1.2. Derecho de familia

El necesario papel de los progenitores y centros docentes como entorno seguros ante el reto de las nuevas tecnologías (IA): análisis de la normativa europea y nacional actual y de futuro.

The necessary role of parents and schools as a safe environment in the face of the challenge of new technologies (ai): analysis of current and future european and national regulations.

por

ANA ISABEL BERROCAL LANZAROT

Profesora Contratada Doctora (acreditada a profesora Titular) de Derecho Civil. Universidad Complutense de Madrid.

RESUMEN. El presente estudio se va a centrar en el importante papel de los progenitores y centros docentes en la protección de los menores de edad y adolescentes ante los retos del uso de las nuevas tecnologías, en especial los sistemas de inteligencia artificial. A tal efecto analizaremos la normativa europea existente (Reglamento General de Protección de Datos, Reglamento de Servicios Digitales y Reglamento de Inteligencia Artificial, entre otros) y la normativa nacional presente y futura.

ABSTRACT. This study will focus on the important role of parents and schools in protecting minors and adolescents from the challenges posed by the use of new technologies, especially artificial intelligence systems. To this end, we will analyze existing European regulations (the General Data Protection Regulation, the Digital Services Regulation, and the Artificial Intelligence Regulation, among others) and current and future national regulations.

PALABRAS CLAVES: Inteligencia artificial, nuevas tecnologías, menores de edad, adolescentes, violencia digital, redes sociales, plataformas en línea, datos personales, daños, ilícitos penales e ilícitos civiles.

KEYWORDS: Artificial intelligence, new technologies, minors, adolescents, digital violence, social networks, online platforms, personal data, damages, criminal offenses, and civil offenses.

SUMARIO: I. INTRODUCCIÓN.—II. REGLAMENTO DE SERVICIOS DIGITALES. EN ESPECIAL, LA PROTECCIÓN DE LOS MENORES Y ADOLESCENTES ANTE LOS RIESGOS DE LAS REDES SOCIALES, PLATAFORMAS EN LÍNEA, MOTORES DE BUSQUEDA.—III. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: DERECHOS Y CONSENTIMIENTO DE LOS MENORES Y ADOLESCENTES. 3.1. En torno al contenido del Reglamento General de Protección de Datos. 3.2. Derechos del interesado (titular de los datos personales) en el Reglamento de Protección de Datos (los conocidos como derechos ARCO). 3.3. El consentimiento de menores de edad en el Reglamento General de Protección de datos y la Ley Orgánica 3/2018, de protección de datos y garantía de derechos digitales. 3.4. El interés superior del menor, las redes sociales y plataformas digitales en línea de gran tamaño y motores de búsqueda.—IV. EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL Y LA PROTECCIÓN DE MENORES Y ADOLESCENTES.—V. EL PROYECTO DE LEY 121/000052 DE PROTECCIÓN DE LOS MENORES EN ENTORNOS DIGITALES.—VI. LAS AUTORIDADES DE CONTROL: EL PAPEL DE LA OFICINA EUROPEA DE INTELIGENCIA ARTIFICIAL Y LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS EN LA SEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD DE MENORES DE EDAD Y ADOLESCENTES.—VII. LA RESPONSABILIDAD CIVIL DE LOS PROGENITORES, TUTORES Y CENTROS DOCENTES.—VIII. BIBLIOGRAFÍA.—IX. ÍNDICE DE RESOLUCIONES.

I. INTRODUCCIÓN

Con la reforma operada por la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, además de datar de un régimen jurídico propio a las personas con discapacidad, se reestructura el ámbito de protección de los menores en el sentido que ya no guarda relación la patria potestad con el hijo mayor de edad discapacitado, al suprimirse la patria potestad prorrogada y rehabilitada, y únicamente se reserva la tutela para los menores de edad no sometidos a patria potestad. En todo lo demás, la configuración de la patria potestad se mantiene tal como se reformó por Ley 11/ 1981, de 13 de mayo. La patria potestad responde a la existencia de un vínculo de filiación, ya sea por naturaleza o por adopción y corresponde a ambos progenitores. Así resulta del artículo 154.1 del Código Civil en cuanto establece *"los hijos e hijas están bajo la potestad de los progenitores"*. Como responsabilidad parental se ejerce siempre en interés de los hijos e hijos de acuerdo con su personalidad y conforme el artículo 154.3 del citado cuerpo legal tienen como deberes y facultades *"velar por los hijos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral"*; y, son los representantes legales de sus hijos menores de edad no emancipados y administradores de sus bienes. No obstante, se exceptúa de la representación legal de los titulares de la patria potestad en relación con determinados actos que, o bien pue-

den ser realizados por el hijo (artículo 162.1 del Código Civil —actos relativos a derechos de personalidad del hijo, de acuerdo con su madurez puede realizar por sí mismo—), o bien conllevan la intervención de un tercero que excluye los padres como representantes del hijo en un acto o negocio jurídico en particular (artículo 162.2 y 3 del Código Civil). De todas formas, los menores de edad no emancipados podrán celebrar aquellos contratos que las leyes les permitan realizar por sí mismos o con asistencia de sus representantes y los relativos a bienes y servicios de la vida corriente propios de su edad de conformidad con los usos sociales (artículo 1263 del Código Civil). Ahora bien, los padres son los responsables de los daños causados por los hijos que se encuentran bajo su guarda; más en concreto en la culpa *in vigilando* o *in educando* (artículo 1903.2 del Código Civil). Estamos ante una responsabilidad subjetiva o por culpa que, alcanza a los ilícitos civiles e ilícitos penales que cometan sus hijos menores de edad no emancipados tanto en el mundo físico como digital o virtual, salvo que pruebe diligencia debida en su actuación paterna o materna. Si tales ilícitos son cometidos durante el tiempo que el hijo menor de edad está en el centro docente de enseñanza no superior en el curso de actividad escolares, extraescolares o complementarias tiene lugar una delegación de guarda y de responsabilidad. De forma que, los centros docentes responden de los daños casado por sus alumnos en el deber de vigilancia que le corresponde (artículo 1903.V del Código Civil). Se habla también de responsabilidad subjetiva o por culpa (culpa *in vigilando* o culpa *in eligiendo*), salvo prueba de su diligencia. Igualmente, el daño puede ser ocasionado en el mundo físico como en el digital. Ambos deben convertirse en entornos seguros y garantes de la privacidad, intimidad y seguridad de los menores de edad no emancipados.

Pues bien, sobre tales bases, procede en este estudio centrarnos en la participación de los menores de edad no emancipados en el mundo digital. Estamos ante los llamados "nativos digitales" que utilizan las tecnologías de la información y la comunicación (Tics), cuentan con suficientes conocimientos para poder "navegar por las redes", a la par que sus derechos pueden verse afectados, infringidos y carentes de las suficientes garantías para asegurarlos y protegerlos. A tal expresión debemos añadir el uso responsable que resulta efectivo, si se acompaña de política públicas, normas y sanciones para quienes incumplan y, estableciendo unos límites en la oferta de servicios digitales.

