DERECHOS DIGITALES DE LOS MENORES Y DATOS MASIVOS. *REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS* DE 2016 Y LA *COPPA* DE ESTADOS UNIDOS

Children's digital rights and big data. The *European general data protection regulation* (*GDPR*), 2016, and the *Children's online personal data protection act* (*Coppa*)

Ana Azurmendi

Ana Azurmendi es profesora titular de Derecho de la Comunicación en la *Universidad de Navarra* (*UNAV*) desde 1991. Directora del *Center for Internet Studies and Digital Life* de la *UNAV*. Investigadora principal del proyecto de investigación *Televisiones autonómicas*. Autora de varios libros como *Derecho de la comunicación. Guía jurídica para profesionales de los medios* (2016); *La reforma de la televisión pública española* (2007); *El derecho a la propia imagen* (1997) y de varios artículos. Sus principales intereses de investigación son la televisión pública y los derechos digitales de los ciudadanos en internet.
http://www.unav.edu/en/web/facultad-de-comunicacion/ana-azurmendi
http://orcid.org/0000-0001-6679-8826

Universidad de Navarra, Departamento de Comunicación Pública
Edificio de Bibliotecas, Campus Universitario. 31080 Pamplona (Navarra), España
aazur@unav.es

Resumen

El impacto de las tecnologías de datos masivos en la protección de los datos personales de los menores de edad es importante. En primer lugar, por la mayor vulnerabilidad de los menores, tanto por su desconocimiento de los riesgos que comporta una gestión inadecuada de sus datos, como porque resulta fácil obtener de ellos todo tipo de datos. En segundo lugar, porque la capacidad de predicción sobre un menor o grupo de menores del que se tenga una larga trazabilidad será enorme, y en consecuencia las posibilidades de discriminación futura para su participación política y social, su contratación, empleo y obtención-disfrute de servicios serán mucho mayores. Ante la entrada en vigor, en mayo de 2018, del *Reglamento General de Protección de Datos Personales* (UE 2016/679) de la Unión Europea este artículo presenta los aspectos relevantes de la protección de los menores en esta norma. Con el fin de valorarlos se contrastan con las propuestas del Grupo de Trabajo, artículo 29 y con la ley estadounidense *Children's online personal data protection act* (*Coppa*).

Palabras clave

Datos masivos; Macrodatos; Derechos digitales; Menores; Protección de datos; *Reglamento general de protección de datos personales*; *Coppa*.

Abstract

The impact of big data technologies on children's data protection is very important. First of all because of children's vulnerability, due their lack of knowledge about the risks of an inadequate data management and, secondly, because the immense possibilities of traceability of a child or a group of children. Consequently, the negative effects in terms of future discrimination for their social and political participation, employability, usability of services, etc., could be immense. Europe has a new *Law on protection of personal data* (UE 2016/679). This paper examines in which way the *Law* pays attention to this particular area of protection of children. In order to value the proposals of the European *Law*, this paper studies comparatively some of the reports of the *Working Group*, art. 29, and the US law *Children's online personal data protection act* (*Coppa*).

Keywords

Big data; Digital rights; Children; Data protection; *The European law of personal data protection* (*GDPR*); *Coppa*.

Azurmendi, Ana (2018). "Derechos digitales de los menores y datos masivos. *Reglamento europeo de protección de datos* de 2016 y la *Coppa* de Estados Unidos". *El profesional de la información*, v. 27, n. 1, pp. 27-35.

https://doi.org/10.3145/epi.2018.ene.03

Artículo recibido el 02-08-2017
Aceptación definitiva: 05-10-2017

1. Introducción

La aprobación del nuevo *Reglamento general de protección de datos* (UE2016/679) de 27 de abril de 2016 (*Unión Europea*, 2016) ha supuesto un avance en la protección de datos de los usuarios en un entorno digital, global y de notoria preponderancia del fenómeno *big data* (datos masivos) Las expectativas de que esta iniciativa europea mejorará la privacidad de los ciudadanos, se refieren también a los menores de edad.

Como ponen de manifiesto el informe *Net children go mobile* (**Garmendia-Larrañaga** *et al.*, 2016) y el informe *PISA* (*OCDE*, 2017), en España cada vez es más temprana la iniciación en internet.

Por otra parte, es creciente entre los menores el acceso privado a internet en la medida en que se ha generalizado el uso de smartphones (un 63% de menores entre los 9 y los 16 años lo tienen). El tiempo que dedican a navegar es de una media de 167 minutos diarios entre semana y 215 minutos en fin de semana. Las actividades online más frecuentes entre los menores son:

- visionado de videoclips (85%);
- realización de tareas escolares (84%);
- mensajería instantánea (68%);
- juegos con otras personas (48%);
- descargas de música o películas (42%).

Son usos que conllevan un tráfico de datos personales de los que no siempre son conscientes los menores.

La metodología de este artículo de carácter ensayístico-propositivo es la revisión documental de tipo comparativo de tres tipos de fuentes:

- normativas: *Reglamento general de protección de datos* de la UE y la Ley estadounidense *Children's online personal data protection act* (*Coppa*);
- propositivas: comunicaciones de la *Comisión Europea* sobre estrategias de protección de derechos frente a los datos masivos;
- académicas: aportarán elementos de discusión acerca de los fundamentos éticos de la protección de datos de menores y su traslado normativo.

