la madurez suficiente ya que había sido capaz de acceder a Internet, buscar páginas con trucos para videojuegos, facilitar sus datos, saber que debía aceptar las condiciones de uso para poder registrarse, etc.[37]), o la culpa *in vigilando* de los padres (al encontrarse el menor conectado un día laborable por la noche). En este caso, ante el evidente error del sistema de verificación de edad, la AEPD sancionó a las empresas, por lo que no tenemos un pronunciamiento explícito acerca de si el sistema de solicitar la fecha de nacimiento constituye un "modo efectivo" de comprobación de la edad, a los efectos del artículo 13 del Reglamento. No obstante, a la vista de las declaraciones de la AEPD en la propia Resolución, puede deducirse que la solicitud de la fecha de nacimiento, junto con otras garantías adicionales, puede considerarse un mecanismo adecuado de comprobación[38].

En la Resolución de 26 de abril de 2010[39], en la que ya era plenamente aplicable el artículo 13 del Reglamento[40], la AEPD sanciona a un portal web dirigido a un público infantil y

---

[36] Aunque la fecha de nacimiento del menor no quedó registrada junto con el resto de sus datos en el fichero de la empresa, ésta alegaba que el usuario introdujo como fecha de nacimiento "95", en lugar de 1995, y dado que el sistema está diseñado para insertar dicho dato con cuatro dígitos, le atribuyó una edad de 1911 años.

[37] Según señala la Resolución, el menor tenía 9 años cuando recibió la publicidad en su casa.

[38] En concreto, la Agencia señala que la empresa advertía con carácter previo a la recogida de datos "que los menores de edad estaban excluidos y se establecía un mecanismo para verificar la edad, al exigir el dato correspondiente a la fecha de nacimiento de los usuarios en el formulario que debía cumplimentarse". Además, la empresa cambió posteriormente el sistema de introducción de fechas, para que sólo se pudieran marcar las predeterminadas en dicho campo, y la casilla de aceptación de los términos y condiciones, estableciéndose "Acepto los términos y condiciones y garantizo que soy mayor de edad". La AEPD señala en la Resolución que estos cambios acreditan que "la implantación de medidas dirigidas a evitar el tratamiento de sus datos como usuarios del servicio, siendo factibles, no fueron implantadas".

[39] Procedimiento nº PS/00468/2009, Resolución R/00893/2010.

juvenil (que ofrece servicios de chat, juegos para interactuar con otros usuarios, etc.), por recabar datos de menores de 14 años sin consentimiento de sus representantes legales. En este caso, la web solicitaba para registrarse únicamente una dirección de correo electrónico, un nombre de usuario y una contraseña, siendo la fecha de nacimiento opcional. En la política de protección de datos se establecía que, en el caso de ser el titular menor de 14 años, manifestaba que contaba con el previo consentimiento de sus representantes legales y que había cumplimentado el formulario bajo su supervisión. La Agencia consideró insuficiente esta cláusula para garantizar la autenticidad del consentimiento parental en los términos del artículo 13.4 del Reglamento[41].

Por último, es importante señalar que el Tribunal Supremo español ha ratificado la legalidad del artículo 13.4 del Reglamento en dos Sentencias de fecha 15 de julio de 2010[42]. En ambos casos, las partes habían alegado que este precepto impone una obligación nueva al margen de la LOPD y de la Directiva europea de protección de datos, y que además se trataba de una obligación de difícil o imposible cumplimiento y desproporcionada. En las Sentencias se afirma que las normas de la LOPD y de la Directiva comunitaria sobre el consentimiento no contienen una regulación específica del consentimiento de los menores de edad, habilitándose así para su desarrollo a través de un Reglamento, que en nada infringe las previsiones de dichas normas. Para el Tribunal, el artículo 13.4 del Reglamento no es más que un complemento del apartado primero de ese precepto, en el que se regula la capacidad de los menores para consentir el tratamiento de sus datos personales. Añade, además, que aunque la comprobación de la edad puede presentarse en ocasiones como difícil, ello no puede servir de excusa para que no se

---

[40] A diferencia del supuesto anterior, cuyos hechos se produjeron antes de la entrada en vigor del Reglamento; lo que no impidió a la Agencia, como hemos visto, hacer un primer pronunciamiento sobre el tema, basándose en la doctrina sentada en sus informes y resoluciones anteriores, que luego se plasmaría en el artículo 13 del Reglamento.