Ciertamente, el acceso a internet y el uso de las aplicaciones móviles se ha convertido en parte esencial de la vida de las personas, especialmente de los menores y adolescentes. Los beneficios de este mundo digital son innegables, les permiten acceso a información, conocimiento, representa una herramienta esencial en el modelo educativo, ofrece oportunidades sociales o creativas; fomenta su derechos a la libertad de expresión, la libertad de pensamiento y la conciencia y la interactuación con su entono social más próximo, con capacidad para mejorar su participación social favoreciendo con ello su desarrollo personal. El uso de las redes sociales y de juegos interactivos en plataformas les permite relacionarse con sus amigos, compartir experiencias, operar entre iguales, e influye en su desarrollo emocional, todo ello en un entorno digital paralelo al presencial[1]. Ahora bien, todo esto tiene consecuencias para su identidad personal, social y también en lo que representa su identidad digital o huella digital; lo que puede representar cierto riesgo en un futuro; de ahí la necesidad de recurrir al derecho al olvido o supre-

sión de datos; pues, no olvidemos que, las redes sociales y las plataformas digitales muestran nuestro comportamiento, forma de ser que, quizá en un tiempo temprano donde la conciencia no está en un proceso maduro y, lo que parece atractivo y divertido, al alcanzar la edad adulta nos damos cuenta de los riesgos que tales comportamientos tienen para nuestra privacidad y desarrollo personal, social y laboral. Constituye una realidad que, los beneficios de los procesos de digitalización y democratización del acceso a los entornos digitales deben ir parejos con las medidas necesarias de protección a la infancia y a la juventud en el ciberespacio, poniendo en el centro sus derechos e interés superior. Es importante destacar la creciente demanda social que durante los últimos años ha tenido lugar exigiendo un entorno digital seguro, inclusivo y educativo para los menores y adolescentes, que garantice su bienestar y desarrollo en la era digital.

No obstante, muchos de estos riesgos y los peligros ya existen en el mundo real (físico), pero han encontrado campo de operatividad también en el mundo digital con los riesgos que comporta y las dificultades de evitarlos. Así impedir la explotación de adicciones, el ciberacoso, la exposición a contenidos inadecuados o inapropiados, e incluso, las diferencias sociales, conductas delictuales o el consentimiento para ciertas operaciones que excede de lo que sería seguro para el menor, a la vez impedir que sean manipulados, dirigidos o convertidos en clientes permanentes y, con ello su monetización a través de su "datiflicación", resulta ser una obligación de los poderes públicos que, debe tener reflejo en un marco normativo adecuado.

Resulta imprescindible, actuar atendiendo al principio del interés superior del menor en cualquier ámbito de actuación sea en el mundo físico o el virtual; además, la actuación de los proveedores de servicio ha de ser no reactiva sino proactiva; y. asimismo, resuelta necesario que internet sea seguro por defecto desde el diseño y siguiendo el principio de minimización en el tratamiento de los datos personales de los menores y adolescentes.

A tal fin, la Observancia General número 25 del Comité de los Derechos del Niño de Naciones Unidas adoptada en marzo de 2021, se centra en los derechos de los niños en relación con el entorno digital, ofreciendo directrices a los Estados parte para implementar los derechos de los menores y adolescentes en el entorno digital.

Esta Observación General fundamenta estos derechos en cuatro principios generales: 1. La no discriminación de forma que ellos Estados parte se aseguren que todos los niños tengan el acceso equitativo y efectivo al entorno digital de manera beneficiosa para ellos; 2. El interés superior del niño, de tal forma que los Estados deban recabar la participación de los órganos nacionales y locales encargados de que se hagan efectivos los derechos de los niños, incluidos su derecho a buscar, recibir y difundir información, a obtener protección contra todo daño y a que sus opiniones se tengan debidamente en cuenta y garantizar el superior interés del menor; 3. El derecho a la vida y a la supervivencia y al desarrollo, debiendo adoptar los Estados parte todas las medidas apropiadas para proteger a los niños frente a todo lo que constituya una amenaza para su derecho a la vida, la supervivencia y el desarrollo; y 4. El respeto a las opiniones del niño (derecho a ser oído y escuchado).

En este contexto, los menores y adolescentes participan en entorno digital donde el acceso y la conexión y la oferta son permanentes e ilimitadas. Desde temprana edad como señala ADRIANA RODRÍGUEZ "están expuestos a una variedad cada vez mayor de tecnología, teléfonos inteligentes, tabletas, ordenadores y diversidad de plataformas en línea, redes sociales, videojuegos y servicios de *streaming*"[2]. Aunque pueden representar nuevas formas de aprendizaje y modelos educativos y sociales, también traen consigo importantes desafíos, riesgos y peligros en la protección de la infancia. Precisamente, la *American Academy of Pediatric* —AAP pone de manifiesto que, el exceso de horas de pantalla se ha vinculado con trastornos de conducta, retraso en el desarrollo y trastornos del lenguaje, dificultades de aprendizaje, trastornos por déficit de atención e hiperactividad (TEDA) y trastornos del espectro autista (TEA). Por su parte, según datos de UNICEF España, el 15% de los adolescentes españoles presentan síntomas de depresión grave y la tasa de comportamientos suicidas se sitúa en un 10%. Asimismo, destaca que un 16% de adolescentes ha sufrido acoso o ciberacoso; y según las investigaciones de *Save de Children* España 7 de cada 10 menores ha sufrido violencia en entornos digitales, siendo las niñas el colectivo más afectado. En este contexto, el Informe TechDispatch sobre neurodatos 2024 del Supervisor Europeo de Protección de Datos y la Agencia Española de Protección de Datos señalan la necesidad de asegurar el tratamiento de neurodatos sean proporcionales y minimizados y que se recojan solo aquellos datos necesarios para cumplir con los fines específicos manifestados. Se destaca, también, los riesgos asociados con la exactitud y fiabilidad de los datos teniendo en cuenta que operamos sobre el cerebro humano, su plasticidad y las numerosas variaciones que presenta el desarrollo neuronal en función de la edad. De ahí que, se hable de neuderechos. En las medidas de consenso para un Pacto de Estado ante la nueva legislatura y la presidencia de España en la UE "Protegiendo a la infancia y la adolescencia en el entorno digital" se establece en la página 33 y 34 los siguientes neuderechos: "derecho a la privacidad mental (datos cerebrales de las personas); el neurodato no sea extraído sin el consentimiento de la persona; (…) derecho a la identidad y autonomía personal (el libre albedrio): busca que no se introduzca neurodatos de manera artificial en la red neuronal de la persona, sin su consentimiento, o del que esté habilitado para darlo; (…) derecho de acceso equitativo a la aumentación cognitiva: los neuroderechos no solo son libertades personales, sino que también incluyen una garantía de igualdad que genera deberes de acceso para el Estado; y, (…) derecho a la protección ante sesgos algorítmicos o procesos automatizados de toma de decisiones: los neuroderechos protegen al individuo de la segregación y exclusión, entrenado no solo al uso directo de instrumentos en el individuo, sino que, particularmente, en sui vínculo con el mundo digital".

Un reto fundamental para toda la sociedad es tener siempre presente la importancia de la protección, privacidad (intimidad) y seguridad en la vida física y virtual, máxime si son menores o adolescentes. Precisamente, éstos sin ser conscientes de ello, en muchas ocasiones comparten una cantidad importante de información personal y datos personales en internet. Y ese comportamiento "inconsciente", "impulsivo" e "ignorante de cualquier peligro" es aprovechado por las plataformas y aplicaciones, por ejemplo, con fines, comerciales y, por adultos

depravados a través de comportamientos delictuales contra menores y adolescentes (material pornográfico y pedófilo).

