Revista de Derecho Civil
http://nreg.es/ojs/index.php/RDC
ISSN 2341-2216
vol. XII, núm. 3 (julio-septiembre, 2025)
Ensayos, pp. 229-261

SOBRE LA NECESIDAD DE CONFIGURAR UN CONSENTIMIENTO VÁLIDO AL TRATAMIENTO DE DATOS PERSONALES OTORGADO POR MENORES DE EDAD EN ENTORNOS DIGITALES

Una cuestión sin resolver en plena era digital

Estela Brión Berdote

Profesora de Derecho Civil, Ayudante Doctor

Universidad de Deusto

TITLE: *The need for valid consent to the processing of personal data given by minors in digital environments. An unresolved issue in the digital age*

RESUMEN: Con la entrada en vigor en el año 2018 del Reglamento Europeo 679/2016, de 27 de abril de 2016, General de Protección de Datos (RGPD), se regulaban por vez primera las condiciones para la prestación válida del consentimiento al tratamiento de datos personales concedido por menores de edad. Si bien, el devenir de los años, unido al acelerado e imparable progreso hacia una sociedad digital, ha evidenciado la falta de eficacia de las medidas que impone la normativa. Constituye así tarea reservada del presente trabajo abordar los principales obstáculos que han impedido garantizar la concesión de un consentimiento válido al tratamiento por los más jóvenes. Se ofrece, además, un estudio sobre el Anteproyecto de Ley Orgánica para la protección del menor en entornos digitales aprobado recientemente por el Gobierno español en lo referente a la materia reseñada, así como posibles soluciones en orden a restaurar y asegurar el interés superior del menor internauta.

ABSTRACT: *With the entry into force in 2018 of General Data Protection Regulation 679/2016 of 27 April 2016 (GDPR), the conditions for the valid provision of consent to the processing of personal data granted by minors were regulated for the first time. However, the passing of the years, together with the rapid and unstoppable progress towards a digital society, has highlighted the lack of effectiveness of the measures imposed by the regulation. It is therefore the task of this paper to address the main obstacles that have prevented the granting of valid consent to processing by young people. It also offers a study of the Draft Bill of the Organic Law for the protection of minors in digital environments recently approved by the Spanish government with regard to the aforementioned matter, as well as possible solutions in order to restore and ensure the best interests of minors on the internet.*

PALABRAS CLAVE: *Protección de datos personales, menores de edad, entorno digital, redes sociales, consentimiento al tratamiento de datos personales, sistemas de verificación de la edad.*

KEY WORDS: *Personal data protection, minors, digital environment, social networks, consent to the processing of personal data, age verification systems.*

SUMARIO: 1. INTRODUCCIÓN. 2. ALGUNAS NOTAS SOBRE LA EVOLUCIÓN NORMATIVA DEL CONSENTIMIENTO AL TRATAMIENTO DE DATOS PERSONALES CONCEDIDO POR EL MENOR DE EDAD. 3. DE LOS PRINCIPALES PROBLEMAS QUE PRESENTA LA REGULACIÓN ACTUAL EN TORNO A LA PRESTACIÓN DEL CONSENTIMIENTO AL TRATAMIENTO DE DATOS PERSONALES DE MENORES A CAUSA DEL AVANCE DE LA SOCIEDAD DE LA INFORMACIÓN. *3.1. El consentimiento al tratamiento de datos personales por el menor en el RGPD y la LOPDGDD.* 3.2. *Principales inconvenientes que presenta la prestación del consentimiento al tratamiento de datos por los más jóvenes, especialmente en línea.* 4. EL ESPACIO DIGITAL EN EL SIGLO XXI: UN ESCENARIO QUE CADA VEZ PRESENTA MÁS RIESGOS PARA LOS MÁS JÓVENES. 4.1. *La privacidad del menor internauta en jaque*. 4.2. *Los grandes peligros que representa el entorno digital para el desarrollo y bienestar del menor.* 5. EL PROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS

MENORES DE EDAD EN LOS ENTORNOS DIGITALES: ¿SOLUCIÓN DEFINITIVA EN LO REFERENTE A LA PRESTACIÓN DEL CONSENTIMIENTO AL TRATAMIENTO DE DATOS POR MENORES DE EDAD? 6. CONCLUSIONES. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

El pasado 11 de abril de 2025, el Gobierno elevaba a Proyecto de ley el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales aprobado en junio de 2024. El ejecutivo, que presentaba el Anteproyecto como pionero y novedoso en el seno de la UE, propone una suerte de modificaciones en diversos ámbitos con el fin de devolver seguridad jurídica al espacio digital en el que los menores de edad se desenvuelven.

En efecto, los menores de edad son un colectivo de gran presencia en el escenario en línea. Desde edades verdaderamente tempranas han interiorizado el manejo de herramientas digitales en su día a día. En la actualidad, no sorprende comprobar que menores con una edad inferior a 4 años manejan tabletas, *smartphones* u ordenadores con una soltura y destreza sorprendente para los adultos. Sin embargo, dicha facilidad con la que los más jóvenes se desenvuelven en las diferentes aplicaciones, webs, etc., no viene acompañada de un manejo responsable y garantista para con sus derechos fundamentales. Lo cierto es que la falta de madurez de la que adolecen, no les permite proteger estos derechos fundamentales como debiera. Consciente de ello, el Anteproyecto propone una serie de medidas y obligaciones en distintos ámbitos como la protección de los consumidores y usuarios, el educativo, el sanitario y sector público con el fin de convertir el espacio digital en un entorno de mayor seguridad.

Entre dichas medidas, destaca-por encontrarse en sintonía con la investigación que se propone- la elevación de la edad para prestar consentimiento válido al tratamiento de datos personales de los 14 años a los 16 propuesta por el legislador. Ahora bien, nos preguntamos si dicho incremento en sí mismo, no acompañado de otras medidas complementarias logra el objetivo que se propone: acabar con la presencia de menores en espacios en los que no alcancen la edad para prestar consentimiento válido al tratamiento de datos.

2. ALGUNAS NOTAS SOBRE LA EVOLUCIÓN NORMATIVA DEL CONSENTIMIENTO AL TRATAMIENTO DE DATOS PERSONALES CONCEDIDO POR EL MENOR DE EDAD

Cabe afirmar, que las normas que han regulado el derecho a la protección de datos personales el pasado siglo han omitido cualquier mención a la minoría de edad en su

articulado. Efectivamente, hasta la primera década del siglo XXI, los textos normativos que han concedido amparo jurídico a la prestación del consentimiento al tratamiento de datos personales no han positivizado la prestación del mismo por personas que no alcanzan la mayoría de edad.

En este orden de cosas, la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE), guardó silencio al respecto, dejando al albur de las normativas nacionales de los Estados miembro la regulación sobre dicha materia. Así, durante varias décadas, el consentimiento al tratamiento de datos personales otorgado por menores de edad se ha guiado por lo dispuesto en las normas generales sobre capacidad.

Sobre este particular, ha de advertirse que el derecho a la protección de datos personales se considera un derecho fundamental regulado en el art. 18.4 de la Constitución Española (en adelante, CE). Consecuentemente, en el caso español, si bien el ejercicio de derechos fundamentales por parte del menor no ha recibido la atención que debiera en comparación con el amplio desarrollo normativo y doctrinal que ha protagonizado en el Derecho privado[1], el menor se encuentra dotado de una capacidad progresiva que depende de la capacidad natural y madurez que esté presente a medida que cumple años[2].

A este respecto, deviene indispensable citar la Convención de los Derechos del Niño, de 20 de noviembre de 1989 (en adelante, Convención de los Derechos del Niño de 1989), como primer texto jurídicamente vinculante que sienta la capacidad progresiva del menor para el ejercicio de derechos fundamentales de su titularidad. Este texto, obliga a los Estados ratificantes a acomodar sus ordenamientos jurídicos con la finalidad de

[1] Abundan trabajos de la doctrina ahondando en el ejercicio de derechos patrimoniales por parte del menor en los que se vislumbra la evolución que ha sufrido la misma desde el siglo pasado. Entre ellos destacan las consideraciones más tradicionales de LASARTE ÁLVAREZ, Carlos, *Compendio de derecho de la persona y del patrimonio,* Madrid, Dykinson, 2014 que abogan por una visión más dualista frente a, por ejemplo, LACRUZ BERDEJO, quien afirma que si bien hasta el siglo XX, se privaba absolutamente al menor de la capacidad de concluir actos con eficacia jurídica, en la actualidad, al menor se le reconoce como una persona capaz, salvo para aquellas cuestiones que la norma le prohíba expresamente. LACRUZ BERDEJO, Jose Luis., *Elementos de Derecho civil I. Parte general,* Vol. II, Madrid, Dykinson, 2010, pp. 119-121.

[2] Reviste especial interés el planteamiento que propone RAMOS CHAPARRO sobre la superación de un esquema dualista o antitético de la edad, por otro gradualista en el cual, la capacidad aumenta progresivamente a medida que la edad del sujeto aumenta, llegando así un momento en el que se determina la plenitud de la misma al alcanzar la mayoría de edad. RAMOS CHAPARRO, Enrique., «Niños y jóvenes en el derecho civil», *Derecho Privado y Constitución*, 1995, núm. 7, p. 183.

garantizar una capacidad evolutiva en el ejercicio de derechos fundamentales. Por tanto, dos son los preceptos que destacan a tal fin en el estado español desde que este ratificara la Convención en el año 1990. Por una parte, el art. 162 CC, que dispone que la representación legal queda excluida para los actos relativos a los derechos de la personalidad que el menor acorde a su madurez pueda ejercitar por sí mismo; por otra parte, la Ley Orgánica 1/1996, de 15 de enero, de Protección jurídica del Menor (en adelante, LOPJM), que apostilla en su exposición de motivos que se reconoce la titularidad de derechos por parte del menor y una capacidad progresiva para ejercitarlos.

En suma, el menor se encuentra dotado de una capacidad progresiva que aumenta a medida que cumple años y siempre que muestre madurez suficiente, la representación legal quedará excluida cuando del ejercicio de un derecho fundamental se trate. Ahora bien, aquellos casos en los que el menor no demuestre madurez bastante para el ejercicio autónomo de derechos, serán sus representantes legales los que habrán de proceder a su ejercicio, pero en calidad de prestarles asistencia, ya que, tal y como dispone el art. 162 CC, la representación legal queda excluida en este contexto[3]. En definitiva, acorde al criterio expuesto, y en ese entonces, el ejercicio del derecho a la protección de datos personales cuya titularidad recayese en menores de edad se acometería de modo autónomo siempre que mostraran madurez bastante. Contrariamente, serían sus representantes quienes procederían a su ejercicio.