[41] No se entró en la cuestión de si era o no suficiente el sistema de comprobación de la edad, pues en el caso les constaba la fecha de nacimiento de la menor y que contaba con menos de 14 años cuando se registró. En realidad, gran parte de la resolución se dedica a dilucidar el carácter de dato personal de la dirección de correo electrónico, que la entidad demandada discute. Por otra parte, en esta Resolución se hace referencia al informe de la Agencia de 29 de junio de 2009, en el que se afirma que solicitar únicamente el documento nacional de identidad a los menores y, en su caso, a los representantes legales, no es un medio de acreditación suficiente de que el consentimiento se haya prestado por éstos, aconsejando que se acompañe además un documento en el que el representante exprese dicho consentimiento, de manera que se pueda comprobar que la firma del representante en el documento de autorización coincide con la de su documento de identidad. Igual solución aporta la AEPD en el informe 0046/2010, sobre tratamiento de datos de menores de edad a los que se facilita una tarjeta de fidelización en un comercio. Señala la Agencia que tanto si la solicitud de la tarjeta se realiza por los padres, como si éstos autorizan la solicitud realizada por el menor, es necesario que se acompañe a dicha solicitud o cupón el documento nacional de identidad de los padres, a fin de comprobar la veracidad de la firma. *Vid.*, también, la Resolución R/01974/2009 (PS/00293/2009).

[42] Dictadas por la Sala de lo Contencioso-administrativo de dicho Tribunal (sección sexta), que es quien tiene competencia para declarar la adecuación de las disposiciones con rango reglamentario a lo dispuesto en las normas de rango superior. Estas sentencias vienen a resolver sendos recursos (23 y 25/2008) interpuestos por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y por la Federación de Comercio Electrónico y Marketing Directo (FECEMD), por los que se pretendía que se declarara la nulidad de diversos preceptos del Reglamento de desarrollo de la LOPD, por infringir esta Ley y la Directiva comunitaria de protección de datos.

adopten las medidas de garantía adecuadas, sin que pueda considerarse esta exigencia desproporcionada, al incidir en un ámbito especialmente sensible como es el de los menores.

4.2. El deber de información

El artículo 5 LOPD establece, como unos de los pilares básicos en materia de protección de datos, la obligación de informar al interesado sobre ciertos extremos del tratamiento recogidos en ese precepto (así, de la existencia de un fichero de datos, la finalidad de la recogida de éstos y de los destinatarios de la información, de la identidad y dirección del responsable, etc.). Se trata de una obligación tan básica que existe incluso cuando no es necesario el consentimiento del titular para el tratamiento de sus datos. En aquellos casos (la mayoría) en que el consentimiento sí es necesario, la información es un requisito básico para la validez del mismo, que se caracteriza, entre otros requisitos, por tratarse de un "consentimiento informado".

Pues bien, el deber de informar adquiere caracteres especiales en el caso de los menores. En efecto, al tratarse de personas en desarrollo, la información que se dirija a ellos debe estar adaptada a sus capacidades de entendimiento. Sólo así se puede garantizar el cumplimiento de este deber, y que el menor presta el consentimiento habiendo comprendido la información relativa al tratamiento de sus datos, es decir, siendo consciente de para qué lo presta. Dispone, así, el 13.3 del Reglamento que "*cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo*". Como vemos, el precepto indica cómo debe redactarse la cláusula informativa y también cuál debe ser su contenido.

En cuanto a la redacción, el precepto hace hincapié en el lenguaje utilizado, esto es, deben usarse palabras que permitan su comprensión por el menor, evitando un lenguaje excesivamente formal o tecnicismos que a veces sólo son comprensibles por expertos. Pero, además, la referencia al lenguaje debería incluir también el tamaño de la letra, que permita que el texto sea legible[43], e incluso la denominación del enlace a este texto, que permita comprender a primera vista cuál es su contenido[44]. El precepto no dice nada sobre cómo y cuándo dar esta información, por lo que habrá que aplicar los criterios generales (con carácter previo al

[43] De modo similar a lo previsto para las condiciones generales en contratos con consumidores (art. 80 de la Ley General para la Defensa de los Consumidores y Usuarios -Real Decreto Legislativo 1/2007, de 16 de noviembre-; arts. 5 y 7 Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación).

[44] Puede dar lugar a dudas incluir la información sobre privacidad en un enlace denominado "advertencia legal" o en el de "ayuda".

tratamiento de los datos, en lugar visible y fácilmente accesible, debe asegurarse que el interesado ha tenido la oportunidad de leerlo, etc.[45]).