Ciertamente, existen distintas campañas de marketing de moda o de cosméticos dirigidas a los menores y adolescentes (como público objetivo), aprovechando la popularidad de los *influencers*. Se habla de la sexualización y comercialización de contenidos dirigidos expresamente a los menores y adolescentes. Por su parte, en el informe elaborado por "*The Child's Rigth to Protection against Economic Explotation in the Digital World*" se indica, al respecto, que los menores y adolescentes están expuestos a prácticas comerciales agresivas de los juegos que utilizan, en los que se incluye publicidad, compras dentro de la aplicación o recompensas a través de la "caja botín" —lo que genera un consumo compulsivo—; y también les ofrecen la posibilidad de ser *influencer* o jugadores profesionales de e-*Sports*, con el peligro de ser víctimas de una explotación económica[3].

Ahora bien, en España el Grupo de expertos en la Lucha contra la violencia contra la mujer del Consejo de Europea (GREVIO) en su primer informe de evaluación —España (en línea) 2020— alertan del hecho importante que "desde hace años las experiencias de violencia de género contra las mujeres y niñas en los entornos digitales y físicos se ha visto amplificadas por la tecnología digital, llegando a una escala de violencia nunca vista". Ya en 2011 la Asamblea Parlamentaria del Consejo de Europa expresó "su profunda preocupación por la mayor accesibilidad del público a material pornográfico violento y extremo, que representa gráficamente escenas de degradación, violencia sexual, tortura, asesinato, necrofilia o bestialidad con finalidad de excitación sexual". No dejamos de mencionar el referente en los estándares internacionales en este campo como es el Convenio del Consejo de Europea sobre Prevención y la Lucha contra la Violencia contra las Mujeres y la Violencia Doméstica (Convenio de Estambul) de 2011, ratificado por España en 2014 en su artículo 5 exhorta a los Estados "la obligación que tienen de evitar que se cometa violencia contra la mujer y actuar con la diligencia debida para prevenir, investigar, castigar, indemnizar los actos de violencia cometido por actores no estatales —particulares, empresas, delincuencia organizada, etc.—, aplicando la perspectiva de género (artículo 6). Un enfoque dual en el que convive de forma trasversal la perspectiva de género y medidas específicas para la protección de la mujer se ve reflejado en la Agenda 2030 en el ODS número 5. Se debe adoptar por los Estados las medidas necesarias para castigar estos comportamientos delictivos; cambiar los comportamientos y los estereotipos que dan lugar a esa violencia; sensibilizar al público sobre las consecuencias negativas que causan estas conductas en la víctima; educar a la sociedad en rechazar la violencia y especializar a los profesionales que trabajan con las víctimas.

Pues bien, de nuevo, en este mundo digital, el papel y la actuación de los padres y centros docentes resulta esencial ante los riesgos en que pueden verse inmerso los menores y adolescentes. Así deben proporcionarles todas aquellas herramientas necesarias que les permita operar de manera segura en el mundo digital. En este sentido los centros educativos deben asumir un rol activo, no sólo limitando el acceso a dispositivos digitales (tablets, teléfonos móviles), sino también incorporando la educación digital segura en sus programas; lo que posibilita, no sólo impartir conocimientos técnicos, sino también informar a los menores y adolescentes lo que representa una navegación en línea segura. No olvidemos

que estos son responsables de los hechos dañosos llevados a cabo por sus hijos o alumnos tanto en el campo presencial como el virtual (responsabilidad subjetiva o por culpa —artículos 1903 y 1904 del Código Civil y en el artículo 61 de la Ley Orgánica 5/2000, de 12 de enero reguladora de la responsabilidad penal de los menores —cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden; y si éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos—)[4].

Sobre tales bases, el Consejo de Derechos Humanos de Naciones Unidas en Resolución "promoción, protección y disfrute de los derechos humanos en internet" significó que los derechos de los sujetos debían ser protegidos en internet, invocando el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.

Por su parte, en el año 2007 UNICEF en su informe "niños en un mundo digital" hace especial referencia a los peligros que los menores y adolescentes pueden encontrarse en el mundo digital.

Ahora bien, ante esta situación de vulnerabilidad en que se pueden situarse los menores y adolescentes, exige también una implicación de los poderes públicos; de ahí, la exigencia de una implementación de manera efectiva de todas aquellas herramientas e instrumentos que, previamente el legislador ha debido prever en la normativa desarrollada a tal fin.

En todo caso, el menor además de desconocer los peligros del entorno digital, ignora sus propios derechos, muchos de ellos fundamentales (derecho al honor, intimidad y propia imagen; protección de datos; y la posibilidad de que puedan ser vulnerados. Se debe imponer herramientas de control del acceso a los dispositivos y al contenido que proporcionan, a la vez que potenciar la inclusión digital

De ahí que, la protección de menores en el ciberespacio es una prioridad abordada en normativas y leyes tanto en España como a nivel internacional.

En concreto, en España la Constitución Española en su artículo 18.4 se refiere a la protección de los datos personales como un derecho fundamental. Este artículo proporciona una base sólida para la normativa que protege los datos personales de los menores en España. Por su parte, en su artículo 39 la Carta Magna establece como mandato a los poderes públicos de asegurarse la protección integral de los hijos; además de gozar los niños de la protección prevista en los acuerdos internacionales que velan por sus derechos; el artículo 154 del Código Civil establece la obligación de los padres de velar por los hijos tanto en un entorno físico como digital. Se habla de la parentalidad positiva y la parentalidad digital; asimismo, la Ley Orgánica 1/1982, de 5 de mayo de protección civil del derecho al honor, la intimidad personal y familiar y a la propia imagen, en su artículo 3 establece que los menores de edad y personas con discapacidad pueden prestar su consentimiento para asuntos relacionados con su honor, intimidad y propia imagen si poseen suficiente madurez. Si los menores no tienen capacidad suficiente, el consentimiento debe ser prestado por sus representantes, legales, quienes están obligados a comunicarlos al Ministerio Fiscal. Este, a su vez, puede oponerse y solicitar que un juez resuelva el asunto, garantizando así que cualquier intromisión no cause perjuicio material o moral al menor.

La Ley Orgánica 1/1996, de 15 de enero de Protección jurídica del Menor (LOPJM) establece un marco integral para la protección de los derechos de los menores en España; y, su contenido trasciende los límites del Código Civil para construir un amplio marco jurídico de protección que vincula a todos los Poderes Públicos, a las instituciones específicamente relacionadas con los menores, a los padres y familiares y a los ciudadanos en general.

Esta Ley reconoce no solo el derecho de los menores a la intimidad y a la propia imagen, sino también aborda la protección contra toda forma de explotación, abuso y negligencia.

En particular, el artículo 4 de esta Ley destaca la importancia de proteger el honor, la intimidad personas y familiar y la propia imagen de los menores en los medios de comunicación y redes sociales. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

Así, se prohíbe la difusión de datos o imágenes referidos a menores de edad en los medios de comunicación cuando sea contrario a su interés, incluso cuando conste el consentimiento del menor. Con ello se pretende proteger al menor, que puede ser objeto de manipulación incluso por sus propios representantes legales o grupos en que se mueve. Completa esta modificación la legitimación activa al Ministerio Fiscal. A tal fin, se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales.