2. Datos masivos, su impacto en la protección de datos y soluciones del *Supervisor Europeo de Protección de Datos*

El concepto de datos masivos del que se parte es el adoptado por el *European Data Protection Supervisor* (autoridad europea para la protección de datos):

> "el procesamiento de enormes volúmenes de información de diversa fuente mediante el uso de algoritmos de autoaprendizaje, válidos para informar decisiones (…). Una de las mayores virtudes de los datos masivos, tanto para las empresas como para los gobiernos, es la posibilidad que ofrece (simultáneamente) para el seguimiento de la conducta humana, colectiva e individual y para su predicción". (*European Data Protection Supervisor*, 2015a).

Una definición compartida por la gran mayoría de especialistas del área computacional, de derecho y de comunicación (**Mayer-Schonberger**; **Cukier**, 2013; **Baesens** *et al.*, 2016; **Peterson**; **Breul**, 2017; **Chen** *et al.*, 2014; **Menon**; **Sarkar**, 2016; **Tomar** *et al.*, 2017); o en el área de privacidad y datos masivos (**Lin** *et al.*, 2016; **Rajkumar**; **Calheiros**; **Vahid-Dastjerdi**, 2016; **Menon**; **Sarkar**, 2016; **Payton**; **Schmidt**; **Claypoole**, 2014; **Mantelero**; **Vaciago**, 2015).

Si realmente la gran aportación de los datos masivos, tal y como todos confirman, está en la posibilidad de gestionar una ingente cantidad de datos de comportamiento humano y no humano, con la finalidad de obtener predicciones con un alto nivel de fiabilidad, una de las primeras cuestiones que se plantean en el uso de datos masivos para predicción de comportamientos humanos es si puede garantizarse el anonimato de las identidades personales origen de los datos.

El *European Data Protection Supervisor* en su opinión *Towards a new digital ethics. Data, dignity and technology* afirma que la tecnología actual permite la re-identificación de datos anonimizados (*European Data Protection Supervisor*, 2015a, p. 13).

Por otro lado, desde hace años se ha argumentado sobre la incompatibilidad entre datos masivos y privacidad (**Tuker**, 2013; **Zook** *et al.*, 2017), puesto que:

> "la riqueza de los datos hace 'algoritmicamente' posible localizar a las personas" de ahí que "cuantos más datos se tengan menos puede hablarse de privacidad" (**Zook** *et al.*, 2017).

Teniendo en cuenta esta posibilidad de que tanto a los grupos como a los individuos se asocien conductas y predicción de conductas con nulo margen de error, se comprende el interés de empresas, operadoras de telecomunicaciones, partidos políticos, entidades financieras, seguros, etc., por las técnicas de procesamiento masivo de datos para el desarrollo de sus estrategias.

> "La capacidad de predicción sobre un menor o grupo de menores del que se tenga una larga trazabilidad será enorme"

A corto plazo es muy probable que limiten su oferta de servicios a aquellos potenciales seguidores/usuarios/clientes targetizados como óptimos, en función de las características del negocio o tipo de servicio de que se trate. Por otra parte, excluirán a los seguidores/usuarios/clientes potenciales que no cumplan con esa condición.

En el medio-largo plazo primará la planificación de estrategias para conseguir la adhesión de los categorizados como clientes óptimos, a partir precisamente del conocimiento que se tiene de sus patrones conductuales.

El riesgo no proviene de la técnica de datos masivos sino principalmente de la combinación de los resultados de su aplicación para predicción de conductas con perfiles personales identificables en poder de empresas, operadores de telecomunicaciones, partidos políticos, entidades bancarias, seguros, etc.

Es evidente que la inclusión de los aportes de los datos masivos en la lógica política y económica implica, entre otros,

los riesgos de:

- aumentar la brecha social entre los ciudadanos: los más favorecidos económicamente, o desde el punto de vista de la salud, educacional, de capacidad de trabajo, de su estabilidad psicológica, etc., tendrían muchas más posibilidades de acceder a servicios, productos y opciones de mejora social;
- crear ámbitos culturales, políticos, económicos aislados dentro de la misma sociedad, actuando como un factor de disgregación social; en la medida en que existe la posibilidad de personalizar, por ejemplo, la información de actualidad o las relaciones y contenidos en redes sociales a las que cada individuo tiene acceso; también en la medida en que las estrategias de partidos políticos, grupos representativos, empresas, para conseguir la adhesión de los ciudadanos interesantes desde su *target*, están planteadas de acuerdo con los gustos, reacciones, motivos de determinados grupos ciudadanos;
- limitar de forma desproporcionada la libertad individual, en la medida en que el conocimiento predictivo de las conductas junto con las estrategias de difusión de mensajes (dirigidas a conseguir el mayor número de adhesiones de ciudadanos) tienen como consecuencia una reducción del marco de visión, acción y elección individual.

Los informes del *European Data Protection Supervisor* en dos documentos:

- *Opinion 9/2016 on Personal information management systems. Towards more user empowerment in managing and processing personal data* (*European Data Protection Supervisor*, 2016), y
- *Opinion 7/2015 Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability* (*European Data Protection Supervisor*, 2015b),

muestran la dificultad, y a la vez la necesidad, del equilibrio entre los criterios de competitividad y crecimiento económico de políticas económicas y empresas por un lado y los derechos personales de los ciudadanos por otro.