Respecto al contenido de la cláusula informativa, deberá incorporar no sólo la información del artículo 5 LOPD, sino también lo establecido en el artículo 13 del Reglamento. Así, la edad a partir de la cual puede prestar consentimiento el menor por sí sólo, la prohibición de recabar datos de otros miembros de la familia, la obligación de contar con el consentimiento de los padres o tutores en el caso de ser menor de 14 años, pero también el mecanismo a través del cual los representantes legales podrán prestar dicho consentimiento de forma efectiva.

Por último, es importante tener en cuenta que el incumplimiento del deber de información en los términos establecidos en los artículos 5 LOPD y 13.3 Reglamento, supone una infracción de la normativa de protección de datos (art. 44 LOPD), lo que puede conllevar importantes sanciones[46].

4.3. El Código Tipo "Confianza Online"

Al tratamiento de datos de los menores de edad con fines de publicidad o prospección comercial le son aplicables las reglas generales establecidas en la LOPD y, en particular, el artículo 13 del Reglamento. Pero en este ámbito hay que hacer referencia, además, al Código Tipo "Confianza Online", sobre comercio electrónico y publicidad interactiva, promovido por las principales asociaciones españolas en estos sectores[47]. Aunque se trata de un texto de carácter autorregulatorio y, por tanto, cuya aplicación depende de la propia industria, es importante tenerlo en cuenta como complemento a la legislación sobre protección de datos, sobre todo, a la vista del sector al que afecta y de que dedica un capítulo específico a los menores.

---

[45] Pueden consultarse, por ejemplo, las recomendaciones para el sector del comercio electrónico realizadas por la AEPD en el año 2000 (https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_comercio_electronico.pdf).

[46] *Vid.* Informe jurídico de la AEPD 0308/2008. En la Resolución de la AEPD nº R/01974/2009 (PS/00293/2009), se sancionó a la empresa Panini por recabar datos personales de menores para participar en un sorteo a través de cupones en la revista High School Musical. En el caso, la empresa había publicado en uno de los números de la revista el cupón de participación en el sorteo sin cláusula informativa, y en los siguientes números, con una cláusula que no cumplía los requisitos del art. 5 LOPD (y mucho menos los del art. 13 del Reglamento). La AEPD considera que la empresa ha incurrido en la infracción leve prevista en el art. 44.2.d) LOPD (incumplimiento del art. 5 LOPD), teniéndose en cuenta el hecho de que los datos en su mayoría sean de menores de edad para graduar la infracción (esto es, para elevar la sanción que se impone, que asciende a 6000 euros).

[47] Principalmente, por la Asociación Española de Comercio Electrónico y Marketing Relacional (AECEM) y la Asociación para la Autorreglación de la Comunicación Comercial (AUTOCONTROL), en colaboración con IAB Spain (*Interactive Advertising Bureau Spain*) y junto a muchas otras Asociaciones participantes. Puede consultarse el texto del Código en la web de la AEPD, en la sección dedicada a los Códigos Tipo (https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php#rgpd).

El artículo 32 LOPD prevé la posibilidad de que empresas o agrupaciones de éstas puedan formular Códigos de buenas prácticas (llamados por la Ley "Códigos Tipo"), con la finalidad de adecuar y conseguir una mejor aplicación de lo previsto en la legislación sobre protección de datos a las especificidades de los tratamientos del sector empresarial de que se trate[48].

En este marco, surge en el año 2002 el Código de Confianza Online, cuya última actualización es de 2009. Su título V se destina específicamente la protección de los menores. En concreto, en el artículo 36, dedicado al tratamiento de datos de menores, se recogen las previsiones del artículo 13 del Reglamento. Se establece, así, la necesidad de consentimiento de los representantes legales para el tratamiento y cesión de datos de menores de 14 años[49], la prohibición de recabar datos del grupo familiar, la información adaptada a las capacidades de comprensión de los menores y la obligación de establecer mecanismos que aseguren de forma razonable, de acuerdo con el desarrollo de la tecnología, la edad del menor y el consentimiento de los representantes legales.

Con el fin de limitar la publicidad que reciben los menores, el Código reconoce a los padres el derecho a oponerse al envío de publicidad o información solicitada por los menores a su cargo[50]. Y, además, se establece otra medida importante, como es el que las entidades adheridas al Código limiten la utilización de los datos de los menores con "la única finalidad de promoción, venta y suministro" de productos o servicios aptos para dichos menores. Se reconoce así la necesidad de reducir el exceso de publicidad que los menores reciben en nuestros días, pues no hay que olvidar que se trata de personas que no tienen todavía plena capacidad de discernimiento. Junto a ello, y aunque no se refiera específicamente al tratamiento de datos, el Código contiene otras normas sobre protección de menores y publicidad, que intentan evitar que ésta se aproveche de la inexperiencia del menor o protegerle frente a contenidos perjudiciales (arts. 34, 35)[51].