Además, el artículo 5 se refiere al derecho a la información; en concreto, los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo. De ahí que, se preste especial atención a la alfabetización digital y mediática, de forma adaptada a cada etapa evolutiva, que permita a los menores actuar en línea con seguridad y responsabilidad y, en particular, identificar situaciones de riesgo derivadas de la utilización de las nuevas tecnologías de la información y la comunicación así como las herramientas y estrategias para afrontar dichos riesgos y protegerse de ellos; asimismo, las Administraciones Públicas incentivarán la producción y difusión de materiales informativos y otros destinados a los menores (…); y, velarán porque los medios de comunicación en sus mensajes dirigidos a menores promuevan los valores de igualdad, solidaridad, diversidad y respeto a los demás, eviten imágenes de violencia, explotación en las relaciones interpersonales, o que reflejen un trato degradante o sexista, o un trato discriminatorio hacia las personas con discapacidad.

En fin, como principios rectores de la actuación de los poderes públicos en relación con los menores destaca el artículo 11.2 letra i) la protección contra toda forma de violencia, incluido el maltrato físico o psicológico, los castigos físicos humillantes y denigrantes, el descuido o trato negligente, la explotación, la realizada a través de las nuevas tecnologías, los abusos sexuales, la corrupción, la violencia de género o en el ámbito familiar, sanitario, social o educativo, incluyendo el acoso escolar, así como la trata y el tráfico de seres humanos, la mutilación genital femenina y cualquier otra forma de abuso.

Por su parte la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia (LOPIVI) en su artículo 1 apartado primero dispone que, esta ley tiene por objeto garantizar los derechos fundamentales de los niños, niñas y adolescentes a su integridad física, psíquica, psicológica y moral frente a cualquier forma de violencia, asegurando el libre desarrollo de su personalidad y estableciendo medidas de protección integral, que incluyan la sensibilización, la prevención, la detección precoz, la protección y la reparación del daño en todos los ámbitos en los que se desarrolla su vida. En su apartado 2 define la violencia como toda acción, omisión o trato negligente que priva a las personas menores de edad de sus derechos y bienestar, que amenaza o interfiere su ordenado desarrollo físico, psíquico o social, con independencia de su forma y medio de comisión, incluida la realizada a través de las tecnologías de la información y la comunicación, especialmente la violencia digital. Se hace, en consecuencia, referencia explícita a una violencia digital.

Asimismo se indica que, en cualquier caso, se entenderá por violencia el maltrato físico, psicológico o emocional, los castigos físicos, humillantes o denigrantes, el descuido o trato negligente, las amenazas, injurias y calumnias, la explotación, incluyendo la violencia sexual, la corrupción, la pornografía infantil, la prostitución, el acoso escolar, el acoso sexual, el ciberacoso, la violencia de género, la mutilación genital, la trata de seres humanos con cualquier fin, el matrimonio forzado, el matrimonio infantil, el acceso no solicitado a pornografía, la extorsión sexual, la difusión pública de datos privados así como la presencia de cualquier comportamiento violento en su ámbito familiar.

En fin, buen trato es aquel que, respetando los derechos fundamentales de los niños, niñas y adolescentes, promueve activamente los principios de respeto mutuo, dignidad del ser humano, convivencia democrática, solución pacífica de conflictos, derecho a igual protección de la ley, igualdad de oportunidades y prohibición de discriminación de los menores y adolescentes.

Ahora bien, se dispone como uno de los fines de la LOPIVI, en su artículo 3 letra m) "establecer los protocolos, mecanismos y cualquier otra medida necesaria para la creación de entornos seguros, de buen trato e inclusivos para toda la infancia en todos los ámbitos desarrollados en esta ley en los que la persona menor de edad desarrolla su vida. Se entenderá como entorno seguro aquel que respete los derechos de la infancia y promueva un ambiente protector físico, psicológico y social, incluido el entorno digital".

En su artículo 33 señala que, la formación en materia de derechos, seguridad y responsabilidad digital impone a "Las administraciones públicas garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales, conforme a lo previsto en el artículo 83 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Específicamente, las administraciones públicas promoverán dentro de todas las etapas formativas el uso adecuado de Internet.

Asimismo, se contempla en la norma el derecho a la imagen, con un refuerzo del respeto al honor, intimidad e imagen del menor que ha sido víctima de violen-

cia, así como sus familiares, contemplando este derecho incluso más allá del fallecimiento del menor. De ahí que, esencialmente, en su artículo 3, letra n) se proteja la imagen del menor desde su nacimiento hasta después de su fallecimiento.

Por otra parte, esta LOPIVI modifica el párrafo a) del artículo 3 de la Ley 34/1988, de 11 de noviembre, General de Publicidad, con el siguiente tenor literal: "a) La publicidad que atente contra la dignidad de la persona o vulnere los valores y derechos reconocidos en la Constitución Española, especialmente a los que se refieren sus artículos 14, 18 y 20, apartado 4. Se entenderán incluidos en la previsión anterior los anuncios que presenten a las mujeres de forma vejatoria o discriminatoria, bien utilizando particular y directamente su cuerpo o partes del mismo como mero objeto desvinculado del producto que se pretende promocionar, bien su imagen asociada a comportamientos estereotipados que vulneren los fundamentos de nuestro ordenamiento coadyuvando a generar la violencia a que se refiere la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. Asimismo, se entenderá incluida en la previsión anterior cualquier forma de publicidad que coadyuve a generar violencia o discriminación en cualquiera de sus manifestaciones sobre las personas menores de edad, o fomente estereotipos de carácter sexista, racista, estético o de carácter homofóbico o transfóbico o por razones de discapacidad".

Se establece también el deber de denuncia por parte de toda persona que observe indicios de violencia, que podrá comunicarlo en todo caso. También podrán denunciar los menores, sin necesidad de estar acompañados por una persona adulta (artículo 50 de la LOPIVI). De ahí que, se contemple que tanto los menores de catorce años, como las personas con discapacidad que están necesitadas de una especial protección, solo deberán declarar una sola vez el testimonio que se grabará durante la fase de instrucción del proceso judicial. Su testificación en sala será excepcional, y se evitará con ello la victimización secundaria que puede producirse durante el procedimiento, ya que no revivan el trauma, ni podrán sentirse culpables. Se establecen una serie de protocolos de actuación en los centros de protección de personas menores de edad, en el artículo 53 de la LOPIVI indicando que "dichos protocolos deberán contemplar actuaciones específicas cuando el acoso se lleve a cabo a través de las nuevas tecnologías de las personas menores de edad o dispositivos móviles y se haya menoscabado la intimidad y reputación". La declaración se realizará ante la policía, que estarán formados con dicha finalidad, ya que se contempla la creación de dotaciones policiales especializadas por comunidades autónomas y entidades locales. Se contempla que las víctimas de delitos violentos graves gocen del derecho a la asistencia jurídica gratuita (artículo 14 de la LOPIVI). Se refuerza el derecho del menor a ser escuchado, sin limitación de edad, y se aplica en todos los procesos que estén relacionados con la violencia y reparación de las víctimas.

En este contexto, se menciona la función de la Agencia Española de Protección de Datos (AEPD) para garantizar los derechos digitales de los menores, ya que se dispone de un canal accesible, con la finalidad de retirar cualquier contenido ilícito de forma inmediata.