Siguiendo estos documentos parece evidente que si se quieren evitar las consecuencias indeseadas de los datos masivos sobre la libertad y la privacidad de los ciudadanos debería afrontarse una regulación basada en 4 puntos (*European Data Protection Supervisor*, 2015b):

- dar al ciudadano el control sobre sus datos: de manera que le resulte fácil ejercer los derechos de información, acceso, rectificación, supresión y oposición en referencia a sus datos personales;
- incluir en el diseño de los programas de procesamiento masivo de datos los principios ético-jurídicos relativos a la privacidad, en particular los principios de minimización, limitación, consentimiento y proporcionalidad (es lo que se llama la protección por diseño);
- promover entre las empresas una responsabilidad proactiva, aumentando las obligaciones de quienes trabajan con datos personales;
- protección legal.

3. Menores de edad y datos masivos. Propuestas del *Grupo de Trabajo, artículo 29*

Es aquí donde se plantean las preguntas sobre el impacto de los datos masivos en la protección de los datos personales de los menores de edad. En primer lugar por la mayor vulnerabilidad de los menores, tanto por su desconocimiento de los riesgos que comporta una gestión inadecuada de sus datos, como porque resulta fácil obtener de ellos todo tipo de datos. En segundo lugar porque la capacidad de predicción sobre un menor o grupo de menores del que se tenga una larga trazabilidad será enorme, y en consecuencia las posibilidades de discriminación futura para su participación política y social, su contratación, empleo y obtención-disfrute de servicios serán mucho mayores.

El *Grupo de Trabajo art. 29* de la *Unión Europea* es un consejo asesor independiente especializado en la protección de datos personales y privacidad, auspiciado por la *Comisión Europea* a partir de la *Directiva europea de protección de datos personales de 1995*[1] (95/46/EC), en particular sus artículos 29 y 30. En la actualidad ha sido relevado por el *Supervisor Europeo de Protección de Datos Personales*. Publicó en 2009 una guía para la protección de datos de los niños, *Opinion 2/2009, on The protection of children's personal data* (*Working Group*, 2009) articulada sobre los principios y derechos de protección de datos. Aunque el documento se refiere a los principios y derechos reconocidos en la *Directiva de protección de datos* de 1995, continúa siendo válido como propuesta (**Jaroszek**, 2015, p. 57).

Para evaluar en qué medida el nuevo *Reglamento general de protección de datos* atiende las propuestas sobre protección del menor del *Grupo de Trabajo, artículo 29*, se examinan las relativas a principios de protección de datos y derechos del menor sobre sus datos en contraste con el texto del *Reglamento*.

3.1. Principios del tratamiento de datos de los niños

Principio de calidad de datos (en el *Reglamento* de 2016: exactitud, temporalidad, minimización)

El *Grupo de Trabajo art. 29* en su *Opinión 2/2009 on The protection of children's personal data* plantea que se tenga en cuenta la falta de madurez del niño, de manera que tanto al recoger como al tratar los datos personales del menor se respete el interés superior del menor. La exigencia del principio de calidad de datos significa que los datos del menor se utilizan sólo para los fines para los que se recogieron, debiendo actualizarlos con una rapidez adecuada al proceso de desarrollo del menor o bien eliminarlos (*Working Group*, 2009) (art. 6 c y d, *Directiva 95/46/EC*, no tiene reflejo en el *Reglamento de 2016*).

En atención también al principio de calidad, el *Grupo de Trabajo art. 29* aconseja aplicar un derecho al olvido que preste especial atención a los niños. Entre otras razones señala que los niños crecen y maduran y en consecuencia, los datos relacionados con ellos pierden exactitud rápidamente, convirtiéndose en datos inadecuados para el fin original para los que se recabaron. El *Reglamento de 2016* no contempla un derecho al olvido específico para los niños a pesar de que sí se había incluido en su borrador[2]. Tiene en cuenta como una condición específica, dentro de la regulación general para el derecho al olvido (derecho de supresión) del artículo 17, que se trate de datos recabados de los menores "en relación con la oferta de la sociedad de la información".

Principio de consentimiento (art. 7 *Directiva 95/46/EC*, art. 8*; Reglamento 2016*, Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información)

Para el *Grupo de Trabajo art. 29*, el consentimiento de los menores debería ser un consentimiento informado y libre. Son características que se exigían en el borrador del *Reglamento*[3] y que posteriormente se eliminaron en el texto definitivo para quedarse en una leve referencia del derecho de transparencia referida al menor. Según el documento *The protection of children's personal data*, el menor está desprotegido ante el riesgo de que el adulto que le tutela, precisamente prevaliéndose de su ascendencia, vulnere la privacidad del menor, vendiendo o difundiendo sus datos. Sería una posibilidad que podría abordarse desde las responsabilidades de la tutela legal del menor, en el sentido de que se previeran sanciones por este tipo de conducta abusiva. En el caso de que el menor fuera consciente de la situación de abuso, el *Grupo de Trabajo art. 29* recomienda que se contemple en la ley el derecho del menor a ser oído por las autoridades competentes, incluidas las autoridades de protección de datos. Una posibilidad omitida por el *Reglamento de 2016*.

Otra de las situaciones que analiza el *Grupo de Trabajo art. 29* es que al menor se le reconozca la capacidad para contratos laborales (por ejemplo, en España el *Real decreto 1435/1985* de contratación de menores en espectáculos públicos, exige el consentimiento del menor si tiene 16 años y el de sus representantes legales si su edad es inferior) y que consecuentemente se puedan procesar sus datos en relación con esa actividad laboral. En todas las situaciones estudiadas el *Grupo de Trabajo art. 29* recomienda que se aplique como criterio prevalente el del interés superior del menor (criterio que no se menciona ni en el borrador del *Reglamento* ni en el texto definitivo).