Expuesto cuanto antecede, no es hasta el año 2018 cuando el derecho europeo positiviza las vicisitudes relativas al tratamiento de datos personales de menores de edad, regulando la capacidad del menor para prestar un consentimiento autónomo al tratamiento de datos personales, como veremos más adelante. No obstante, la Unión Europea (en adelante, UE), no se mostraba ajena a la problemática que suscitaba la ausencia de regulación de la mentada cuestión hasta señalada fecha. En tal sentido, el Dictamen 2/2009, de 11 de febrero de 2009, sobre la protección de datos personales de los niños elaborado por el Grupo de Trabajo del Artículo 29[4], ya denunciaba que la

[3] En sintonía con dicha consideración se muestran DIEZ PICAZO Y GULLÓN cuando disponen que se exceptúan de la representación de los progenitores los actos relativos a derechos de la personalidad que el hijo o la hija pueda realizar por sí mismo de acuerdo con las leyes y sus condiciones de madurez. DIEZ PICAZO, Luis., Y GULLÓN, Antonio., *Sistema de Derecho civil,* Volumen IV, Tomo I, Madrid, Tecnos, 2012.

[4] El Grupo de Trabajo del Artículo 29 se trata de un organismo asesor independiente creado por la Directiva 95/46/1995 con el fin de asesorar respecto a la protección de datos personales y privacidad. Este organismo, se sustituye formalmente por el Comité Europeo de Protección de Datos (CEPD) desde la entrada en vigor del Reglamento Europeo 679/2016, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos

Directiva 95/46/CE no mencionaba expresamente los derechos de los menores a la privacidad, ni tomaba en consideración en su articulado las particularidades de la vida de los menores[5].

Advertida dicha carencia, el objetivo del Dictamen 2/2009 recientemente expuesto, se identificaba con analizar los principios generales a aplicar a la protección de datos personales de los menores de edad al fin de salvaguardar la protección de su privacidad. Dadas las circunstancias, el Dictamen opta por adaptar los principios del tratamiento consagrados en la Directiva 95/46/CE a la minoría de edad.

En particular, relacionado con la presente investigación, aborda las condiciones del consentimiento al tratamiento de datos concedido por menores (recordemos que, en el año 2009, no existía normativa que regulara las condiciones de validez del consentimiento prestado por personas menores de edad). En sintonía con la Convención de los Derechos del niño, el Grupo de Trabajo del Artículo 29 dispone que el menor podrá prestar consentimiento al tratamiento de manera autónoma siempre que demuestre madurez suficiente. Por tanto, habrá de considerarse el nivel de desarrollo físico y psicológico en el ejercicio del derecho a la protección de datos personales del que son titulares. En caso contrario, los progenitores habrán de prestar dicho consentimiento, siempre en interés superior de este.

Puede observarse cómo el organismo europeo, se alinea con el concepto de capacidad evolutiva sentando por la Organización de las Naciones Unidas en la Convención de los Derechos del niño de 1989 recientemente citada. Antes bien, el legislador español se desvincula de dicho criterio a la hora de regular la capacidad del menor para prestar consentimiento válido al tratamiento de datos personales.

Efectivamente, el legislador español, dos años antes de que el Grupo de Trabajo del Artículo 29 diera a conocer el Dictamen, establece la edad de catorce años para la prestación del consentimiento del menor por medio del art. 13 del Real Decreto Legislativo 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, Real Decreto 1720/2007). El legislador pareció decantarse por un criterio cronológico que, posteriormente, también emplearía la UE

datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (en adelante, RGPD).

[5] Este hecho también se ha advertido por la doctrina. Para más concreción véase GÓMEZ JUÁREZ SIDERA, Isidro., «Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la Legislación Española», *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2006, núm. 11, 2ª parte, p. 2.

como quedará de manifiesto. En tal sentido, a pesar de que la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal guardara silencio, al igual que la Directiva 95/46/CE que trasponía en cuanto a la prestación del consentimiento concedido por menores de edad, el legislador español impone dicho límite por medio de un Real Decreto Legislativo[6].

3. DE LOS PRINCIPALES PROBLEMAS QUE PRESENTA LA REGULACIÓN ACTUAL EN TORNO A LA PRESTACIÓN DEL CONSENTIMIENTO AL TRATAMIENTO DE DATOS PERSONALES DE MENORES A CAUSA DEL AVANCE DE LA SOCIEDAD DE LA INFORMACIÓN

3.1. El consentimiento al tratamiento de datos personales por el menor en el RGPD y la LOPDGDD

Si bien la positivización de la prestación del consentimiento al tratamiento de datos personales por menores de edad puede tildarse de excesivamente pausada y tardía[7], finalmente la UE acoge en su articulado el mismo. En concreto, esta materia se regula en el art. 8 del Reglamento Europeo 679/2016, de 27 de abril de 2016, 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) (en adelante, RGPD). El organismo europeo toma conciencia, al amparo del Considerando 38, de la necesidad de protección específica de los más jóvenes ante la posibilidad de que sean menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales.

Fruto de dicho considerando, la normativa europea incorpora tres garantías fundamentales destinadas expresamente a la protección de la información personal de la minoría de edad: la adaptación del principio de transparencia a las vicisitudes de los más jóvenes; las condiciones de validez para la prestación de un consentimiento válido; por último, la relevancia del derecho de supresión o "al olvido" de informaciones cuya titularidad recaiga en menores de edad. Habida cuenta del objeto de la presente

[6] Este hecho, no se ha encontrado libre de críticas por la doctrina, que pronto visibilizó que una cuestión de tal transcendencia debería regularse bajo la figura de Ley Orgánica VÁZQUEZ DE CASTRO, Eduardo., «Protección de datos personales, redes sociales y menores», *Revista Aranzadi de Derecho y nuevas Tecnologías*, 2012, núm. 29/2012 parte Doctrina, p. 54.

[7] Sobre este particular, cabe afirmar que la inseguridad jurídica sufrida por el menor en relación a la protección de los datos personales de su titularidad se ha extendido durante décadas habida cuenta que el derecho a la protección de datos personales se consagra por el Tribunal Constitucional en el año 2000 por medio de sus célebres sentencias STC 290/2000, de 30 de noviembre, Boletín Oficial del Estado, de 4 de enero de 2001, núm. 4, pp. 70-93 y STC 292/2000, de 30 de noviembre, Boletín Oficial del Estado, núm. 4, pp. 104-118.

investigación, nos centraremos pues en la segunda de las garantías concernientes a la prestación del consentimiento.

El art. 8 del RGPD, dispone que los menores de edad podrán prestar consentimiento de manera autónoma al tratamiento de datos cuando alcancen la edad de 16 años. Sin embargo, también sienta que los Estados miembro podrán decantarse por una edad inferior, siempre que se encuentre comprendida entre los 13 y 16 años de edad (art. 8.1 párrafo segundo). Para los casos en los que los menores no tengan la edad señalada y consecuentemente, no posean capacidad para ejercitar de modo autónomo este derecho, serán los representantes legales quienes deberán proceder a su prestación. Así, el ordenamiento jurídico nacional, al igual que en el año 2007, continúa inclinándose por establecer la edad en 14 años por medio del art. 7 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (en adelante, LOPDGDD). Aun así, debe matizarse que la edad finalmente elegida, no recibió el respaldo de la totalidad de los grupos parlamentarios. El Grupo Parlamentario Confederal Unidos Podemos presentó una enmienda al establecimiento de la edad en 14 años proponiendo mantenerla en los 16 propuestos por el RGPD[8].

Convenimos con determinadas conclusiones expuestas en la enmienda por el Grupo Político. En primer lugar, aducen que la rebaja de la edad de 16 años dispuesta en el RGPD ha de tildarse de injustificada habida cuenta que una de las razones alegada por el legislador nacional defiende que la edad seleccionada por otros países colindantes es de 13 años. Nada más lejos de la realidad, Francia se decanta por instaurar la edad para prestar consentimiento válido al tratamiento en 15 años[9]. En segundo lugar, la enmienda afirma que el interés superior del menor debe imperar sobre los intereses del mercado y las empresas, pues estas frecuentemente poseen intereses lucrativos diversos a los que inicialmente se disponen. En último lugar, manifiestan firmemente su descontento al afirmar que no cabe aceptar que el proyecto se decante sin justificación suficiente por el menor nivel de protección permitido por el RPGD, pues ello colisiona con el interés superior del menor que ha de imperar frente a cualquier decisión en la que se involucren derechos de menores. Estas afirmaciones cobrarán especial relevancia más adelante, como veremos.

[8] Boletín Oficial de las Cortes Generales, XII Legislatura, Serie A, 13-2, enmienda núm. 5, de 18 de abril de 2018, p. 6.

[9] Otros países de la UE- que no son cercanos a España- como Croacia, Alemania, Hungría, Irlanda, Luxemburgo, Holanda, Polonia, Rumania, Eslovaquia y Eslovenia han establecido la edad para prestar consentimiento en 16 años. BADILLO LÓPEZ, Mª Teresa., «Las medidas contenidas en el Anteproyecto de la Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. En particular, la elevación de la edad mínima de los menores para ceder sus datos personales», *Revista Estudios Jurídicos. Segunda Época,* 2025, núm. 25, p. 15.

Por otra parte, queda en evidencia que, tanto el legislador europeo, como el legislador español se desligan del criterio de madurez instaurado durante décadas por la Convención de los Derechos del niño de 1989. Este cambio de parecer se ha tratado de una cuestión fuertemente debatida por la doctrina española. En este sentido, determinado sector doctrinal encabezado por HERRÁN ORTIZ aduce que el criterio cronológico instaurado no cohonesta con el espíritu del restante ordenamiento jurídico civil en cuanto a la valoración de la madurez del menor para el ejercicio autónomo de derechos de su titularidad[10].

Cierto es que, si bien el criterio de madurez continúa inspirando la normativa civil en lo referente a la capacidad del menor, el establecimiento de una edad concreta a partir de la cual se presume capaz al menor contraviene el mismo. Antes bien, no se debe soslayar que no todos los contextos relacionados con la prestación del consentimiento al tratamiento de datos del menor permiten valorar la madurez de este. Ciertamente, cuando la prestación del consentimiento ocurre en el ámbito digital, dicho criterio ha demostrado no ser útil ante la falta de contacto físico con el menor en aras de determinar su grado de madurez. En definitiva, a nuestro parecer, valorar la capacidad del menor para ejercitar el derecho a la protección de datos personales conforme a un criterio cronológico, resulta acertado de conformidad con GIL MEMBRADO[11]. Especialmente ahora que nos encontramos inmersos en plena era digital y los derechos fundamentales se ejercitan, cada vez más, en línea.

Sin perjuicio de lo expuesto, nos preguntamos si la principal medida incorporada en la normativa, esto es, el establecimiento de una edad concreta para presumir capaz al menor para ejercitar su derecho a la protección de datos personales constituye garantía suficiente ante el imparable avance de la Sociedad de la información. En este orden de cosas, el RPGD impone a los responsables del tratamiento la obligación de realizar esfuerzos razonables al fin de verificar la edad del interesado, así como la prestación del consentimiento por sus representantes legales cuando no alcanza la edad preestablecida por el Estado miembro (art. 8.1 y 8.2 RGPD). Ello implica, que el responsable del tratamiento debe verificar eficazmente, por una parte, la edad del

[10] HERRÁN ORTIZ, Ana Isabel., «Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?», *Revista R.V.A.P.* 2010, núm. 87-88, p. 553. En idéntico parecer manifiesta GRIMALT SERVERA, Pedro., «Los menores e internet: capacidad versus protección de la vida privada» en CUENCA CASAS, M., ANGUITA VILLANUEVA, J. A., ORTEGA DOMÉNECH, J., (Coordinadores), *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa*, Madrid, Dykinson, 2013, p. 188.