Por otra parte, se disponen nuevos delitos, ya que se castigará a quienes promuevan a través de internet el suicidio, la autolesión o trastornos alimenticios entre menores, o la comisión de delitos sexuales contra menores. Además, se prevé

que los contenidos se retiren de la red. Se crea un registro central de información sobre violencia contra la infancia, y se ha elabora *una estrategia de erradicación de la misma*. Asimismo, se indica que, las conductas inadecuadas a través de internet pueden consistir en diversas tipologías como el ciberbullying o acoso en las redes, el grooming o acoso para ganar la confianza de un menor con propósitos sexuales, la ciberviolencia de género o acoso que lleva un comportamiento de violencia de género, siendo un ejemplo de comportamiento machista, y el sexting o difusión de imágenes sin consentimiento; y en su artículo 45 aboga por un uso seguro y responsable de Internet, mediante el establecimiento de campañas de sensibilización, indicando lo siguiente: "1. Las administraciones públicas desarrollarán campañas de educación, sensibilización y difusión dirigidas a los niños, niñas y adolescentes, familias, educadores y otros profesionales que trabajen habitualmente con personas menores de edad sobre el uso seguro y responsable de Internet y las tecnologías de la información y la comunicación, así como sobre los riesgos derivados de un uso inadecuado que puedan generar fenómenos de violencia sexual contra los niños, niñas y adolescentes como el ciberbullying, el grooming, la ciberviolencia de género o el sexting, así como el acceso y consumo de pornografía entre la población menor de edad"[5]. Conviene precisar que, el menor, como usuario de internet y todo lo que ello implica, puede adoptar una conducta activa o pasiva en relación con el acceso al mundo digital y a los contenidos que se ofrecen[6].

Respecto de la citada Estrategia de erradicación de la violencia procede indicar que, cubre el periodo 2023-2030 y contiene cinco áreas estratégicas, para cada una de las cuales se establece un objetivo, una serie de líneas de actuación, así como las medidas más importantes con sus respectivos resultados para evaluar el impacto. Para facilitar su seguimiento, se incluye en el anexo 1 un cuadro de las medidas, actores responsables de su ejecución y posibles indicadores. Respetando las normas y los procesos presupuestarios, se propondrán planes operativos con objetivos, presupuestos y cronograma, concretando mejor la Estrategia. Cada Plan tendrá una evaluación y memoria económica. Las medidas contempladas en esta Estrategia se enmarcan en el Objetivo de Desarrollo Sostenible 16 de la Agenda 2030, sobre Paz, Justicia e Instituciones Sólidas y que incluye la meta "Poner fin al maltrato, la explotación, la trata y todas las formas de violencia y tortura contra los niños" (Meta 16.2). También se tiene en cuenta la normativa internacional y nacional aplicable y la preparación a nivel estatal de otros textos estratégicos relevantes como la Estrategia de Derechos de la infancia y la adolescencia. La Estrategia no pretende recoger una enumeración exhaustiva de todas las acciones necesarias para la erradicación de la violencia, sino impulsar un proceso en torno a las cinco áreas estratégicas claves para alcanzar ese objetivo y, define una serie de directrices generales y medidas que pretenden garantizar un estándar de protección y prevención. Dentro de dicho proceso deberá existir una coordinación y colaboración entre las diferentes administraciones, entidades y organizaciones que, en el marco de este estándar garantista, aseguren la implementación de las actuaciones.

En todo caso, siguiendo con la normativa nacional, la Ley Orgánica 8/2015, de 22 de julio de modificación del sistema de proyección a la infancia y a la adolescencia, modifica la Ley Orgánica 1/1996, afectando al artículo 2 referente al interés superior del menor, en que se establece como primordial y debe ser objeto de

valoración. Para la interpretación y aplicación de este interés superior del menor se atenderá a unos criterios generales, así como otros que se estimen adecuados en relación a las circunstancias del caso. Se ponderarán atendiendo a la edad y madurez del menor, la necesidad de garantizar su igualdad y no discriminación, entre otros. Menciona, pues, como criterio a tener en cuenta la satisfacción de las necesidades del menor, aludiendo a las educativas. De esta forma queda redactado el mencionado precepto relativo al interés superior del menor: "1. Todo menor tiene derecho a que su interés superior sea valorado y considerado como primordial en todas las acciones y decisiones que le conciernan, tanto en el ámbito público como privado. En la aplicación de la presente ley y demás normas que le afecten, así como en las medidas concernientes a los menores que adopten las instituciones, públicas o privadas, los Tribunales, o los órganos legislativos primarán el interés superior de los mismos sobre cualquier otro interés legítimo que pudiera concurrir. Las limitaciones a la capacidad de obrar de los menores se interpretarán de forma restrictiva y, en todo caso, siempre en el interés superior del menor".

Respecto a los Objetivos de Desarrollo Sostenible (ODS) formulan una serie de acciones para lograr unos objetivos concretos y determinados que forman parte de la Agenda 2030 sobre el desarrollo sostenible. Consisten en un total de 17 objetivos, de los que consideramos que alguno de ellos se puede aplicar al caso objeto de estudio. Estas propuestas se deben alcanzar en el año 2030. De esta forma, el ODS 10 resulta adaptable, pues, los menores forman parte de los denominados colectivos vulnerables.

El entorno digital está íntimamente vinculado a la sociedad de la información y a la sociedad del conocimiento, se manejan una cantidad ingente de datos personales, a la par que, se fomenta la utilización de la inteligencia artificial en el ámbito digital. De hecho, ante el reto que supone la protección de datos y la inteligencia artificial se han aprobado tres Reglamentos europeos: Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, 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 datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos —RGPD—)[7]; el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre del 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de servicios digitales); y, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establece normas armonizadas en materia de inteligencia artificial y por el que se modifican el Reglamento (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139, y (UE) nº 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797; y (UE) 2020/1828 (Reglamento de Inteligencia Artificial —RIA—) donde se fijan las pautas de utilización de la misma en diversos ámbitos. Así, se contempla la prohibición de sistemas de inteligencia artificial que constituyan una amenaza para los derechos de los sujetos. En el caso de los menores, estos pueden determinar un comportamiento en el que la inteligencia artificial influya, por ejemplo, a través de videojuegos, u otros juguetes o actividades que inciten a la violencia digital o a comportamientos discriminatorios[8].

También se comenta que la inteligencia artificial provoca los denominados riesgos digitales, fomentando la desigualdad en la utilización de algoritmos y afec-

tar a los menores. Precisamente, el Libro Blanco sobre la inteligencia artificial —un enfoque europeo orientado a la excelencia y la confianza—, de 19 de febrero de 2020 menciona el potencial peligro que pueden tener los relojes de pulsera inteligentes destinados a los menores al ser posible acceder a su geolocalización ante la existencia de una brecha en su seguridad, o también las aplicaciones de móviles que llevan consigo esa localización, o la cesión de determinados datos personales por parte de los menores sin información previa, sin su consentimiento expreso o el de sus padres y desconociendo los riesgos que esto supone.