> "Una de las primeras cuestiones que se plantean en el uso de los datos masivos es si puede garantizarse el anonimato de las identidades personales origen de los datos"

Principio de seguridad (art. 17 de la *Directiva 95/46/EC* y art. 5.1 f)*; Reglamento 2016*, Integridad y confidencialidad de los datos)

El principio de seguridad de los datos del art. 17 de la *Directiva 95/46/EC* se reconoce en el reglamento en el art. 5.1 f) mediante las exigencias de integridad y confidencialidad de los datos. Los menores de edad no son conscientes de los riesgos de permitir el procesamiento de sus datos, tampoco en el supuesto de los datos sensibles. Estos son categorías especiales de datos según la *Directiva de 1995*, art. 8, que se amplían en el art. 9 del *Reglamento* al comprender entre ellos los datos que revelen

> "origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, a la vida sexual o a la orientación sexual de una persona".

Una circunstancia que según el *Grupo de Trabajo art. 29*, puede ser aprovechada por empresas y departamentos online para obtener y tratar todo tipo de datos de los menores si no se contempla alguna medida *ad hoc*, como por ejemplo una obligación de dar información adaptada al menor, u otras de carácter técnico como hacer imposible la opción de rellenar casillas con datos si no se ha podido verificar el consentimiento de los padres o representantes legales del menor (no hay referencia a esto en el *Reglamento* salvo el mandato general del lenguaje claro y sencillo teniendo en cuenta al menor, art. 12).

3.2. Derechos de protección de datos de los niños

Respecto a los derechos de protección de datos y su adaptación para su ejercicio por los niños, el *Grupo de trabajo art. 29*, en la *Opinión 2/2009 on The protection of children's personal data*, en sus páginas 8 a 14, señala algunas peculiaridades que se deberían tener en cuenta para garantizar su efectividad en el caso de menores:

Derecho a ser informado

Según el *Grupo de Trabajo art. 29* se debería prestar atención a que la información que se ofrece a los menores o a sus representantes legales se diera de forma dosificada mediante avisos, que a su vez fueran simples, concisos y escritos con un lenguaje pedagógico. El art. 12.1 del *Reglamento de 2016* hace una mención a que se debe facilitar la información de

> "forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño".

Se trata de una exigencia menos concreta de lo que propone el *Grupo de Trabajo art. 29*, quien añade la necesidad de que el aviso breve (tipo *pop-up* de las *cookies*) se complete con un aviso más detallado donde se ofrezcan todos los detalles relevantes. La información, según el documento *The protection of children's personal data* debería situarse siempre en el lugar de la pantalla más visible y durante el tiempo necesario. Al mismo tiempo debería garantizarse que llega siempre a los padres y responsables legales simultáneamente al menor.

> "Se debe facilitar la información de "forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño" (*Reglamento europeo*, art. 12.1)

Derecho de acceso

De forma habitual quienes ejercen este derecho en representación de los menores son sus padres o tutores, y deben hacerlo en el interés superior del menor (principio que no se recoge en el *Reglamento de 2016*). En función de la madurez del menor debería considerarse una variedad de opciones para que el menor pudiera ejercitar el derecho de acceso solo, junto con los padres o tutores, o en su caso, mediante la representación de sus padres o tutores. La *Opinion 2/2009 on The protection of children's personal data* reflexiona sobre el problema existente sobre todo con adolescentes y en el área de salud, en temas como vida sexual, consumo de drogas, deseos de suicidio, etc., cuando el menor ha evitado informar a sus padres o tutores. Se plantea la discusión sobre si éstos mantienen el derecho de acceso a esa información y si, por el contrario, los menores podrían oponerse. El *Grupo de Trabajo art. 29* considera que se debe buscar el equilibrio entre las opciones posibles desde el criterio del interés superior del menor, siempre prestando relevancia a la apreciación del profesional de la salud al respecto. Defiende que las prácticas que mantienen los estados podrían considerarse como modelos para aplicar ese equilibrio. Así menciona Reino Unido, donde los mayores de 12 años pueden ejercer solos su derecho de acceso. Sin embargo, el *Grupo de Trabajo art. 29*, recomienda considerar no sólo la edad del menor sino también de qué datos se trata y la forma en la que han sido obtenidos.

Tal y como argumenta la *Opinión 2/2009 on The protection of children's personal data*, aunque el derecho de acceso tiene valor por sí mismo, su alcance es mayor en la medida en que hace posible el ejercicio de derechos como el de rectificación, borrado o bloqueo, para aquellos datos inexactos o inadecuados. En esta línea cabe reseñar que el *Reglamento* menciona indirectamente al menor para el ejercicio del derecho al olvido en el caso de datos personales recabados en las "ofertas relacionadas con la sociedad de la información" (art. 17.1 f).

Derecho de oposición

En la *Directiva de Protección de datos de 1995*, sobre la que reflexiona el *Grupo de Trabajo art. 29*, los límites del derecho de oposición deben tener un fundamento legítimo, y se comprende que en el caso de los menores de edad el espectro de intereses protegibles que actúen como fundamento de esos límites sean aún mayores. En opinión del *Grupo de Trabajo art. 29*, cuando se trate de procesamiento de datos con finalidad de marketing directo (art. 14 b) de la *Directiva de 1995*) debería quedar más claro que las personas, con mayor razón en el caso de menores, tienen derecho a oponerse en cualquier momento y sin necesidad de justificación alguna. Aspectos a los que el *Reglamento de 2016* hace referencia general (no considera las circunstancias especiales del menor), al mencionar que en relación con el marketing

"el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles" (art. 22 del *Reglamento de 2016*).