[11] GIL MEMBRADO, Cristina., «Límites a la autonomía de la voluntad en la disposición de la imagen del menor a través de las Redes Sociales», *La Ley Derecho de Familia,* 2017, núm. 13, p. 7.

potencial interesado o titular de la información personal: por otra parte, eventualmente, la concesión del consentimiento por los representantes legales para los casos en los que no alcanza dicha edad (14 años). Queda en evidencia, que la normativa actualmente en vigor no ha evolucionado en exceso en relación con esta cuestión desde el año 2007 cuando se aprobó el Real Decreto Legislativo 1720/2007 de desarrollo de la LOPD de 1999 a pesar de que el escenario digital haya evolucionado con carácter vertiginoso.

3.2. Principales inconvenientes que presenta la prestación del consentimiento al tratamiento de datos por los más jóvenes, especialmente en línea

A pesar de que los arts. 8 RGPD y 7 LOPDGDD, instauren que el menor de edad cuya edad supere los 14 años (en el caso de España), podrá prestar por sí mismo consentimiento válido al tratamiento de datos personales, varios son los impedimentos que se presentan en orden a garantizar su validez cuando ocurre en línea.

Sin desmerecer los restantes contratiempos a los que se enfrenta esta prestación del consentimiento[12], a nuestro juicio, destaca sobre los demás que el gran elenco de los servicios digitales de los que el menor es usuario en la actualidad, no se encuentran dotados de mecanismos de verificación eficaces de la edad del menor.[13] Por tanto, muchos de los consentimientos otorgados carecen de validez al concederse por menores faltos de capacidad. Resulta evidente la falta de seguridad jurídica que genera esta circunstancia, pues durante décadas los menores llevan prestando consentimientos al tratamiento no válidos que atentan contra su interés superior[14].

Véase así, que los menores solamente deben faltar a la verdad sobre su edad para sortear los sistemas implementados por el gran porcentaje de servicios en el espacio en línea[15]. Las consecuencias son devastadoras si se tiene en cuenta que, por una parte,

[12] A saber, la información que se comparte con los menores de edad a efectos de reputar el consentimiento informado acorde al art. 4.11 RGPD carece de claridad y sencillez, ni se adapta al público joven; el diseño del consentimiento al tratamiento, cuando este ocurre en línea, resulta cuestionable desde el punto de vista de la normativa, pues no puede estimarse inequívoco, ni expreso al configurarse en bloque junto con la aceptación de las condiciones del servicio, entre otros.

[13] Redes sociales más empleadas por los jóvenes como TikTok no poseen ningún mecanismo de verificación más allá de uno declarativo de la edad; lo mismo sucede con X. Esto es, a pesar de que estos espacios deben verificar la edad de los futuros usuarios, no llevan a cabo dicha comprobación.

[14] Sin duda, no le falta razón a BARRIUSO RUIZ cuando afirma que estos consentimientos pueden reputarse nulos. BARRIUSO RUIZ, Carlos., «Las Redes sociales y la protección de datos hoy», *Anuario de la Facultad de Derecho-Universidad de Alcalá II,* 2009, núm. 2, p. 328.

[15] En tal sentido, DAVARA FERNÁNDEZ DE MARCOS manifiesta que los menores de edad, desde los ocho o nueve años que, sin conocimiento de sus representantes legales, se registran en redes sociales

diariamente consienten el tratamiento de su información personal y acceden a servicios *online* millones de menores de 14 años; por otra parte, esta circunstancia lleva ocurriendo desde la irrupción masiva de estos espacios en el año 2009 aproximadamente[16].

Sin embargo, tras varios años desde la irrupción de los servicios en línea, tales como redes sociales, videojuegos *online*, etc., que los menores emplean con asiduidad, la verificación de los potenciales usuarios (interesados) continúa sin solución jurídica[17]. Efectivamente, la doctrina lleva más de una década denunciando esta realidad. Ya en el año 2009 MITLLANS PERELLÓ mostraba la preocupación señalada cuando identificaba que en el caso de las redes sociales, el principal problema en su empleo se identificaba con cómo detectar de forma efectiva a sujetos menores de 14 años[18]. Varios años después, GUARDIOLA SALMERÓN afirmaba que ninguna red social dispone de un sistema eficaz y seguro de verificación de la edad que garantice su autenticidad y veracidad. En plena segunda década del siglo XXI, las afirmaciones expuestas continúan resultando válidas.

En este orden de ideas, lo cierto es que las dificultades parecen residir en la falta de consenso acerca del sistema de verificación idóneo desde el punto de vista jurídico. En realidad, el legislador y los organismos oficiales cuyo fin se identifica con interpretar la normativa sobre protección de datos, han mostrado sus recelos sobre aquellos sistemas que no cumplieran el principio de minimización, esto es, que exigieran el tratamiento de más datos al fin de verificar la edad del potencial usuario. A tal efecto, sistemas como exigir una fotografía del Documento Nacional de Identidad se han descartado con carácter reiterado por el motivo expuesto.

(consintiendo al tratamiento de datos), declarando una fecha de nacimiento anterior a la real. DAVARA FERNÁNDEZ DE MARCOS., Laura, «Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos Breve referencia al fenómeno Pokémon Go», *XX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos,* Madrid, 2007. p. 15.

[16] Encuesta de la FUNDACIÓN PFIZER sobre la Juventud y las redes sociales en Internet. Informe de resultados de la encuesta, septiembre 2009. Disponible en https://www.fundacionpfizer.org/sites/default/files/informe_final_encuesta_juventud_y_redes_sociales.pdf, [Consulta: 7 de mayo de 2025].

[17] Recientemente, MORILLAS FERNANDEZ aduce que continúa la incógnita de cómo se está aplicando en la actualidad el art. 8.2 RGPD en cuanto a los sistemas de verificación de la edad. MORILLAS FERNÁNDEZ, Marta., «Menores vulnerables y redes sociales: Nuevos retos jurídicos en la protección ante el uso inadecuado. Edad, educación y controles por defecto», *Revista Internacional de Doctrina y Jurisprudencia,* 2024, núm. 32, p. 55.

[18] La autora profería dicha afirmación en el año 2016, en MITLLANS PERELLÓ, Esther., «Impacto de las redes sociales en el derecho a la protección de datos personales», *Anuario de la Facultad de Derecho-Universidad de Alcalá II*, 2009, núm. 2, p. 113.

Antes bien, debemos subrayar que, si bien el sistema a implementar debe respetar el principio de minimización, igualmente debe configurarse desde un enfoque proporcionado basado en la evaluación de los riesgos incurridos[19]. Así, debe abandonarse la idea de que el espacio en línea y en particular, las redes sociales, se configuran como espacios inofensivos que fomentan la interacción entre los jóvenes. Ciertamente, el mecanismo de verificación habrá de considerarse proporcionado, es decir, deberá adecuarse a los fines de tratamiento alegados por el servicio digital y al riesgo que estos generen para la privacidad del usuario. Especialmente, cuando este es menor de edad, pues determinados riesgos se potencian dada su falta de madurez[20]. Sobre esta cuestión, volveremos más adelante.

4. EL ESPACIO DIGITAL EN EL SIGLO XXI: UN ESCENARIO QUE CADA VEZ PRESENTA MÁS RIESGOS PARA LOS MÁS JÓVENES

Resulta innegable que el espacio digital, y en especial las redes sociales, constituyen un grave peligro, tanto para la privacidad del menor, como para su desarrollo hacia la madurez. De hecho, varias décadas de presencia de los más jóvenes en la red han terminado por visibilizar una pluralidad de peligros a los que estos se enfrentan.

Ahora bien, fruto de la rápida evolución que sufre el espacio digital, los riesgos asociados al manejo de herramientas digitales y redes sociales por personas menores de edad han proliferado considerablemente en la última década. Sobre este particular, resulta de especial interés el trabajo culminado por la Organización para la Cooperación y Desarrollo Económico (en adelante, OCDE) en el que actualiza y visibiliza en un Informe los principales riesgos en el entorno virtual para el menor, atendiendo a su evolución desde el año 2011 hasta 2021[21].

La propia OCDE, reconoce que los peligros han progresado considerablemente en los años sometidos a análisis, por lo que se propone brindar un estudio de los mismos

[19] En ese sentido, revisten especial interés las palabras de la Comisión francesa de protección de datos (CNIL) en Recomendación núm. 7 en relación con los derechos digitales de los menores. Disponible en: https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-prive [Consulta: 14 de marzo de 2025]

[20] Así lo dispone el CEPD, aportando, además, que, si el proveedor de servicios que desea verificar la edad se encuentra dotado de contenido apto para todos los públicos, ello no superaría el principio de proporcionalidad y necesidad. Véase así, *Statement 1/2025, on Age Assurance*, adopted on 11 February 2025, p. 3.

[21] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO, «Children in the digital enviroment, revised typology of risks». Disponible en: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf [Consulta: 10 de marzo de 2025].

estructurándolos en cuatro categorías, a saber: riesgos de contenido, riesgos de conducta en el entorno virtual, riesgos generados por el contacto o interacción en línea y, por último, los riesgos para el consumidor. Adicionalmente, también identifica tres peligros transversales a las cuatro categorías señaladas como es el caso de los riesgos para la privacidad, los peligros a causa de la tecnología avanzada y los riesgos para la salud y el bienestar del menor.

Sin perjuicio de que analizaremos todas las categorías señaladas por el organismo, comenzaremos por profundizar en los riesgos transversales para todas las categorías de riesgos expuestos, pues estimamos que, con salvedad de los riesgos para la salud, son aquellos que guardan mayor relación con la privacidad del menor. Posteriormente, nos centraremos en el estudio de las categorías que, si bien su vínculo con la privacidad es menor, inciden considerablemente en el desarrollo y proceso de maduración del menor.

4.1. *La privacidad del menor internauta en jaque*

Existe consenso sobre la erosión que sufre la privacidad del menor en el espacio digital, pues el diseño de estos espacios predispone un desvelo constante e indiscriminado de información personal propia, pero también de terceras personas. Es más, los más jóvenes viven en estos espacios, por lo que han terminado por asimilar una falsa sensación de control sobre su información personal en un canal expuesto al mundo[22]. Conformes con BATUECAS CALETRÍO, los menores navegan con una sensación de encontrarse en un entorno privado y de confianza. Antes bien, cualquier información disponible en la red, resulta susceptible de alcanzar una gran difusión[23].

En adición, cuando comparten información personal concerniente a terceras personas, pueden poner en riesgo otros derechos fundamentales relacionados con la privacidad de los que estas son titulares, a saber: el derecho a la intimidad personal o familiar, la propia imagen o el honor (art. 18.1 CE), pero también el derecho a la protección de datos personales (art. 18.4 CE). Efectivamente, los menores pueden publicar fotografías, vídeos, críticas, etc., sobre terceras personas que pueden llegar a lesionar

[22] En verdad, los menores navegan en la red con una falsa sensación de seguridad y confianza generada por la cotidianeidad en el manejo de las TIC desde su mismo nacimiento. CASTILLA BAREA, Margarita., «La protección de los menores el internet (Comentario al artículo 84 LOPDGDD)», en TRONCOSO REIGADA, A., (director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 3951-3952.