---

[48] Esta previsión se desarrolla en el Título VII del Reglamento (arts. 71 y ss.).

[49] Que el Código denomina como "niños", para diferenciarlos de los mayores de 14 años, a los que considera "adolescentes" (art. 1).

[50] Derecho de oposición que consideramos discutible en el caso de menores perfectamente capaces para consentir por sí mismos el tratamiento de sus datos, sobre todo, en el caso de adolescentes cerca de la mayoría de edad.

[51] Así, deben identificarse los contenidos dirigidos únicamente a adultos, no se deberá incitar a los menores a la compra de un producto o servicio explotando su inexperiencia o credulidad, o a que persuadan a sus padres o tutores o a los de terceros a dicha compra. Parecidos requisitos sobre el contenido de la publicidad se pueden encontrar para otros sectores en el art. 7 de la Ley 7/2010, de 31 de marzo, General de Comunicación Audiovisual. Vid., asimismo, la Recomendación del Parlamento Europeo y del Consejo 2006/952/CE, relativa a la protección de los menores y de la dignidad humana y al derecho de réplica en relación con la competitividad de la industria europea de servicios

El Código supone un intento loable por regular la protección de los datos de los menores en un tema tan sensible con el de la publicidad online o el comercio electrónico, e incluso incorpora alguna medida adicional (por ej., en cuanto a la publicidad dirigida a menores, el ejercicio de los derechos en materia de protección datos por los representantes legales o en el establecimiento de medidas informativas y educativas dirigidas a los padres para ayudarles en la protección de la intimidad de sus hijos). Sin embargo, peca de cierta imprecisión, sobre todo al recoger las obligaciones establecidas en el artículo 13 del Reglamento, que apenas desarrolla, concediendo así un gran margen de actuación a las empresas que deben aplicarlo. Hubiera sido deseable, por ejemplo, una mayor concreción sobre el deber de información dirigido a menores, mecanismos para recabar el consentimiento de los representantes legales, etc.

5. CONCLUSIONES

Como se puede comprobar de los documentos analizados en este artículo, existen una serie de criterios básicos para el tratamiento de los datos personales de los menores de edad comúnmente aceptados, y que se han recogido en la regulación española contenida en el artículo 13 del Reglamento de protección de datos. Las divergencias se pueden encontrar en la edad a la que se considera a un menor maduro en relación con el derecho a la protección de datos personales (normalmente entre los 13 y los 16 años), pero los principios para el tratamiento de su información personal son semejantes. Así, la obligación de informar y obtener el previo consentimiento de los representantes legales en el caso de menores no maduros, y reconocerles el ejercicio de los derechos de acceso, rectificación, cancelación u oposición al tratamiento de datos de sus hijos, la prohibición de obtener datos del grupo familiar u otros terceros a través del menor, o la necesidad de adaptar la información sobre el tratamiento de los datos personales a las capacidades de comprensión del menor.

De entre ellas, la que plantea mayores problemas es la obligación para el responsable del tratamiento de los datos de verificar la edad del usuario y la autenticidad del consentimiento prestado por los representantes legales, en particular, en el caso de los datos recabados *online*. Esta obligación deberá adaptarse a las particularidades del medio a través del cual se recaban los datos y a los instrumentos tecnológicos existentes en cada momento, sin que el hecho de la dificultad de su aplicación constituya en una excusa para eliminar o rebajar su exigibilidad. Más bien, hay que aceptar que cierto número de fallos en el sistema son inevitables, al menos hasta que no se incorporen al entorno *online* medios de comprobación más seguros.

---

audiovisuales y de información en línea, y la Directiva europea 2010/13/UE del Parlamento y del Consejo, de 10 de marzo de 2010, de servicios de comunicación audiovisual.

En cualquier caso, estos criterios constituyen un importante comienzo para la protección de los datos personales y la intimidad de los menores de edad. Con ellos se quiere conseguir un mayor control de la información que se refiere a los menores, por ellos mismos si tienen suficiente capacidad, o por sus representantes legales. Medidas que desde luego habrá que ir completando con otras adicionales que los protejan frente a una comercialización directa agresiva, bien en el ámbito de la protección de datos (limitando claramente el uso de los datos de los menores con estos fines), bien a través de otras normas para la protección de los consumidores (evitando, por ej., que la información o publicidad dirigida a los menores explote su falta de experiencia o credulidad).