Derecho de notificación

La *Opinión 2/2009 on The protection of children's personal data* defiende la necesidad de que se notifique de forma obligatoria la existencia de procesamiento de datos a las personas afectadas, muy en particular cuando se trate de menores. Tanto la *Directiva de 1995* (art. 18) como el *Reglamento de 2016* (art. 33) contemplan la notificación a las autoridades de control pero sólo cuando exista una violación de la seguridad de los datos. El *Reglamento de 2016* limita la obligación de comunicación a los usuarios (no notificación) a la existencia de una violación de la seguridad de los datos del interesado que

> "entrañe un alto riesgo para sus derechos y libertades" (art. 34).

4. *Reglamento europeo de protección de datos personales* y la *Children's online privacy protection act* (*Coppa*) de Estados Unidos: dos planteamientos diferentes para la protección de los menores

4.1. *Reglamento europeo de protección de datos*: parquedad en el reconocimiento de la protección de datos de menores

El *Reglamento general de protección de datos* (UE) 2016/679, de 27 de abril (*Unión Europea*, 2016), tiene el mérito de proponer una articulación de principios, derechos, obligaciones, controles, límites y sanciones válidos para la defensa

de la privacidad de los ciudadanos en la situación tecnológica actual, cuyo máximo exponente referido a los datos son las tecnologías de datos masivos. Desde el punto de vista de los menores de edad, es una norma coherente con la *Carta europea de derechos fundamentales* de 2000 (*Unión Europea*, 2000), que vincula protección de datos con dignidad personal (art. 1 y 8) y que establece entre los derechos del menor el de la libertad de expresión. Además reconoce su capacidad de obrar en las materias que le conciernen, al señalar que la opinión de los menores

> "será tenida en cuenta en relación con los asuntos que les afecten, en función de su edad y de su madurez" (art. 24).

Por otra parte, el *Reglamento europeo* centra la protección especial del menor en las cuestiones que tienen que ver con su consentimiento y la información que debe recibir sobre las características del tratamiento de sus datos. Dispone la edad de 16 años para el consentimiento válido dado por el menor en relación con servicios de la sociedad de la información –aunque admite que los Estados pueden establecer otra edad que no sea inferior a los 13 años (art. 8.1)[4]-; y que cuando sea necesario el consentimiento de los padres o responsables legales deberá poder verificarse, teniendo en cuenta la tecnología disponible (art. 8.2). Al mismo tiempo se exige que la información sobre el tratamiento de datos sea

> "concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño" (art. 12).

Y no se dice nada más acerca de los menores hasta el art. 40 que menciona la obligación de los Estados y autoridades de control de promover códigos de conducta que apliquen el *Reglamento europeo*. Se recomienda además que entre otras cuestiones se preste atención a

> "la información proporcionada a los niños y la protección de éstos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño".

Completan estas previsiones específicas sobre los menores la introducción en el *Reglamento* del principio de protección de datos por diseño (art. 25), con medidas técnicas recomendadas como la seudonimización. La norma europea promueve con este medio una gestión del riesgo del tratamiento de datos personales desde el momento mismo de la concepción del diseño de aplicaciones, servicios y productos. Dentro de esta protección por diseño entraría también la especificidad de la protección de datos del menor (**Recio-Gayo**, 2017).

Si se compara la extensión de propuestas del *Grupo de Trabajo art. 29* sobre la protección de datos de los menores, referidas a los principios y a los derechos de protección de datos, llama la atención la parquedad con la que el *Reglamento general de protección de datos de 2016* resuelve la protección de los menores. Se ha optado por una extensión de los principios generales del *Reglamento* a la especificidad de los menores, en lugar de incorporar en el texto las normas específicas referidas al menor. Como señala **Lievens** (2016), deja a los legisladores nacionales y a las autoridades de protección de datos un amplio margen de acción que va desde la concreción de varios niveles de edad (la franja 13-16 como diferente a la franja 0-13, diferenciando adolescentes y niños o simplemente una única franja de menores de 16) con sus aspectos relativos a:

- representación, consentimiento y prevalencia del interés mejor del menor;
- grado de obligatoriedad de las medidas de verificación de edad y del consentimiento parental, así como al establecimiento de las técnicas *ad hoc*;
- grado de privacidad, transparencia, control, consentimiento revocable, etc., que la protección de datos del menor por diseño debe implementar.

Más pesimistas son **Macenaite** y **Kosta** (2017, p. 193) para quienes la escasez de protección específica para el menor en el *Reglamento* se debe a que los debates previos a su aprobación se han centrado sobre todo en el impacto económico que la protección de datos supone para las empresas en el mercado único europeo, abandonando las cuestiones que afectan a los sujetos más vulnerables.

Un aspecto negativo del *Reglamento general de protección de datos de 2016* es la eliminación de la referencia al derecho al olvido de los menores, algo que estuvo presente a los borradores del *Reglamento* y cuya omisión significa una disminución del nivel de protección del menor.

> "Los menores de edad no son conscientes de los riesgos de permitir el procesamiento de sus datos, tampoco en el supuesto de los datos sensibles"

4.2. Comparación con *Children's online personal data protection act* de Estados Unidos

Estados Unidos cuenta con una ley específica de protección de datos de niños en Internet, *Children's online protection act* (*Coppa*) de 1998, cuyo *Reglamento* ha tenido una última reforma en julio de 2013 (está pendiente una reforma iniciada en 2015)[5].