[23] BATUECAS CALETRÍO, Alfredo., «El control de los padres sobre el uso que sus hijos hacen de las redes sociales», en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información,* Granada, Comares, 2015, p. 139.

los derechos fundamentales señalados. En tal sentido, cabe traer a colación el reciente pronunciamiento de la Audiencia Provincial de Bizkaia, de 20 de septiembre de 2024, en el que se condena en el ámbito civil a un menor por la difusión de fotografías íntimas del demandante (menor de edad también) en un perfil de Instagram creado a tal efecto[24].

Por otra parte, los peligros no terminan con el riesgo de compartir información personal propia y de terceros, sino que gran parte de los proveedores de servicios digitales, y particularmente los proveedores de redes sociales, han hallado el modo de rentabilizar sus negocios a partir del desmesurado volumen de información generado por nuestros hábitos en línea. Acertadamente identifica la OCDE, que la información de menores tratada, no se conforma exclusivamente por aquella que estos comparten activamente en diversos servicios en línea. En la actualidad, el volumen de datos recabado con el objetivo de someterla a exhaustivos tratamientos de datos personales se divide en tres grupos.

El primero, lo conforman los datos activos, esto es, los datos que el propio usuario comparte en la red. Huelga decir, que los usuarios toman conciencia, principalmente, sobre estos datos sometidos a tratamiento. En la actualidad, en cambio, constituye una realidad el tratamiento de datos personales recabados de la observación del comportamiento del usuario o datos pasivos en el espacio *online*[25]. Sirva como ejemplo, que las redes sociales acceden a un gran abanico de datos personales deducidos del comportamiento de sus usuarios como, la señal del teléfono, el modelo de este, la ubicación, la mensajería, etc.[26] Las *cookies* de análisis o medición también

[24] Efectivamente, la Sentencia de la Audiencia Provincial de Bizkaia 271/2024, de 20 de septiembre de 2024, ECLI: ES: APBI:2024:765, condena a un menor al resarcimiento de daños y perjuicios generados a causa de la publicación de fotografías de otro menor en perfiles de Instagram creados por el demandado a tal efecto. La sentencia señala que el menor demandado creaba perfiles de Instagram desde los que enviaba tanto las fotografías íntimas, como los mensajes por los que amenazaba al demandado con difundir las mismas. Señala la sentencia, que dichas imágenes se recababan tras ganarse la confianza del demandado a través de la red social. Lamentablemente, no se trata de un caso aislado. Desde hace varios años que los organismos judiciales conocen de conductas en las que se revelan imágenes íntimas con el objetivo de dañar a la víctima. A tal efecto, véase a la sentencia de la Audiencia Provincial de Valencia 372/2019, de 27 de septiembre de 2019, ES: APV:2019:4490.

[25] Se entiende por dato pasivo toda aquella información que se intercambia en segundo plano por el dispositivo y las aplicaciones sin ninguna notificación obvia al usuario. LLANEZA GONZÁLEZ, Paloma., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*, Barcelona, 2019, p. 75.

[26] Concretamente, redes sociales como Instagram, pertenecientes al Grupo Meta, recaban las características del dispositivo tales como, la información sobre el sistema operativo, la versión de *hardware* y *software*, el nivel de carga de la batería, la potencia de la señal, el espacio de almacenamiento disponible, el tipo de navegador, los tipos y nombres de aplicaciones o archivos, y los

poseen idéntico propósito, que no es otro que compartir con el responsable de su instalación información sobre los hábitos del usuario[27]. Por último, la tercera categoría de datos se corresponde con los datos inferidos, es decir, aquella información que tras un análisis de los datos recabados por medio de algoritmos inteligentes, infieren nuevos datos a raíz de los datos primitivos. En este contexto, estos servicios elaboran perfiles con la información de los más jóvenes con el objetivo de predecir sus comportamientos y así compartir dicha información con anunciantes[28]. Lo que la OCDE identifica como tecnología avanzada en el tratamiento de datos como segundo riesgo transversal, alumbra los peligros que el tratamiento de información por medio de Inteligencia Artificial, análisis predictivo de datos o tratamientos biométricos puede generar sobre los menores.

Estos potentes algoritmos predictivos, pueden resultar dañinos para el desarrollo de los más jóvenes, pues los mismos pueden inducir comportamientos y decisiones en seres que, por encontrarse en formación, pueden resultar más vulnerables. Sobre este punto, el desmesurado rastro que los menores generan en la red-pues navegan durante muchas horas compartiendo ingentes volúmenes de datos al fin de entretenerse- contribuye a facilitar a las compañías la predicción de su comportamiento futuro[29]. El

plugins. A su vez, recopilan las operaciones realizadas con el terminal, como poner una ventana en primer o segundo plano o los movimientos del ratón. Además, también recopilan las señales del dispositivo como, por ejemplo, señales de Bluetooth e información sobre balizas, torres de telefonía móvil y puntos de acceso a redes wifi cercanos. También compilan información sobre la red y conexiones empleadas como: el nombre del operador de telefonía móvil o proveedor de Internet, el idioma, la zona horaria, el número de teléfono móvil, la dirección IP, la velocidad de la conexión y, en algunos casos, información sobre otros dispositivos que se encuentran cerca o están en la red del dispositivo. Véase la Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse, apartado ¿Qué información recogemos?, (última consulta el 13 de marzo de 2025).

[27] Las *cookies* se definen como ficheros de texto alfanuméricos generados por las páginas web que se visitan y que se almacenan en el dispositivo del usuario con la finalidad de recuperar y leer los datos que esta recaba APARICIO SALOM, Javier., y SANFULGENCIO TOMÉ, Sergio., «El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos», *Revista Aranzadi Doctrinal,* 2014, núm. 11, p. 1.

[28] La publicidad comportamental, se define como la publicidad basada en la observación continuada del comportamiento de las personas internautas que busca analizar las características de dicho comportamiento en orden a desarrollar un perfil específico y proporcionar a los usuarios anuncios acomodados a los intereses inferidos de su conducta. Dictamen 2/2010 Grupo de Trabajo de protección de datos del Artículo 29 sobre publicidad comportamental en línea, de 22 de junio de 2010, GT 171, p. 5.

[29] En tal sentido, el Informe del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia, visibiliza que los perfiles de menores son económicamente muy valiosos, pues permiten construir relaciones desde una edad muy temprana. Este mismo informe señala que un 31,5% de los menores pasa más de 5 horas diarias conectado a Internet entre semana, ascendiendo dicha cifra a un 49,6% en fin de semana. MINISTERIO DE JUVENTUD Y DE LA INFANCIA. Informe del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. Disponible en: https://www.juventudeinfancia.gob.es/sites/default/files/infancia/comite_expertos/Informe-comite-

Comité Europeo de Protección de Datos (en adelante, CEPD), manifiesta que las técnicas de análisis de datos que se valen de *big data* potencian la manipulación de los usuarios, dado que estas técnicas de análisis de macrodatos buscan influenciar el comportamiento y las elecciones de las personas[30]. Convenimos con COTINO HUESO cuando sienta que con el *big data* se puede inducir a determinados comportamientos como, a quién votar, qué estudiar, dónde viajar o incluso qué comprar[31].

En otro orden de ideas, la práctica de estas técnicas de tratamiento de tecnología avanzada fomenta la falta de objetividad en el acceso a la información, limitando así el acceso a las fuentes de información a los usuarios. Lo cierto es que los algoritmos empleados en el análisis de datos masivos muestran a cada individuo la información que mejor se ajusta a sus intereses (deducidos del rastro que arroja en la red). En consecuencia, las plataformas, inducidas por las predicciones que sus algoritmos infieren, muestran a cada usuario informaciones diversas[32]. Por tanto, los menores de edad, tendentes a informarse principalmente *online*, crecen condicionados por un sistema que puede mostrarles información de forma sesgada resaltando algunas informaciones en detrimento de otras. Además, acertadamente dispone GARRIGA DOMÍNGUEZ, que la elaboración de perfiles puede determinar la información a la que las personas tendrán acceso, limitando su derecho a recibir información veraz aun cuando la CE exige esta condición en su art. 20.1.d)[33].

Paralelamente, tal y como señala la OCDE en su informe, el tratamiento de datos por medio de algoritmos predictivos o IA, aumentan el riesgo de discriminación y exclusión de los colectivos más vulnerables de personas de la oferta de determinados productos o de determinadas informaciones. Cierto es, que el análisis de datos masivos puede discriminar de manera directa o indirecta a determinado grupo de personas que cumplan criterios específicos, no mostrándoles ofertas de trabajo, ofertas de préstamos, etc. Consecuentemente, la libertad de elección sufre una considerable merma en este contexto, pues la inclusión de una persona en un concreto perfil al que se le atribuyen una serie de comportamientos futuros, genera la exclusión de esta de

---

personas-expertas-desarrollo-entorno-digital-seguro-juventud-infancia.pdf, p. 16 [Consulta: 11 de abril de 2025].

[30] *Guidelines 8/2020 of European Data Protection Board on the targeting of social media users*, Version 2.0, adopted on 2 september 2020, p. 5.

[31] COTINO HUESO, Lorenzo., «Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales», *Dilemata,* 2017, núm. 24, p. 141.

[32] Efectivamente, esta circunstancia se conoce como el filtro burbuja, véase a tal efecto PARISIER, E., *El filtro burbuja: cómo la web decide lo que leemos y lo que pensamos*, Madrid, Taurus, 2017, p. 18.

[33] GARRIGA DOMÍNGUEZ, Ana., «La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de protección de Datos de la Unión Europea», *Derechos y libertades,* 2018, núm. 38, Época II, p. 136.

serle mostrada el resto de información que, en cambio, sí se compartirá con personas que cumplan los criterios a tal efecto[34].

Con todo, estas técnicas de tratamiento de datos sobre información de personas que no alcanzan la mayoría de edad pueden conducir a las futuras generaciones a normalizar conductas como no acceder a información veraz y plural, crecer en un ambiente de manipulación en línea o no poseer una igualdad de oportunidades para forjar su futuro.

4.2. Los grandes peligros que representa el entorno digital para el desarrollo y bienestar del menor

La presencia de menores en el espacio *online* ha evidenciado que los riesgos no se ciernen sobre su privacidad exclusivamente. Por tanto, un análisis de los riesgos que acechan el desarrollo personal y tránsito hacia la madurez del menor deviene indispensable.

De vuelta a las categorías de riesgos que identifica la OCDE, esta reconoce que, a los clásicos riesgos de contenido como el contenido ilegal, el contenido inapropiado para la edad del menor y al contenido que predispone un ejemplo perjudicial para el menor, cabe añadir nuevos riesgos como la desinformación. El organismo dispone que el entorno digital ha auspiciado la proliferación de contenido de odio por medio de insultos u ofensas (potenciadas, además, por la sensación de anonimato y distancia con la víctima). Asimismo, también ha facilitado que el menor acceda a contenido tanto perjudicial como ilegal. Ejemplo de ello constituyen, por una parte, el acceso a contenido pornográfico, estafas o noticias desagradables; por otra parte, a contenido ilegal como mensajes que constituyen apología al terrorismo o al abuso sexual.