En este plano internacional, además de la Convención sobre los Derechos del Niño, de 20 de noviembre de 1989 y siguiendo las directrices de la Declaración de Ginebra de 1924 relativa a los Derechos del Niño, así como en la Declaración de los Derechos del Niño, de 20 de noviembre de 1959, junto con la Declaración Universal de Derechos Humanos, y el Pacto Internacional de Derechos Civiles y Políticos que protegen al menor antes y después de su nacimiento y los considera un grupo vulnerables que necesita de una especial protección, obligando a todos los Estados parte a asegurarse y otorgar especial consideración a la atención de su interés —algo que también fue reafirmado en el artículo 24.2 de la Carta de los derechos Fundamentales de la Unión Europea—; el Comité sobre los Derechos del Niño en su Observación General número 14, página 32 define el interés superior del menor como uno de los valores fundamentales de la Convención que, debe entenderse y aplicarse en una triple vertiente: es un derecho sustantivo; es un principio jurídico interpretativo fundamental; y es una norma de procedimiento. Y, asimismo, en esta Observación General, el Comité precisa que el interés superior de los menores y adolescentes debe entenderse y aplicarse en relación con los otros tres principios generales de la Convención: el derecho a la no discriminación; el derecho a la vida, a la supervivencia y al desarrollo; y el derechos a ser escuchado (pp. 41-45). Y en la ya citada Observación General número 25 adoptada en 2021 en relación con los derechos de los menores y adolescentes en el entorno digital, recuerda que sus facultades evolucionan a través de un proceso gradual de adquisición de competencias, comprensión y autonomía y que los menores y adolescentes "pueden participar con mayor independencia respecto de la supervisión de sus padres y cuidadores". Ciertamente, se concibe el interés del menor como un concepto dinámico que, debe ser tenido en cuenta por los Estado a la hora de elaborar medidas encaminadas a proteger a los menores y adolescentes en ese entorno digital.

En el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía de la Asamblea General de Naciones Unidas, de 25 de mayo de 2000 siguiendo los resultados de la Conferencia Internacional de Lucha contra la Pornografía Infantil en Internet de Viena en 1999 se solicita una penalización de todo tipo de material audiovisual, tanto en la producción como en la propaganda de dicho material. En el año 2021, la UNESCO presentó una guía titulada Recomendación sobre la ética de la IA, en la cual se recogen una serie de principios generales, en consonancia con los presentados previamente por parte de otras entidades internacionales como los Principios de Asilomar Future of Life Institute (2017); la Declaración de la universidad de Montreal para un desarrollo respon-

sable de la IA (2018); o las Directrices éticas para una IA confiable de la Comisión Europea (2019).

Posteriormente, de nuevo en el plano nacional, la Carta de los derechos digitales de los niños, niñas y adolescentes de la Fundación ANAR, el Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España, y a través de un Comité de Expertos, redacta la Carta de Derechos Digitales, que somete a consulta pública, y en cuyo articulado contiene un precepto específico dentro de los derechos de igualdad, el X sobre la "Protección de las personas menores de edad en el entorno digital".

Los derechos que se reconocen en la Carta, se entienden sin perjuicio de los que se reconocen en las siguientes normas: 1. 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; modificada posteriormente por Ley Orgánica 3/1985, de 29 de mayo; 2. La Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación; 3. La Ley 34/2002, de 11 de julio de servicios de la sociedad de la información y de comercio electrónico; 4. El Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia —actualmente derogado—; y, 5. La Ley 10/2021, de 9 de julio, de trabajo a distancia.

En este texto se reconocen una serie de derechos: "Derechos y Libertades en el entorno digital", dentro del apartado I, punto 3. "Se promoverá que, en los procesos de transformación digital, el desarrollo y el uso de la tecnología digital, así como cualquier proceso de investigación científica y técnica relacionado con ellos o que los utilice instrumentalmente, se tenga presente la exigencia de garantizar la dignidad humana, los derechos fundamentales, la no discriminación, el libre desarrollo de la personalidad y orientarse al logro del bien común". En el apartado III, se establece el derecho a la protección de datos, en su punto 1. También se indican el derecho a la identidad en el entorno digital; el derecho al pseudonimato; el derecho a no ser localizado ni perfilado; el derecho a la seguridad digital; el derecho a la herencia digital; el derecho a la igualdad y no discriminación en el entorno digital. En el ámbito de los derechos digitales en entornos específico, se menciona el derecho a la protección de la salud en el entorno digital. Dentro de los derechos de participación y de conformación del espacio público, se mencionan los derechos a la neutralidad en Internet; libertad de expresión y libertad de información; derecho a la participación ciudadana por medios digitales; el derecho a la educación digital. Asimismo, se promoverá la implantación de procedimientos para la verificación de la edad, el derecho a recibir formación e información adecuada y adaptada a sus necesidades sobre los entornos digitales a los que accedan y el acceso a medios para solicitar y en su caso obtener la tutela de sus derechos frente a comportamientos o acciones lesivas o ilícitas

Como hemos indicado en líneas precedentes, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8 apartado 1 de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16 apartado 1 del Tratado de Funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de datos de carácter personal que le conciernan. Asimismo, como hemos mencionado en líneas precedentes, nuestro artículo 18.4 de la Constitución Española reconoce este derecho fundamental a la protección de datos personales al disponer que "la ley

limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Al respecto, la sentencia del Tribunal Constitucional 94/1998, de 4 de mayo[9] señala que, nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos personales y sobre su uso y destino para evitar el tráfico ilícito de los mismos o lesivos para la dignidad y los derechos de los afectados; por lo que, el derecho a la protección de datos se confiere como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la sentencia de este mismo Tribunal 292/2000, de 30 de noviembre[10] se considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que, faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular o cuales puede este tercero recabar y que también permite al individuo saber quien posee estos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

En este contexto, para garantizar un nivel uniforme y elevado de protección de las personas físicas, eliminar los obstáculos a la circulación de datos personales dentro de la Unión Europea y que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea, el RGPD de aplicación directa en toda la Unión Europea reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, incluso con relación al tratamiento de categorías especiales de datos personales —datos sensibles— y respecto a determinadas circunstancias relativas a situaciones específicas de tratamiento, entre otras, las relativas a las condiciones de licitud del tratamiento de datos. A tal fin, en España se aprobó la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDPYGDD), cuya entrada en vigor ha tenido lugar el día 7 de diciembre de 2018.

En esta norma española como el Reglamento comunitario se refuerza la protección de los menores en el entorno digital. Precisamente, el considerando número 38 del citado Reglamento señala que, "los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario y a la obtención de datos personales relativos a los niños cuando se utilicen servicios ofrecidos directamente a un niño".

Se ha de proteger su derecho a la privacidad que abarca los derechos fundamentales al honor, intimidad personal y familiar y a la propia imagen (artículo 18.1 de la Constitución Española) y el derecho a la protección de datos personales (artículo 18.4 de la citada Carta Magna). Además, se ha de primar en cualquier actuación en que intervengan menores su interés superior.

En todo caso, antes que cualquier persona física consienta el tratamiento de sus datos personales, atendiendo al principio de transparencia y el derecho a la información, se ha de informar previamente del tratamiento de los datos de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cuando se trata de información dirigida específicamente a un menor

y esta información se facilitará por escrito o por otros medios incluso los electrónicos (artículo 12.1 del Reglamento).