En ella se considera como información personal del menor protegible, además del nombre, la dirección postal de la casa, la dirección de correo electrónico o de otras formas de contacto online, teléfono, número de la seguridad social, cualquier identificador que permita reconocer al usuario en las diferentes plataformas y servicios online (el identificador incluye, pero no se limita a, un número de cliente contenido en una *cookie*, una dirección de protocolo de internet (IP), un número de serie de un procesador o dispositivo o un identificador único de dispositivo), fotografía, vídeo o archivo de audio que contenga la imagen o la voz del niño, la información de geolocalización suficiente para identificar el nombre de la calle y de la ciudad o pueblo, así como la información sobre el niño o sus padres que el operador de que se trate tenga vinculada al identificador (ref. sección § 312.2 *Definitions*).

La ley americana tiene como objeto la protección de datos de los menores de 13 años, motivo por el cual da a los padres el control de la información que se obtenga de los niños vía online. Se aplica tanto a webs como a los servi-

cios online dirigidos a menores, que incluyen las apps de los teléfonos móviles, así como a los operadores de webs dirigidas a audiencias generales o servicios online que tengan conciencia de que, de hecho, están recogiendo, usando u ofreciendo información personal de niños menores de 13 años y a webs o servicios online que tienen conocimiento de que están recogiendo información personal de usuarios de otra web o servicio online dirigidos a menores. Entre estos servicios online la *FTC* (*Federal Trade Commission*) menciona las plataformas online de videojuegos, redes sociales como *Facebook*, *Instagram*, *Twitter*, *MySpace*, etc., servicios de tiendas online, de publicidad, de música y de vídeos como *Spotify*, *YouTube* o *YouTube Kids*, de comunicación por voz e imagen, de mensajería como *WhatsApp*, servicios de búsqueda geolocalizada, etc.[6].

> Llama la atención la parquedad con la que el *Reglamento europeo de protección de datos* de 2016 resuelve la protección de los menores

Las obligaciones de todos estos operadores son:

- publicar la política de privacidad de forma clara y comprensible, describiendo los usos que dan a la información obtenida online de niños (§312.4 *Notice*);
- dar un aviso directo a los padres y obtener el consentimiento verificable de los mismos, con excepciones limitadas, antes de obtener información personal online de los niños (§312.5 *Parental consent*);
- proveer a los padres el acceso a la información personal de los niños para rectificarla y/o para eliminarla (§312.6 *Right of parent to review personal information provided by a child*);
- se prohíbe condicionar la participación de un niño en una actividad online a que el niño proporcione más información de la razonablemente necesaria para participar en esa actividad (§312.7 *Prohibition against conditioning a child's participation on collection of personal information*);
- mantener la confidencialidad, seguridad e integridad de la información obtenida de los niños, extendiéndose esta obligación en los pasos siguientes de una razonable transferencia de información sólo a partes capaces de mantener la confidencialidad y seguridad (§312.8 *Confidentiality, security, and integrity of personal information collected from children*).

La *Coppa* aborda al detalle cada una de estas obligaciones, de forma que apenas queda margen para una interpretación flexible de la normativa (**Golob**, 2015, p. 3471). Por ejemplo, dentro de la obligación de notificación a los padres y comunicación de la política de privacidad de la empresa responsable del tratamiento de datos se requiere que se ofrezca información entre otras cuestiones (ref. sección § 312.4) sobre:

- tipo de información personal que recogen de los niños (por ejemplo, nombre, dirección, correo electrónico, *hobbies*, etc.);
- cómo se obtiene esa información: directamente del niño o pasivamente mediante *cookies*;
- cómo será usada la información: por ejemplo para marketing dirigido al niño, para notificar resultados de concursos, o permitir al niño que publique la información en un chat;
- si se transferirá la información personal de los niños a terceras partes: y en este caso, la política de privacidad debe incluir la lista de los tipos de negocios a los que se ofrece la información (por ejemplo, *plug-ins* o redes publicitarias de marketing online) y cómo utilizan los terceros esa información;
- la obligación de exponer a los padres sus derechos respecto a la obtención y uso de los datos de los niños por parte del operador, además de facilitarles el ejercicio de los mismos.

Probablemente la exhaustividad de la regulación es más llamativa en la exigencia del consentimiento parental (ref. sección § 312.5). Como requerimiento general debe obtenerse el consentimiento de los padres siempre de forma previa a la recolección y uso de la información personal del niño. Se pide al responsable del tratamiento de datos que haga un esfuerzo razonable para obtener la verificación del consentimiento parental, teniendo en cuenta la tecnología disponible. Se acepta con este fin:

- firma en un certificado de consentimiento que se envía vía fax, mail o scanner electrónico;
- uso de la tarjeta de crédito o débito u otro medio de pago online que ofrece notificación de cada transacción en la cuenta del titular de la tarjeta;
- llamada por teléfono efectuada por personal preparado del operador;
- conexión por video-conferencia con personal preparado del operador;
- proveer una copia del DNI que pueda comprobarse en una base de datos, que se destruye una vez que se haya acabado el proceso de verificación.