[34] Señala así el Grupo de Trabajo del Artículo 29, que esta técnica puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren. A causa de ello, se socava la libertad de las personas a la hora de elegir ciertos productos o determinados servicios. Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 6. En ese sentido, la plataforma *Netflix* no permite al usuario acceder al catálogo completo de sus contenidos, obligando a este a elegir entre las recomendaciones que la aplicación propone. No obstante, el usuario cree elige entre la serie o película que realmente desea visualizar. CASTILLO, C., «La oferta y la demanda del contenido audiovisual en la era de los datos masivos», 2018. Disponible en: https://chato.cl/papers/castillo_2018_oferta_disponiblidad_contenido_audiovisual-ES.pdf [Consulta: 11 de marzo de 2025].

Adicionalmente, la OCDE identifica novedosamente el riesgo que supone la desinformación para los menores como sujetos en formación. Ciertamente, el fenómeno conocido como *fake news* ha cobrado entidad en los últimos años en el espacio en línea, dificultando a los más jóvenes poder identificar aquellas noticias verdaderas de las que no revisten tal condición[35]. Más aún, la manipulación de imágenes y vídeo por medio de sistemas de IA, además de entorpecer y dificultar, más si cabe, las posibilidades de discernir aquellas que resulten verídicas, también se ha empleado entre menores con fines lesivos. Así, comienzan a abundar casos en los que menores manipulan las imágenes de otros menores al fin de crear la apariencia de que figuran desnudos en las mismas. El fenómeno *deepnude* consiste en emplear una fotografía de una persona real vestida que, mediante el procesamiento de la imagen por el sistema de IA, muestra la misma persona desnuda con un elevado efecto de realidad[36].

La segunda categoría de riesgos identificada por la OCDE viene de la mano de los peligros de conducta que este espacio puede generar. En tal sentido, conviene diferenciar aquellos comportamientos que pueden resultar constitutivos de delito de los que, si bien pueden resultar lesivos, no se tipifican penalmente. De menor a mayor gravedad, los menores pueden compartir información sobre terceras personas que puede perjudicar sus derechos fundamentales, tal y como ha quedado señalado en el apartado anterior. Antes bien, determinadas conductas que se desenvuelven en línea, pueden resultar constitutivas de delito, como, por ejemplo, comportamientos de odio motivados por la raza, etnia, religión, orientación sexual, identidad de género, etc., en los que el fin último se identifica con ofender a la víctima, insultarla o abusar de la misma.

En tal sentido, la Memoria de la Fiscalía General del Estado concerniente al ejercicio del año 2024, señala que el aumento de la brecha empática con la víctima, unido a un agravamiento de la violencia que se ejerce contra la misma, ocasiona que las redes sociales y canales de mensajería instantánea puedan convertirse en espacios idóneos para la comisión de delitos contra la intimidad, la libertad, la integridad moral, delitos

[35] Destacan casos como el de Pizzagate, escándalo que durante las elecciones estadounidenses del año 2016 acusó al director de campaña de Hilary Clinton de organizar actividades de trata sexual en una pizzería en las afueras de Washington D.C. La información, que no era verídica, además de extenderse a gran velocidad en la red, generó la credulidad de millones de personas.

[36] El primer caso de *deepnude* ocurrió en septiembre de 2023 en la localidad de Almendralejo, donde se difundieron imágenes de menores desnudas, a pesar de que nunca llegaron a tomarse dichas fotografías en tal condición. NAVARRO, I., "Imágenes con IA y *deepnudes*: ¿cómo actuar cuando se utilizan estos recursos?". Disponible en: https://diariolaley-laleynext-es. [Consulta: el 31 de marzo de 2025].

de odio, acoso, etc[37]. Además, respecto al último, hay que recordar que si estos comportamientos se reiteran en el tiempo pueden desembocar en *cyberbullying*[38].

En lo que a los riesgos de contacto o motivados por la interacción en el espacio virtual se refiere, debemos subrayar que el menor puede resultar víctima de diversos ataques. Puede observarse que, mientras que los peligros causados por la conducta identifican al menor como actor, en los riesgos de contacto, los jóvenes son las víctimas. En esta categoría, la OCDE destaca el *childgrooming,* donde el menor resulta víctima de un control y abuso por parte de una persona mayor de edad que se gana la confianza de este a través de medios en línea[39]. Por añadidura, los delitos de los que un menor puede resultar víctima van más allá del *childgrooming*. En verdad, tal y como señala la Fiscalía General, el menor puede ser víctima de la usurpación de su identidad en la red, pornovenganza o *sexting,* entre otros[40].

Como última categoría, la OCDE informa sobre los riesgos como consumidores de servicios digitales. Nuevamente, clasifica los riesgos en los ya identificados en el año 2011 y riesgos adicionales. Comenzando por los primeros, el organismo afirma que los menores reciben mensajes en línea de marketing sobre productos inapropiados, como, por ejemplo, bebidas alcohólicas o juegos de azar. Asimismo, reciben mensajes

[37] Véase la Memoria de la Fiscalía General del Estado correspondiente al ejercicio 2024. Disponible en: https://www.fiscal.es/memorias/memoria2024/FISCALIA_SITE/index.html, p. 1138. [Consulta: 13 de marzo de 2025]. Así, la Memoria señala que entre los delitos contra la intimidad, los menores pueden resultar autores de múltiples conductas delictivas como amenazas, coacciones, delitos contra el honor, contra la dignidad, revelación de secretos o todas las variantes de acoso. Por otra parte, entre los delitos que atentan contra la integridad física, destaca que ha aumentado la conducta conocida como *happy slappyng* entre los jóvenes, consistente en una modalidad de acoso en la que, por medio de teléfonos móviles, se procede a la grabación de agresiones y vejaciones para su posterior difusión a través de redes sociales. La finalidad de este comportamiento reside en publicitar dichas fechorías y avergonzar a la víctima. A tal efecto, recientemente se ha conocido el caso de acoso a un estudiante con discapacidad del instituto IES Torres Quevedo en Cantabria. Cuatro estudiantes han compartido en las redes un vídeo agrediendo a la víctima con parálisis cerebral. La Fiscalía de menores de Cantabria ha abierto diligencias de investigación a los cuatro menores agresores.

[38] Resultan alarmantes los datos publicados por la fundación COTEC sobre el acoso escolar y su incidencia en las redes sociales cuando señala que más del 35% de los jóvenes encuestados (menores de 12 a 16 años) manifestó haber sido víctima de conductas agresivas. De las mismas, el 80% afirmaban haberlas sufrido en redes sociales. Fundación COTEC, «Hilando voces: estudio del discurso de odio en la escuela». Disponible en: https://cotec.es/proyectos-cpt/estudio-del-discurso-de-odio-en-la-escuela/ [Consulta: 11 de marzo de 2025].

[39] Abundan pronunciamientos jurisprudenciales en los que se condena por el delito de Childgrooming. Sirva como ejemplo, la Sentencia del Tribunal de Justicia de Cataluña, 131/2023, de 2 de mayo de 2023.

[40] Memoria de la Fiscalía General del Estado correspondiente al ejercicio 2024. Disponible en: https://www.fiscal.es/memorias/memoria2024/FISCALIA_SITE/index.html, p. 1135. [Consulta: 13 de marzo de 2025].

comerciales que no se identifican como tales, lo cual genera un riesgo ante menores debido a su inexperiencia y credulidad.

Así, entre los riesgos más novedosos, señala que las estrategias de marketing han sufrido una gran evolución, tal y como se ha expuesto en el presente epígrafe a propósito de la elaboración de perfiles con fines de mercadotecnia directa. A causa de ello, los menores se han convertido en un blanco fácil dada su falta de madurez, ya que pueden no comprender la motivación presente tras este tipo de mercadotecnia, ni sus lesivas consecuencias. Tanto es así, que la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual (en adelante, Ley General de Comunicación Audiovisual), prohíbe en su art. 90 el tratamiento de datos de menores de edad con fines comerciales, mercadotecnia directa, elaboración de perfiles o publicidad personalizada basada en el comportamiento. Antes bien, estos tratamientos continúan practicándose en la actualidad por los prestadores de servicios digitales.

Adicionalmente, el organismo añade nuevos peligros derivados de este tipo de publicidad en línea. En primer lugar, los menores reciben publicidad de *influencers* que no en todo momento se identifica como tal a pesar de su obligatoriedad actualmente[41]. En segundo lugar, existen múltiples subscripciones trampa en juegos y redes sociales que, si bien al comienzo pueden resultar gratuitas, pasado determinado tiempo comienzan automáticamente a generar cargos. Por último, señala los riesgos de seguridad, tales como el acceso indiscriminado a datos del menor mediante el control de su comportamiento en línea (circunstancia relacionada con la elaboración de perfiles como hemos podido ver anteriormente).

Por último, tal y como señala la exposición de motivos del propio Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales mencionado anteriormente, resultan de obligada mención aquellos peligros para la salud y bienestar de los más jóvenes. En tal sentido, el entorno digital puede favorecer problemas de salud, tanto físicos como psicológicos, que se identifican con conductas sedentarias, desórdenes alimentarios (anorexia y bulimia), comportamientos autolesivos o incluso problemas de adicción y dependencia ante el indiscriminado y

[41] En efecto, el Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma, desarrolla los arts. 89 y 91 de la Ley 13/2022, de 7 de julio, General de la Comunicación Audiovisual donde se establece la obligación para estos usuarios (*influencer*), tanto de identificar el contenido publicitario en sus publicaciones, como no publicitar tabaco o medicamentos, asegurarse que la publicidad de alcohol respeta las franjas horarias establecidas a tal efecto y por supuesto, no promocionar juegos de azar a menores.

masivo empleo de herramientas digitales de ocio. A tal efecto, determinados espacios digitales se han diseñado creando patrones de adicción para los usuarios. Ello se debe a que, a mayor tiempo de empleo de sus servicios, el usuario resultará más rentable para el proveedor de servicios que precisa de dichos datos al fin de rentabilizar sus espacios aparentemente gratuitos[42]. En efecto, la industria tecnológica diseña los espacios de modo que influya intencionadamente en el comportamiento de los usuarios con el objetivo de maximizar el tiempo de uso o *engagement*[43].

En definitiva, sin desmerecer el avance que supone la integración de la tecnología en el día a día de las personas, podemos afirmar que el espacio en línea constituye un grave peligro para el desarrollo y la privacidad de los menores de edad. En consecuencia, queda en evidencia que han de reforzarse los controles y garantías en este ámbito, en especial, para el público más vulnerable como menores de edad. Concretamente, esta situación nos conduce a respaldar la implementación de medidas más eficaces y descartar aquellos sistemas de verificación meramente declarativos.