En este contexto, el RIA que es, precisamente, fruto de largas negociaciones en el seno de las instituciones europeas y nace en el contexto de la Estrategia Europea de Inteligencia Artificial de la Comisión Europea, a través de la cual se pretende convertir a la Unión Europea en una región de referencia mundial para la Inteligencia Artificial (en adelante, IA), garantizando el respeto a los derechos fundamentales, la democracia, el Estado de Derecho y la sostenibilidad medio ambiental; establece, asimismo, normas para garantizar el uso seguro y ético de la IA, incluyendo medidas para proteger a los menores[11]. Su objetivo es evitar riesgos como la discriminación, la vigilancia indebida y el uso de la IA en prácticas que pueden afectar negativamente a los derechos fundamentales de los niños. A los riesgos asociados a la privacidad se deben unir los riesgos asociados a las nuevas tecnologías: como los derivados del uso de la inteligencia artificial; el internet de las cosas; el tratamiento de los neurodatos o la autenticación biométrica[12].

Además, el Reglamento de Servicios Digitales refuerza también la protección de los menores en línea, exigiendo que las plataformas digitales implementen medidas de adecuadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad en su servicio; y, protección contra contenidos perjudiciales (artículo 28)[13]. En el considerando número 71 se establece, precisamente, que: "la protección de los menores es un objetivo político importante de la Unión. Puede considerarse que una plataforma en línea es accesible para los menores cuando sus condiciones generales permiten a los menores utilizar el servicio, cuando su servicio está dirigido a menores o es utilizado predominantemente por ellos, o cuando el prestador es consciente de que algunos de los destinatarios de su servicio son menores, por ejemplo, porque ya trata para otros fines datos personales de los destinatarios de su servicio que revelan su edad. Los prestadores de plataformas en línea utilizadas por menores deben adoptar medidas adecuadas y proporcionadas para proteger a los menores, por ejemplo, diseñando sus interfaces en línea o partes de estas con el máximo nivel de privacidad, seguridad y protección de los menores por defecto, cuando proceda, o adoptando normas para la protección de los menores, o participando en códigos de conducta para la protección de los menores. Deben tener en cuenta las mejores prácticas y las orientaciones disponibles, como las que ofrece la Comunicación de la Comisión titulada "Una década digital para los niños y los jóvenes: la nueva estrategia europea para una internet mejor para los niños (BIK+)". Los prestadores de plataformas en línea no deben presentar anuncios basados en la elaboración de perfiles mediante la utilización de datos personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor. De conformidad con el Reglamento (UE) 2016/679, en particular el principio de minimización de datos previsto en su artículo 5, apartado 1, letra c), esta prohibición no debe llevar al prestador de la plataforma en línea a mantener, obtener o tratar más datos personales de los que ya dispone para evaluar si el destinatario del servicio es un menor. Por lo tanto, esta obligación no debe incentivar a los prestadores de plataformas en línea a capturar la edad del destinatario del servicio antes de su uso. Esto debe aplicarse sin perjuicio del Derecho de la Unión en materia de protección de datos personales"[14].

A tal fin, se debe operar sobre el llamado "diseño adecuado para la edad" en servicios, aplicaciones, términos, condiciones, políticas, interfaces y experiencia del usuario que sean adecuados para los menores y adolescentes, teniendo en cuenta sus derechos y su bienestar. Asimismo, se debe ofrecer a los menores y adolescentes desde todos los sectores implicados: una protección de dispositivos frente a los riesgos y amenazas, adoptando medidas de seguridad y protección; una protección de datos y privacidad: proteger los datos personales y la intimidad personal; una protección de la salud física y mental: riesgos para la salud y el bienestar físico y psicológico; y protección frente a la violencia en el entorno digital (ciberacoso, sexting, grooming, etc.); a lo que debemos añadir un diseño de los productos y servicios digitales teniendo en cuenta la edad —lo que exige evaluaciones de impacto obligatorias y accesibles—; medidas de prevención que permitan un uso responsable y seguro —incluir información y advertencias sobre un uso responsable y riesgos para prevenir conductas aditivas—; o medidas que limiten el acceso a contenidos inadecuado —mediante un etiquetado inteligente por edades en contenidos y productos que faciliten la detección de contenidos potencialmente dañinos para los menores y adolescentes—; o, en fin, obligar a los algoritmos y sistemas de tratamiento automático a que sean auditados por terceros independientes y autoridades de control para evitar sesgos discriminatorios, la manipulación, la adicción y ofrezcan una clara protección a la privacidad, recordando a quienes diseñen, desarrollen, mantengan, apliquen o usen el algoritmo que son responsables de los daños que se ocasiones a los menores y adolescentes en la aplicación del algoritmo.

En línea con lo anterior, en 2012 se elaboró la primera estrategia europea para una Internet mejor para los niños (BIK, por sus siglas en inglés), que ha sido actualizada en mayo de 2022 (BIK+7), con el objetivo de garantizar la protección, el respeto y la capacitación de los menores y adolescentes en línea, en la nueva década digital. Esta estrategia da soporte a la red de Centros de Seguridad en Internet, cuyo nodo en España opera INCIBE, y que llevan a cabo actividades de sensibilización y formación, ofrecen ayuda, orientan el reporte e identifican las tendencias y amenazas emergentes a través de líneas de ayuda, organizan anualmente el Día de Internet Segura, con el soporte de la red paneuropea INSAFE y operan líneas directas o hotlines para reducir la disponibilidad de contenido de abuso sexual infantil en línea. INCIBE coordina, desde 2018, el consorcio europeo SIC-Spain, una plataforma público-privada de colaboración nacional en materia de diagnóstico y concienciación, con un impacto constatable en cuanto a número de iniciativas ejecutadas, personas concienciadas y formadas y diagnósticos elaborados. En este sentido, a las iniciativas llevadas a cabo, hay que sumarles las realizadas por entidades del tercer sector, como la liderada por Adolescencia Libre de Móviles, que incluye a distintas asociaciones nacionales y a más de 30.000 familias adheridas, y han abogado por un pacto de familias para retrasarla llegada del primer móvil. Otro ejemplo serían las medidas de consenso para un Pacto de Estado que proteja a los y las menores en el entorno digital sugeridas por la Asociación Europea para la Transición Digital junto con UNICEF España, ICMedia, Dale una Vuelta, Fundación ANAR y Save the Children. Entre ellas se plantean —con un enfoque global en el abordaje de la problemática— medidas relacionadas con la salud, la educación y la responsabilidad de todos los actores implicados, incluida la industria.

Esta iniciativa, que se ha plasmado en el "Pacto de Estado: Protegiendo a la infancia y la adolescencia en el entorno digital", ha contado con el apoyo institucional de la AEPD, la Comisión Nacional de los Mercados de la Competencia, la Fiscalía General del Estado y el Instituto de la Juventud (INJUVE). El citado pacto cuenta con más de 200 adheridos entre fundaciones, asociaciones, colegios profesionales, sociedades científicas y patronales.