> Un aspecto negativo del *Reglamento europeo de protección de datos* de 2016 es la eliminación de la referencia al derecho al olvido de los menores

En el caso de que la información personal del niño sólo se vaya a emplear para uso interno del operador, entonces se permite el método llamado "e-mail plus", que consiste en el envío a los padres de un correo electrónico al que los mismos contestan dando su consentimiento. Se completa la verificación con un envío de confirmación a los padres vía email, carta o llamada por teléfono. En este método debe ofrecerse a los padres la información de que pueden revocar su consentimiento en cualquier momento.

Otra característica de la *Coppa* es su apuesta decidida por la autorregulación de las empresas en la protección de la privacidad de los menores. La ley describe los mecanismos disciplinarios que deben contener los llamados *Programas de puerto seguro* (*Safe harbour programs* ref. sección § 312.11), a partir de las directrices que cada empresa o asociación de empresas resuelvan adoptar. El cumplimiento de

la *Coppa* a través de esos programas es el estándar mínimo exigido, de manera que pueden aprobarse directrices de protección de la privacidad de los niños en internet que sean aún más exigentes. Se añaden a las directrices, evaluaciones periódicas sobre su cumplimiento, indemnizaciones a los usuarios dañados, información y consultas públicas, así como los requisitos para mantener la adscripción de la empresa a los programas de puerto seguro.

Como resumen, la *Coppa* intensifica los principios de control parental y verificación del consentimiento de los padres, así como la responsabilidad proactiva de los responsables de datos (las empresas, negocios, asociaciones, etc. que tienen datos personales). Es exhaustiva en sus exigencias al mismo tiempo que permite una actualización de las mismas en función del principio del esfuerzo razonable, atendiendo a la tecnología del momento.

> La *Coppa* apuesta por la autorregulación de las empresas en la protección de la privacidad de los menores

6. Conclusiones

El *Reglamento europeo de protección de datos* se inhibe de la protección de los datos de los menores, a partir de la opción de ofrecer unos principios generales (en términos de consentimiento, transparencia y representación legal) y transferir a los Estados la tarea de elaborar una regulación más concreta sobre la protección de datos de menores

Se ha ignorado la mayoría de las propuestas presentadas en la *Opinion 2/2009* del *Grupo de Trabajo art. 29* on *The protection of children's personal data*; es cierto que se trata de propuestas sobre la *Directiva de protección de datos de 1995*, pero por su exhaustividad y por el carácter de los principios que señala, era lógico que el *Reglamento* recogiera parte de su planteamiento. En particular llama la atención que el *Reglamento* no mencione un principio clave en la protección de derechos del menor como es el principio de "interés superior del menor".

La exigencia de una protección de la privacidad por diseño, introducida en el art. 25 del *Reglamento*, puede contribuir a la mejora de la protección de los derechos del menor, pero al no haberse vinculado en el texto a los menores queda como una obligación general pendiente de concretarse, diluyéndose de alguna forma su especial adecuación para la protección de la privacidad de los menores.

La *Coppa* (*Children's online protection act*) de 1998 de Estados Unidos, con su última reforma de 2013, ofrece un modelo aplicable en muchos países europeos, tanto para establecer las obligaciones de los responsables de datos de transparencia y verificación del consentimiento parental, como para promover la responsabilidad proactiva de los responsables de datos (por ejemplo, mediante la obligación de elaborar y de informar de las políticas de privacidad).

Notas

1. Sus funciones se describen en los artículos 30 de la *Directiva 95/46/EC* y en el artículo 15 de la *Directiva 2002/58/EC*.

2. Enmiendas 157 a 159 sobre el art. 17, Derecho de supresión y al olvido. *Parlamento Europeo, Comisión de Libertades Civiles, Justicia y Asuntos de Interior*, 22 noviembre 2013.
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//ES

3. Enmienda 102 sobre el art. 8, Tratamiento de los datos personales relativos a los niños. *Parlamento Europeo, Comisión de Libertades Civiles, Justicia y Asuntos de Interior*, 22 noviembre 2013.
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//ES

4. **Serrano-Maíllo** (2013) señala algunos de los problemas de la validez del consentimiento de menores.

5. Texto de la ley accesible en:
http://bit.ly/2syMdWP

Un amplio estudio de la *Coppa* hasta el momento previo de su reforma en 2013 en **Andreu-Martínez** (2014).

6. FTC, *Children's online protection act, enforcement, rulemaking, reform.*
http://bit.ly/1IJZNI0

7. Referencias

Andreu-Martínez, María-Belén (2014). *La protección de los datos personales de los menores de edad*. Cizur: Thomson-Reuters Aranzadi. ISBN: 978 84 90149928

Baesens, Bart; **Bapna, Ravi**; **Marsden, James R.**; **Vanthienen, Jan**; **Zhao, J. Leon** (2016). "Transformational issues of big data and analytics in networked business". *MIS quarterly*, v. 40, n. 4, pp. 807-818.
https://www.misq.org/misq/downloads/download/editorial/646

Buyya, Rajkumar; **Calheiros, Rodrigo**; **Vahid-Dastjerdi, Amir**; (2016). *Big data: principles and paradigms.* Cambridge: Elsevier. ISBN: 978 0 128053942

Chen, Min; **Mao, Shiwen**; **Zhang, Yin**; **Leung, Victor** (2014). *Big data: Related technologies, challenges and future prospects*. London: Springer. ISBN: 978 3 319 06245 7

European Data Protection Supervisor (2015a). *Towards a new digital ethics. Data, dignity and technology. Opinion 4/2015.* September 11.
https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf

European Data Protection Supervisor (2015b). *Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability. Opinion 7/2015*, November 19.
https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