5. EL PROYECTO DE LEY ORGÁNICA PARA LA PROTECCIÓN DE LAS PERSONAS MENORES DE EDAD EN LOS ENTORNOS DIGITALES: ¿SOLUCIÓN DEFINITIVA EN LO REFERENTE A LA PRESTACIÓN DEL CONSENTIMIENTO AL TRATAMIENTO DE DATOS POR MENORES DE EDAD?

En junio de 2024, el Gobierno español anunciaba la aprobación del Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales cuyo fin principal se identifica con garantizar la protección de las personas menores de edad en el espacio en línea. Recientemente, en abril de 2025, el Consejo de Ministros ha remitido a las Cortes el Proyecto para su tramitación[44]. El texto propuesto se encuentra provisto de doce artículos divididos en cinco títulos, una

[42] A modo de ejemplo, el sistema *pull to refresh* implementado por primera vez en la red social Twitter y diseñado por la ingeniera Loren Brichter, consistente en deslizar la pantalla al fin de que la red social cargue nuevo contenido, posee idéntico patrón que las máquinas tragaperras de los casinos de Las Vegas con el objetivo de enganchar al usuario a la visualización del nuevo contenido emergente. Este sistema, finalmente terminó por implementarse por otras redes sociales como Instagram o TikTok. LLANEZA GONZÁLEZ, Paloma., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos, op, cit.,* p. 149.

[43] Expresamente señala el Informe que los modelos de negocio de los prestadores de servicios en el entorno digital se basan en lo que el Comité de expertos denomina "economía de la atención", lo que apareja el uso generalizado de algoritmos al fin de provocar adicción a la pantalla mediante el contenido. MINISTERIO DE JUVENTUD Y DE LA INFANCIA. Informe del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. Disponible en: https://www.juventudeinfancia.gob.es/sites/default/files/infancia/comite_expertos/Informe-comite-personas-expertas-desarrollo-entorno-digital-seguro-juventud-infancia.pdf, p. 12 y p. 95 [consulta: 11 de abril de 2025].

[44] Boletín Oficial de las Cortes Generales, XV Legislatura, Serie A, 52-1, de 11 de abril de 2025.

disposición derogatoria única y diez disposiciones finales que se proponen modificar diversas normativas pertenecientes a distintos ámbitos, como el de la salud, el comercio, la educación y el sector público.

Finalmente, tras varias décadas de inseguridad jurídica en lo referente a la protección jurídica del menor en el espacio digital, el legislador, consciente de los graves peligros a los que se enfrenta el desarrollo y la información personal de los más jóvenes, se propone garantizar la protección de las personas menores de edad en los entornos digitales. A pesar de que el Gobierno resalta que España se constituye como pionera en la tramitación de una norma como la recientemente citada, no podemos dejar de visibilizar que llega con manifiesto retraso a la luz del avance del escenario digital. La LOPDGDD, cuya entrada en vigor ocurre en 2018, ya contenía el compromiso del Gobierno en su art. 97.2 de que, en el plazo de un año desde la entrada en vigor de la norma, abordaría la consecución de un Plan de Acción como el que se propone en el texto. Sin embargo, han transcurrido seis años sin que todavía se haya materializado dicha promesa normativa.

Sin perjuicio de lo expuesto, debemos confesar que la aprobación de este Proyecto de Ley Orgánica se recibía con gran entusiasmo, pues entre el abanico de medidas que propone al fin de garantizar una mayor protección de los jóvenes en el espacio digital[45], se encuentra aumentar la edad legal para la prestación del consentimiento al tratamiento de datos. En efecto, la Disposición final quinta incrementa de la edad mínima para la prestación válida del consentimiento al tratamiento de datos por personas menores de edad. Concretamente, el texto aspira a aumentar la edad de 14 años establecida en el art. 7 de la LOPDGDD a los 16 años de edad. Recordemos a tal efecto, que el RGPD permite a los Estados miembro decantarse por una edad comprendida entre los 13 a 16 años, tal y como se ha expuesto en apartados anteriores. Antes bien, nos preguntamos si dicha medida, no acompañada de otras adicionales resulta suficiente al fin de devolver a los menores la seguridad jurídica de la que padecen cuando navegan en las distintas aplicaciones de la red.

Sin intención de desmerecer el esfuerzo del legislador al tratar de revertir la inseguridad jurídica con la que navegan los menores, en relación con el presente

[45] Cabe señalar, que el Anteproyecto se propone proteger los derechos de la infancia ante los contenidos digitales que puedan resultar dañinos para su desarrollo, proponiendo una suerte de medidas en diversos ámbitos como: la protección de los consumidores y usuarios, el ámbito educativo, el ámbito sanitario y en el sector público.

trabajo, deseamos centrarnos, tal y como se ha adelantado, en la medida que propone expresamente en

Así las cosas, el legislador, parece optar por incrementar la edad a partir de la cual el menor puede ejercitar autónomamente el derecho a la protección de datos personales a la preestablecida en otros ámbitos como, por ejemplo, la edad para emitir un consentimiento informado en el ámbito sanitario. En ese sentido, el art. 9 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica sienta la edad de 16 años para emitir un consentimiento informado válido. Cierto es, que también se prevén algunas excepciones en el mismo precepto, como, por ejemplo, que el menor demuestre madurez suficiente sin alcanzar la edad señalada para prestar consentimiento informado; o por el contrario, también determina algunos supuestos en los que, en todo caso, se precisará el consentimiento de los representantes legales[46].

A nuestro juicio, habida cuenta de la vertiginosa y peligrosa evolución de la tecnología en un breve lapso de tiempo y las limitadas capacidades de los más jóvenes para desenvolverse de manera responsable y consciente desde edades excesivamente tempranas en este entorno[47], valoramos positivamente el incremento de la edad propuesta por el Proyecto[48]. Antes bien, esta medida no se ha recibido como acertada

[46] Adviértase, asimismo, que el incremento de la edad propuesto por el Anteproyecto terminaría con la incongruencia existente entre la edad de 14 años establecida por la normativa sobre protección de datos personales para prestar consentimiento al tratamiento y el sistema instaurado en el ámbito sanitario para prestar consentimiento informado que, en ocasiones, terminaba por dificultar el acceso a la historia clínica de menores por parte de sus progenitores una vez cumplidos 14 años. Efectivamente, la historia clínica del menor queda amparada bajo la protección del derecho a la protección de datos personales, cuyo consentimiento el menor puede otorgar con 14 años. Por tanto, los progenitores se encontraban con obstáculos a la hora de acceder a dicha historia clínica cuando el propio menor puede decidir cómo ejercitar dicho derecho fundamental.

[47] Véase que, a la luz del estudio publicado por el Observatorio Nacional Tecnología y Sociedad, sobre El uso de las tecnologías por los menores en España, edición 2024. Disponible en: https://www.ontsi.es/sites/ontsi/files/2024-07/El%20uso%20de%20menores%20en%20Espa%C3%B1a%202023.pdf [consulta: 31 de marzo de 2025], el 23,3% de los niños de 10 años disponen de teléfono móvil. El porcentaje crece hasta el 45,7% a los 11, al 72,1% a los 12 y al 88,2% a los 13. La disponibilidad de móvil ya es casi universal al alcanzar los 14 (94,1%) y los 15 años (94,8%).

[48] Determinados autores se han mostrado contrarios a elevar la edad aduciendo, entre otros motivos, que los propios progenitores también acostumbran a publicar datos personales sobre sus descendientes (lo que se conoce como *sharenting*). Sin embargo, debemos denunciar que los riesgos a los que se enfrenta el menor cuando emplea redes sociales o servicios digitales en primera persona, no se limitan a exponer sus datos e imagen a terceras personas únicamente como ha quedado evidenciado en el apartado 4 de la presente investigación. BADILLO LÓPEZ, Mª Teresa., «Las medidas contenidas en el Anteproyecto de la Ley Orgánica para la protección de las personas menores de edad en los entornos

por determinado sector doctrinal, que denuncian que la medida propuesta continúa generando una divergencia entre la LOPDGDD y la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen que se decanta por el criterio de madurez positivizado en el CC, como hemos señalado en apartados anteriores[49]. Entendemos que ello puede ocurrir cuando el menor comparte imágenes en redes sociales, por ejemplo, pero debemos subrayar que los datos del menor sometidos a tratamiento no se limitan únicamente a imágenes en plena era digital. A riesgo de resultar reiterativos, recordemos, a su vez, que determinar la madurez del menor en el entorno digital se antoja imposible.

Estimamos que se deben superar dichas diferencias y abogar por un criterio eficaz que asegure que el titular de la información personal posee capacidad para ejercitar autónomamente dicho derecho fundamental. El cambio de escenario desde la Convención de los derechos del niño de 1989, en el que el mundo todavía se regía por patrones analógicos, quizás merezca abrir paso a nuevos sistemas para determinar la capacidad del menor, sobre todo en línea. Antes bien, convenimos que, aunque el criterio cronológico puede resultar más garantista en el entorno *online*, carece de efectividad práctica si no va de la mano del establecimiento definitivo de mecanismos de verificación de dicha edad[50]. Debemos lamentar, que el texto no otorga respuesta a este problema que, como hemos señalado previamente, continúa sin solución desde la entrada en vigor del RGPD.

Sorprendentemente, el Proyecto sí que impone a los proveedores de contenido audiovisual (también en línea) la necesidad de verificar la edad del menor a fin de garantizar que este no recibe contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores y que, en todo caso, impidan el acceso de estos a contenidos audiovisuales como la violencia gratuita y la pornografía, al resultar más nocivos.

Para ello, el Proyecto modifica el art. 89 de la Ley General de Comunicación Audiovisual citada anteriormente, obligando a estos proveedores a verificar la edad garantizando

digitales. En particular, la elevación de la edad mínima de los menores para ceder sus datos personales», *op, cit.*, pp. 20-21.

[49] Véase GRIMALT SERVERA, Pedro y ANDREU MARTÍNEZ, Mª Belén., «Anteproyecto de ley Orgánica para la protección de las personas menores de edad en los entornos digitales: aspectos civiles y de protección de datos», *LA LEY privacidad*, 2024, núm. 21, p. 3.

[50] Ciertamente, de nada sirve prohibir legalmente el uso de estas plataformas en caso de no alcanzar determinada edad, si ello no viene de la mano de fórmulas que eficazmente comprueben la misma. BRION BERDOTE, Estela., *Protección de datos personales, redes sociales y menores de edad. Nuevos retos normativos en tiempos de big data y de inteligencia artificial,* Madrid, Dykinson, 2025, p. 177.

unos niveles de seguridad y privacidad, particularmente en relación a la minimización de datos y limitación de la finalidad y protección de datos desde el diseño, como mínimo, a los de la cartera de identidad digital europea (EUDI Wallet) acorde al Reglamento 2024/1183, de 11 de abril de 2024 por el que se modifica el Reglamento 910/2014, en lo que respecta al establecimiento del marco europeo de identidad digital. No obstante, no comprendemos que el Proyecto no abogue por establecer idéntica necesidad de verificación de la edad al fin de garantizar que la prestación del consentimiento al tratamiento de datos ocurre a partir de los 16 años de edad, en su caso.

Entendemos que la propuesta decide poner coto al consumo de contenido más perjudicial para los menores, al igual que promovía la UE en el documento sobre *Empowering citizens and businesses in the digital transformation through a streamlined and ambitious use of the EUDI Wallet*[51]. Sin embargo, consideramos que convendría comenzar por controlar la misma prestación al consentimiento, pues de ello depende la participación de estos jóvenes en espacios que pueden resultar dañinos, no solamente por contenido perjudicial para estos como ha quedado de manifiesto. Más aún, no olvidemos que de la configuración de este mecanismo depende el ejercicio, con carácter válido, de un derecho fundamental como es el derecho a la protección de datos personales tan presente en el escenario digital.

Al hilo de lo expuesto, el Gobierno español trabaja en una aplicación que cumpla los estándares EUDI Wallet exigidos por la UE. La culminación del Proyecto que acomete el desarrollo de la aplicación denominada Cartera Digital Beta, se esperaba para finales de verano de 2024[52]. Resalta el ejecutivo español que, mediante el diseño de esta herramienta se responde a la necesidad de verificar la edad de los usuarios con vistas a garantizar que los menores no acceden a contenidos para adultos en el espacio digital. A su vez, anima a los actores no obligados por la norma a verificar la edad por medio de este sistema. Ahora bien, no creemos que la voluntariedad resulte fructífera en este contexto. Ello se debe a que, desde la misma entrada en vigor el RPGD, se impone la obligación de verificar la edad de los futuros internautas a la hora de prestar el consentimiento al tratamiento de datos personales de su titularidad; en cambio, al no

[51] Documento de la UE sobre *Empowering citizens and businesses in the digital transformation through a streamlined and ambitious use of the EUDI Wallet*. Disponible en: https://vlada.gov.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha-c--1_32.pdf [consulta: 21 de marzo de 2025], p.2.

[52] Véase así la Nota de prensa de la Moncloa, de 1 de julio de 2024, en la que se presenta la Cartera Digital Beta. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/transformacion-digital-y-funcion-publica/paginas/2024/010724-cartera-digital-beta.aspx [Consulta: 21 de marzo de 2025].

obligar reactivamente a estos proveedores de servicios a comprobar la edad, la medida ha terminado por no cumplirse a pesar de su preceptividad.

Así las cosas, la Cartera Digital Beta puede erigirse como un sistema de verificación válido a la par de robusto para la verificación de la edad, también a la hora de garantizar la prestación de un consentimiento válido al tratamiento de datos personales. Sobre las cualidades de este sistema que destacan positivamente, señalar que la verificación no depende del responsable del tratamiento, sino de una aplicación diseñada por el Gobierno español y, además, no identifica al usuario ni determina su edad exacta[53].Sin perjuicio de ello, también presenta sus inconvenientes, pues habrá de generalizarse su uso por la población, para lo que resultará de vital necesidad el lanzamiento de campañas informativas sobre esta e imponer su implantación por los espacios que requieran de un consentimiento al tratamiento de datos personales. Por otra parte, si bien la Cartera Digital Beta se esperaba para finales del verano de 2024, continuamos sin noticias sobre su implementación efectiva. Así, la UE concede un plazo que discurre hasta 2027 para que los Estados miembro desarrollen e instauren las respectivas Carteras Digitales que cumplan con las especificaciones del Reglamento EUDI Wallet mencionado previamente.

Definitivamente, podemos afirmar que la verificación de la edad del menor para la prestación del consentimiento al tratamiento de datos personales en línea continua y parece que continuará sin solución en un futuro cercano. Denunciamos dicha demora, pues los menores llevan décadas accediendo a estos espacios y prestando consentimientos carentes de validez a pesar de que deba verificarse su edad desde el año 2018 con carácter unánime en el espacio europeo.

Entretanto, hay que recordar que el Proyecto obliga a los proveedores afectados por la medida a instaurar sistemas de verificación que garanticen unos niveles de seguridad y privacidad, particularmente en torno a la minimización de datos y limitación de la finalidad y protección de datos desde el diseño, “como mínimo”, a los de la cartera de identidad digital europea (EUDI Wallet). Entendemos que la expresión “como mínimo” no cierra la puerta a otros mecanismos de verificación que resulten respetuosos con el principio de minimización de datos, la limitación de la finalidad y la protección de datos desde el diseño.

[53] Para más información, consúltese el Informe del Ministerio para la Transformación digital y de la Función pública en el que se presenta la Aplicación. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/transformacion-digital-y-funcion-publica/Documents/2024/010724-cartera-digital-beta.pdf [Consulta: 29 de mayo de 2025].

Con relación a la idoneidad de otros sistemas alternativos a la Cartera Digital Europea, los mayores inconvenientes aducidos por el legislador, reiteradamente, se han presentado con el principio de minimización. Esto es, varios de los sistemas se han rechazado por el propio legislador al solicitar más información personal a efectos de verificar la edad. Sin embargo, este principio regulado en el art. 5.1.c) RGPD, no supone que en todo caso deban tratarse pocos datos personales, sino que ello vendrá determinado por la finalidad de tratamiento alegada al amparo del Considerando 39 del RGPD. A este respecto, resultan esclarecedoras las palabras de TRONCOSO REIGADA cuando sienta que, los parámetros tradicionales del principio de proporcionalidad pueden señalar en qué contextos puede considerarse que la recopilación y tratamiento resultan excesivos. De este modo, habrán de ponderarse los bienes y derechos constitucionales en conflicto, con el propósito de determinar si la injerencia en el derecho a la protección de datos personales se estima equilibrada por derivarse más beneficios para el interés general derivados de su práctica, que perjuicios para el mentado derecho fundamental[54].

A nuestro parecer, las afirmaciones expuestas nos conducen a no rechazar sistemas de verificación que precisen un volumen considerable de datos personales al fin de verificar la edad. Ello se debe a que, en el presente contexto, los datos se recaban y tratan, por una parte, con la finalidad de garantizar el ejercicio efectivo y válido de un derecho fundamental por parte del colectivo de menores; por otra parte, para proteger a estos de un entorno hostil para con su privacidad y desarrollo personal. Así las cosas, evidenciados los riesgos, el interés superior del menor y la protección de sus derechos debe imponerse en este contexto a la hora de aceptar la validez de diversos mecanismos de verificación de la edad.

En consecuencia, creemos que no deberían descartarse sistemas de IA con el objetivo señalado. La IA, a pesar de someter a tratamiento volúmenes considerables de información personal, puede erigirse como una herramienta válida para lograr dicho cometido. Véase que, la combinación del análisis de datos como la voz, la imagen y el modo de escribir, puede determinar con un porcentaje elevado de exactitud la edad de un potencial usuario[55]. Ciertamente, el estado de la técnica actual permite el diseño de

[54] TRONCOSO REIGADA, Antonio., «Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGG)», en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021*,* pp. 873-886.

[55] SHOPON, M.; TUMPA, S.N.; BATHIA, Y.; PAVAN KUMAR, K.N.; GAVRILOVA, M.L., «Biometric Systems De-Identification: Current Advancements and Future Directions», *Journal of Cybersecurity and Privacy,* 2021, núm. 1, pp. 470-495.

diversos mecanismos de verificación que pueden cumplir con las premisas expuestas por la normativa europea en lo relativo al tratamiento de datos.

Somos conscientes de que estos mecanismos, han suscitado el recelo de la Agencia Española de Protección de Datos (en adelante, AEPD) en lo que a la verificación de la edad para impedir el acceso a contenido inadecuado se refiere[56]. Ello se debe a que, la AEPD sostiene que han de evitarse mecanismos que revelen la condición de persona menor de edad de los potenciales usuarios. En cualquier caso, cuando se trata de consentir el tratamiento a un proveedor de una red social, por ejemplo, dicha condición quedará revelada rápidamente a través del tratamiento de la información personal por medio de algoritmos cuando el menor comience a emplear el servicio[57]. Por tal razón, el Principio 5 expuesto por el organismo consistente en que en ningún caso el sistema de verificación de edad permita inferir la edad concreta, decae por completo mediante el empleo de este servicio a posteriori.

Adicionalmente, ha suscitado preocupación en la AEPD que estos sistemas de verificación se empleen con fines diversos a comprobar la edad, especialmente para facilitar a los proveedores de servicios la identificación, la localización, el rastreo o la elaboración de perfiles. Lamentablemente, si bien se han descartado sistemas de verificación por dicho motivo, tal y como ha quedado señalado, estos tratamientos ocurrirán posteriormente durante el empleo del servicio[58] (salvo que se sancione a quienes incumplan el art. 90 de la ley de Contenido Audiovisual que prohíbe su práctica cuando el usuario es menor). Tal y como apunta el CEPD, el proceso de verificación de la edad no deberá permitir el rastreo y la elaboración de perfiles con fines comerciales[59]. Adviértase, que el CEPD se muestra más abierto que la AEPD a la hora de aceptar diversos sistemas de verificación siempre que respeten las premisas expuestas. Como no podía ser de otro modo, en este contexto, los datos han de tratarse exclusivamente con la finalidad de cumplimiento de una obligación legal (art. 6. 1. c RGPD) que impone el art. 8 RGPD. Más aún, los organismos de control deberían asegurarse de que los datos se recaban y someten a tratamiento con dicho fin exclusivamente.

[56] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Decálogo de principios. Verificación de la edad y protección de personas menores de edad ante contenidos inadecuados. Disponible en: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf [Consulta: 14 de abril de 2025]

[57] Desde luego, un gran número de espacios digitales elaboran perfiles con la información personal de sus usuarios, lo que permite desvelar con facilidad la condición de menor de edad de estos.

[58] En efecto, los proveedores de servicios digitales elaboran perfiles con fines de mercadotecnia directa por medio de sus potentes algoritmos sin importar la edad de los usuarios.

[59] CEPD. *Statement 1/2025, on Age Assurance*, adopted on 11 February 2025, p. 4.

Por todo ello, no podemos comprender que mientras la actitud en lo referente a la elaboración de perfiles con información personal de menores fines comerciales puede tildarse de permisiva, dicha actitud resulte restrictiva cuando su cometido se identifique con el ejercicio con carácter válido de un derecho fundamental.

Sea como fuere, se debe garantizar que aquellos menores que no alcancen la edad preceptiva para prestar el consentimiento no consigan acceder a espacios que no verifiquen su edad al amparo de su interés superior. Ante la manifiesta duda sobre la edad del interesado, se debe optar por denegar cautelarmente el acceso a dicho espacio; sin embargo, ocurre lo contrario. Nos mostramos convencidos, que ello se debe a que los perfiles de los menores son verdaderamente valiosos económicamente por dos razones principales. En primer lugar, a más transacciones, mayor será el volumen de datos recabado y más ganancias obtendrá la *big tech* o mayor resultará su calidad, eficiencia o productividad. En segundo lugar, permiten cimentar relaciones de consumo desde edades tempranas y con un nivel de precisión elevado al discurrir estos jóvenes muchas horas navegando en estos espacios diseñados adictivamente.