European Data Protection Supervisor (2016). *EDPS opinion on personal information management systems. Towards more user empowerment in managing and processing personal data. Opinion 9/2016*, October 20.
https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

Garmendia-Larrañaga, Maialen; **Jiménez-Iglesias, Estefanía**; **Casado-del-Río, Miguel-Ángel**; **Mascheroni, Giovanna** (2016). *Net children go mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015)*. Madrid: Red.es; Universidad del País Vasco.
https://addi.ehu.es/handle/10810/21546

Golob, Brandon (2015). "How safe are safe harbors? The difficulties of self-regulatory children's online privacy protection act programs". *International journal of communication*, v. 9, pp. 3469-3476.
http://ijoc.org/index.php/ijoc/article/view/3327

Jaroszek, Agatha (2015). "Online behavioural advertising and the protection of children's personal data on the Internet". *Wroclaw review of law, administration & economics*, v. 4, n. 2, pp. 56-65.
https://doi.org/10.1515/wrlae-2015-0015

Lievens Eva (2016). "Wanted: evidence base to underpin a children's rights-based implementation of the GDPR". *LSE. Media policy project blog*, November 10.
https://goo.gl/fxULwM

Lin, Chi; **Wang, Pengyu**; **Song, Houbing**; **Zhou, Yanhong**; **Liu, Qing**; **Wu, Guowei** (2016). "A differential privacy protection scheme for sensitive big data in body sensor networks". *Annales des telecommunications*, v. 71, n. 9-10, pp. 465-476.
https://goo.gl/md3Xjj
https://doi.org/10.1007/s12243-016-0498-7

Macenaite, Milda; **Kosta, Eleni** (2017). "Consent for processing children's personal data in the EU: Following in US footsteps?". *Information & communications technology law*, v. 26, n. 2, pp. 146-197.
https://goo.gl/L3nQye
https://doi.org/10.1080/13600834.2017.1321096

Mantelero, Alessandro; **Vaciago, Giuseppe** (2015). "Data protection in a big data society. Ideas for a future regulation". *Digital investigation*, v. 15, pp. 104-109.
https://goo.gl/G9syHC
https://doi.org/10.1016/j.diin.2015.09.006

Mayer-Schonberger, Viktor; **Cukier, Kenneth** (2013). *Big data: La revolución de los datos masivos*. Madrid: Turner. ISBN: 978 84 15832 10 2

Menon, Syam; **Sarkar, Sumit** (2016). "Privacy and big data: Scalable approaches to sanitize large transactional databases for sharing". *Management information systems quarterly*, v. 40, n. 4, pp. 963-982.
https://goo.gl/E9WgNo

OCDE (2017). *Informe PISA: El bienestar de los estudiantes 2015*.
http://bit.ly/2v1xBks
https://www.oecd.org/pisa/PISA2015-Students-Well-being-Country-note-Spain-Spanish.pdf

Payton, Theresa M.; **Schmidt, Howard A.**; **Claypoole, Theodore** (2014). *Privacy in the age of big data: Recognizing threats, defending your rights, and protecting your family.* Lanham: Rowman & Littlefield Publishers. ISBN: 978 1 442225466

Petersson, Gustav-Jakob; **Breul, Jonathan D.** (2017). *Cyber society, big data, and evaluation: Comparative policy evaluation*. New Brunswick: Transaction Publishers. ISBN: 978 1 412864367

Recio-Gayo, Miguel (2017). "Protección de datos desde el diseño: principio y obligación en el RGPD". *Elderecho.com*, 20 febrero.
https://goo.gl/7NQGmw

Serrano-Maíllo, Isabel (2013). "El derecho a la imagen de los menores en las redes sociales. Referencia especial a la validez del consentimiento". En: Corredoira-Alfonso, Loreto; Cotino-Hueso, Lorenzo (dirs.). *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*. Madrid: Centro de estudios Políticos y Constitucionales, pp. 442-475. ISBN: 978 84 25915611

Tomar, Geetam S.; **Chaudhari, Narendra S.**; **Bhadoria, Robin-Singh**; **Deka, Ganesh-Chandra** (2017). *The human element of big data: Issues, analytics, and performance*. Boca Ratón, FL: Chapman and Hall/CRC. ISBN: 978 1 498754156

Tucker, Patrick (2017). "Has big data made anonymity impossible?". *MIT technology review*, 7 May.
https://www.technologyreview.com/s/514351/has-big-data-made-anonymity-impossible

Unión Europea (2000). "Carta de los derechos fundamentales de la Unión Europea". *Diario oficial de las comunidades europeas*, 18 diciembre.
http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Unión Europea (2016). "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos". *Diario oficial de la Unión Europea*, 4 mayo.
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Working Group art. 29 (2009). *Opinion 2/2009, on The protection of children's personal data (General guidelines and the special case of schools),* February 11th, p. 7.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf

Zook, Matthew; **Barocas, Solon**; **Boyd, Danah**; **Crawford, Kate**; **Keller, Emily**; **Gangadharan, Seeta-Peña**; **Goodman, Alyssa**; **Hollander, Rachelle**; **Koenig, Barbara A.**; **Metcalf, Jacob**; **Narayanan, Arvind**; **Nelson, Alondra**; **Pasquale, Frank** (2017). "Ten simple rules for responsible big data research". *PLoS compututational biology*, v. 13, n. 3, e1005399.
https://doi.org/10.1371/journal.pcbi.1005399