Defendemos así, la superación de sistemas meramente declarativos e instamos al legislador a imponer y abogar por el cumplimiento del art. 8.2 RGPD que obliga a la verificación de la edad de las personas interesadas a la hora de prestar el consentimiento. Asimismo, sería deseable que el legislador facilitara un listado de diversos mecanismos de verificación aceptables desde el punto de vista del tratamiento de datos (principio de minimización, limitación de la finalidad y protección desde el diseño)[60].

En plena era de la Sociedad de la Información, no se puede permitir que los menores de edad continúen prestando consentimientos faltos de validez en el contexto en línea. El estado actual de la tecnología, hace años que permite configurar sistemas que verifiquen dicho extremo, por lo que urge que el legislador haga cumplir el art. 8.2 RGPD que impone la verificación de la validez del consentimiento otorgado. Por ende, el Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, se erigía como una buena oportunidad para realizar extensiva la obligación de verificar la edad para evitar el consumo de contenido nocivo para el

[60] Nótese que, a pesar de que EEUU posea una normativa más permisiva sobre el tratamiento de datos personales que la UE, la Children's Online Privacy Protection Act of 1998 (COPPA), 15 USC 6501-6505 issued in November 1999 by the Federal Trade Commission (FTC) and became effective in April 2000. Véase Section 312.5, *Parental Consent,* acoge en su articulado un listado de sistemas de verificación aceptables desde el punto de vista de la normativa sobre privacidad.

menor a la configuración e implantación de sistemas de verificación de la edad para la prestación al consentimiento al tratamiento. Solo así se puede asegurar la efectividad de la medida consistente en aumentar la edad para otorgar consentimiento válido de 14 a 16 años.

Cabe decir, que la propia AEPD manifestaba que el sistema de verificación diseñado para evitar que los menores accedan a contenido inadecuado, no debe articularse en todo caso y por defecto, sino únicamente cuando se desea acceder a espacios específicos con limitación de la edad, como por ejemplo, cuando el menor desea acceder a contenido inadecuado (se exige la edad mínima de 18 años) o cuando, el servicio impone una determinada edad de empleo, como es el caso de las redes sociales, en las que el menor ha de acreditar 14 años[61].

Empero, como ha quedado de manifiesto, las últimas novedades normativas lejos de otorgar una respuesta definitiva a esta realidad, solo se centran en aportar soluciones que parecen decantarse por atajar el consumo de contenido nocivo *online.* Todo ello, a pesar de que la AEPD, en su Nota técnica sobre la "Descripción de las pruebas de concepto sobre sistemas de verificación de edad y protección de personas menores ante contenidos inadecuados" apuntara asimismo que, la protección del interés superior del menor es más amplia que impedir el acceso a contenidos inadecuados. Concretamente, apostilla el organismo que, la protección de este interés abarca la protección de todos sus derechos fundamentales y, particularmente, todos los aspectos que puedan afectar a la seguridad, salud y desarrollo e intimidad de los menores[62].

6. CONCLUSIONES

A pesar de valorar positivamente que el legislador, aunque con retraso, haya acometido la tarea de devolver seguridad jurídica a los menores de edad en el espacio digital y velar por su interés superior, no podemos evitar señalar que una de las principales medidas como es el incremento de la edad de los 14 años a los 16 para prestar un consentimiento válido al tratamiento continuará adoleciendo de efectividad. En efecto, la falta de exigencia de la verificación de edad a la hora de otorgar

[61] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Decálogo de principios. Verificación de la edad y protección de personas menores de edad ante contenidos inadecuados. Disponible en: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf [Consulta: 14 de abril de 2025], p. 10.

[62] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Descripción de las pruebas de concepto sobre sistemas de verificación de edad y protección de personas menores ante contenidos inadecuados. Disponible en: https://www.aepd.es/guias/nota-pruebas-concepto-verificacion-edad.pdf [Consulta: 19 de mayo de 2025].

consentimiento al tratamiento de datos personales convierte el aumento en ineficaz por sí mismo.

Comprendemos que la complejidad que apareja lograr un consenso sobre el sistema de verificación idóneo, especialmente desde el punto de vista de la protección de los datos, contribuye en gran medida a la falta de decisiones relacionadas con la cuestión. No obstante, en plena era digital en la que los tratamientos de datos han alcanzado un nivel de sofisticación impensable años atrás, no se puede continuar sin conceder una solución a esta carencia que abre la puerta a un entorno extremadamente peligroso a los más jóvenes.

Así las cosas, impera la necesidad de instaurar mecanismos de verificación para evitar la presencia de los menores de edad en espacios cuyo diseño atenta contra su interés superior. Para ello, exigimos al legislador que, al igual que se ha decantado por imponer sistemas de verificación que cumplan con los requisitos de la cartera digital EUDI Wallet para evitar el consumo de contenido inadecuado por los menores, manifieste idéntica obligación para el ejercicio del derecho fundamental a la protección de datos personales por los menores. En ese sentido, además de garantizar que los menores no participen en espacios nocivos para su privacidad y desarrollo personal, también se logra que no accedan a contenido inadecuado en estas plataformas digitales.

A su vez, recordemos que también cuentan con el beneplácito expreso del legislador los sistemas que cumplan con los requisitos del sistema EUDI Wallet sin necesidad de que sea este mismo el que se implemente por los proveedores de servicios digitales. Ahora bien, sobre esta cuestión creemos que el legislador debería ser explícito y enunciar aquellos sistemas válidos, pues desde el punto de vista técnico, hace años que resulta posible verificar la edad del menor con altas probabilidades de éxito. Exigimos al legislador, que valore los sistemas que ha descartado reiteradamente por colisionar, a su juicio, con el principio de minimización.

Por último, lamentamos que el legislador sí haya advertido correctamente que la edad de 14 años es insuficiente dada la falta de madurez y conciencia del menor para la concesión de un consentimiento válido, pero no haya dotado la medida de las garantías precisas para su efectividad. Se desaprovecha así una oportunidad legislativa que el devenir de los años ha demostrado que no ocurre con asiduidad, pues las medidas y compromisos del legislador en torno a la materia, hemos podido comprobar que se demoran durante más de un lustro y en muchas ocasiones una década. Prueba de ello constituye que el RGPD tardara más de una década en regular el consentimiento al

tratamiento por menores de edad o, por otra parte, que el Gobierno español tardara seis años en acometer un plan de Acción cuyo compromiso se señalaba en un año.

BIBLIOGRAFÍA

APARICIO SALOM, Javier, y SANFULGENCIO TOMÉ, Sergio, «El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos», *Revista Aranzadi Doctrinal,* 2014, núm. 11, pp. 1-17.

BADILLO LÓPEZ, Mª Teresa, «Las medidas contenidas en el Anteproyecto de la Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. En particular, la elevación de la edad mínima de los menores para ceder sus datos personales», *Revista Estudios Jurídicos. Segunda Época,* 2025, núm. 25, pp. 1-27.

BARRIUSO RUIZ, Carlos, «Las Redes sociales y la protección de datos hoy», *Anuario de la Facultad de Derecho-Universidad de Alcalá II,* 2009, núm. 2, pp. 301-338.

BATUECAS CALETRÍO, Alfredo, «El control de los padres sobre el uso que sus hijos hacen de las redes sociales», en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información,* Granada, Comares, 2015, pp. 105-135.

BRION BERDOTE, Estela, *Protección de datos personales, redes sociales y menores de edad. Nuevos retos normativos en tiempos de big data y de inteligencia artificial,* Madrid, Dykinson, 2025.

CASTILLA BAREA, Margarita, «La protección de los menores el internet (Comentario al artículo 84 LOPDGDD)», en TRONCOSO REIGADA, A., (director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 3945-3978.

COTINO HUESO, Lorenzo, «Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales», *Dilemata,* 2017, núm. 24, pp.131-150.

DAVARA FERNÁNDEZ DE MARCOS, Laura, «Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos Breve referencia al fenómeno Pokémon Go», *XX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos,* Madrid, 2007.

DIEZ PICAZO, Luis, Y GULLÓN, Antonio, *Sistema de Derecho civil,* Volumen IV, Tomo I, Madrid, Tecnos, 2012.

GARRIGA DOMÍNGUEZ, Ana, «La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de protección de Datos de la Unión Europea», *Derechos y libertades,* 2018, núm. 38, Época II, pp. 107-139.

GIL MEMBRADO, Cristina, «Límites a la autonomía de la voluntad en la disposición de la imagen del menor a través de las Redes Sociales», *La Ley Derecho de Familia,* 2017, núm. 13, pp. 1-24.

GÓMEZ-JUÁREZ SIDERA, Isidro, «Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la Legislación Española», *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2006, núm. 11, 2ª parte, p. 1-19.

GRIMALT SELVERA, Pedro, «Los menores e internet: capacidad versus protección de la vida privada» en CUENA CASAS, M., ANGUITA VILLANUEVA, J.A., ORTEGA DOMÉNECH, J., (Coordinadores), *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa*, Madrid, Dykinson, 2013, pp. 179-194.

GRIMALT SERVERA, Pedro, y ANDREU MARTÍNEZ, Mª Belén, «Anteproyecto de ley Orgánica para la protección de las personas menores de edad en los entornos digitales: aspectos civiles y de protección de datos», *LA LEY privacidad*, 2024, núm. 21, pp. 1-7.

HERRÁN ORTÍZ, Ana Isabel, «Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?», *Revista R.V.A.P.* 2010, núm. 87-88, pp. 521-566.

LACRUZ BERDEJO, Jose Luis, *Elementos de Derecho civil I. Parte general,* Vol. II, Madrid, Dykinson, 2010.

LASARTE ÁLVAREZ, Carlos, *Compendio de derecho de la persona y del patrimonio,* Madrid, Dykinson, 2014.

LLANEZA GONZÁLEZ, Paloma, *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*, Barcelona, 2019.

MITLLANS PERELLÓ, Esther, «Impacto de las redes sociales en el derecho a la protección de datos personales», *Anuario de la Facultad de Derecho-Universidad de Alcalá II*, 2009, núm. 2, p. 113.

MORILLAS FERNÁNDEZ, Marta, «Menores vulnerables y redes sociales: Nuevos retos jurídicos en la protección ante el uso inadecuado. Edad, educación y controles por defecto», *Revista Internacional de Doctrina y Jurisprudencia,* 2024, núm. 32, pp. 47-70.

RAMOS CHAPARRO, Enrique, «Niños y jóvenes en el derecho civil», *Derecho Privado y Constitución*, 1995, núm. 7, pp. 167-229.

SHOPON, M.; TUMPA, S.N.; BATHIA, Y.; PAVAN KUMAR, K.N.; GAVRILOVA, M.L., «Biometric Systems De-Identification: Current Advancements and Future Directions», *Journal of Cybersecurity and Privacy,* 2021, núm. 1, pp. 470-495.

TRONCOSO REIGADA, Antonio, «Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGG)», en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021*.,* pp. 848-907.

VÁZQUEZ DE CASTRO, Eduardo, «Protección de datos personales, redes sociales y menores», *Revista Aranzadi de Derecho y nuevas Tecnologías*, 2012, núm. 29/2012 parte Doctrina, pp. 1-26.

Fecha de recepción: 03.06.2025

Fecha de aceptación: 24.09.2025