Sobre tales bases, el presente estudio se va a centrar en el análisis de los diferentes instrumentos y medidas dirigidas a la protección de los menores en el entorno digital —los llamados millenials o nativos digitales o tecnológicos, o Generación Y— en el Reglamento de IA de 2024 pues, aunque son expertos usuarios de las nuevas tecnologías, son también pocos conscientes de los riesgos que se derivan de su uso, máxime si se trata de sistemas con inteligencia artificial y que deben conocer los progenitores y centros docentes. Si bien, nos parece oportuno hacer, en primer lugar, una referencia al RGPD y, lo que representa el consentimiento de los menores y adolescentes, a la par que, aludimos, brevemente por razones de espacio a las redes sociales y plataformas digitales por su especial uso por los citados colectivos. No debemos olvidar la necesaria interrelación o interacción del RIA con otras Reglamentos, en especial, RGPD el responsable del tratamiento puede ser el responsables del despliegue o proveedor. Ciertamente, la interacción entre el RIA y el RGPD afecta a aspectos críticos como el análisis de riesgos, las evaluaciones de impacto y el consentimiento informado. El RIA exige una evaluación de impacto sobre derechos fundamentales para sistemas de alto riesgo, mientras que el RGPD establece la obligación de realizar evaluaciones de impacto en protección de datos personales. Ambos marcos normativos imponen requisitos de consentimiento explícito: en el RIA para pruebas reales con datos personales y en el RGPD para su tratamiento en dichos sistemas. Además, la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) y las directrices del Supervisor Europeo de Protección de Datos (SEPD) confirman que toda normativa que implique tratamiento de datos personales debe acompañarse de una evaluación de impacto para determinar sus riesgos y garantizar su proporcionalidad, idoneidad y necesidad. La mera existencia de operaciones de tratamiento previstas por la legislación supone una restricción del derecho a la protección de datos, aunque dicha restricción pueda justificarse.

En todo caso, el Comité Europeo de Protección de Datos destaca la importancia del papel de las autoridades de protección de datos (DPAs) en el marco del RIA. Dado que este Reglamento regula la comercialización y el uso de sistemas de IA en la UE, debe interpretarse en conjunto con la normativa de protección de datos, ya que el tratamiento de datos personales es un componente clave en muchas aplicaciones de IA, especialmente en aquellas de alto riesgo.

Todo ello sin olvidar lo que se conoce como datos sintéticos se conocen comúnmente como datos artificiales que se han generado utilizando un modelo matemático especialmente diseñado (incluidos los modelos de inteligencia artificial (IA)/aprendizaje automático (ML, por sus siglas en inglés)) o algoritmo. Se puede derivar entrenando un modelo (o algoritmo) con un conjunto de datos de origen para imitar las características y la estructura de los datos de origen. Los datos sintéticos de buena calidad pueden conservar en gran medida las propiedades estadísticas y los patrones de los datos de origen. Como resultado, la realización

del análisis en datos sintéticos puede producir resultados similares a los obtenidos con los datos de origen. Los datos sintéticos se pueden utilizar en una variedad de casos de uso, que van desde la generación de conjuntos de datos de entrenamiento para modelos de IA hasta el análisis de datos y la colaboración. El uso de datos sintéticos no solo puede acelerar la investigación, la innovación, la colaboración y la toma de decisiones, sino que también puede mitigar las preocupaciones sobre incidentes de ciberseguridad y brechas de datos, lo que permite un mejor cumplimiento de las regulaciones de protección de datos/privacidad[15].

En todo caso, antes de proceder al análisis del RGPD nos parece oportuno hacer una breve mención del Reglamento de Servicios Digitales por el uso de redes sociales y de plataformas en línea, motores de búsqueda.

De todas formas, el RIA se complementa con dos normativas europeas: la Propuesta de Directica del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la IA (Directiva sobre responsabilidad en materia de IA) de 28 de febrero de 2022 cuyo objetivo es mejorar el funcionamiento del mercado interior mediante el establecimiento de requisitos uniformes para determinados aspectos de la responsabilidad civil extracontractual por daños causados por sistema de inteligencia artificial[16]; y, la Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo de 23 de octubre de 2024 sobre responsabilidad por daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo cuyo objeto es establecer normas comunes sobre la responsabilidad de los operadores económicos por los daños sufridos por personas físicas causados por productos defectuosos y sobre la indemnización por esos daños, a la par que contribuir al correcto funcionamiento del mercado interior, garantizando al mismo tiempo un elevado nivel de protección de los consumidores y otras personas físicas (artículo 1)[17].

En fin, indicar que en abril de 2024, el Consejo Europeo destacó la necesidad de reforzar el liderazgo de la Unión Europea en asuntos digitales globales e invitó a la Comisión y al Alto Representante a preparar una comunicación conjunta sobre el tema.

El 8 de mayo de 2025, la Comisión ha lanzado una convocatoria pública de información para recabar ideas que ayuden a definir la política digital exterior de la UE. Diversas partes interesadas, como empresas tecnológicas, asociaciones comerciales, autoridades nacionales de la UE y de terceros países, la sociedad civil, organizaciones no gubernamentales, el mundo académico y la ciudadanía, compartiendo sus opiniones, como analizaremos.

En junio de 2025 la Unión Europea, asimismo, ha presentado su Estrategia Digital Internacional a través de la cual pretende entre otras cosas: Implementar una Oferta Comercial Tecnológica de la Unión Europea, combinando inversiones de los sectores público y privado de la Unión europea para apoyar la transición digital de los países socios, incorporando componentes como Fábricas de IA, inversiones en conectividad segura y confiable, Infraestructura Publica Digital, ciberseguridad; y fortaleces la gobernanza digital global, promoviendo un orden digital basado en normas, en consonancia con los valores fundamentales de la Unión Europea.

II. REGLAMENTO DE SERVICIOS DIGITALES. EN ESPECIAL, LA PROTECCIÓN DE LOS MENORES Y ADOLESCENTES ANTE LOS RIESGOS DE LAS REDES SOCIALES, PLATAFORMAS EN LÍNEA, MOTORES DE BUSQUEDA.

Veinte años después de la adopción de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo nos encontramos con nuevos e innovadores modelos de negocio y servicios, como las redes sociales y las plataformas en línea que permiten a los consumidores celebrar contratos a distancia con comerciantes, a los usuarios profesionales y a los consumidores comunicar información y acceder a ella, y efectuar transacciones de formas novedosas. La mayoría de los ciudadanos de la Unión utiliza ahora este tipo de servicios a diario, incluyendo los menores de edad y adolescentes. Si bien, la transformación digital y el creciente uso de esos servicios entraña también nuevos riesgos y desafíos para los destinatarios individuales de los correspondientes servicios, las empresas y la sociedad en su conjunto. De ahí, la necesidad de adoptar un Reglamento en el que se establezcan las condiciones para que en el mercado interior surjan y se desarrollen servicios digitales innovadores. Resulta necesario aproximar en el ámbito de la Unión las disposiciones reguladoras nacionales referidas a los requisitos aplicables a los prestadores de servicios intermediarios a fin de evitar y eliminar la fragmentación del mercado interior y garantizar la seguridad jurídica; de modo que se reduzca la incertidumbre para los desarrolladores y se fomente la interoperabilidad. Si se aplican requisitos tecnológicamente neutros, la innovación no debería verse obstaculizada sino estimulada. Ciertamente, la Unión Europea quiere asegurarse que: 1. Las tecnologías digitales y las plataformas en línea respeten los derechos de todos; 2. Podamos confiar en los servicios digitales que utilizamos; y, 3. Estemos seguros y protegidos en línea, independientemente del tipo de servicio digital que utilicemos

Este Reglamento de Servicios Digitales (DSA, por sus siglas en inglés) comenzó a utilizarse el 16 de noviembre de 2022. Las diecinueve primeras plataformas designadas como plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño anunciadas por la Comisión en abril de 2023 tuvieron que empezar a respetar las normas cuatro meses más tarde. A partir del 17 de febrero de 2024, todos los servicios digitales, incluidas las plataformas más pequeñas, deben respetar las normas pertinentes del Reglamento de Servicios Digitales recoge el conjunto de normas necesarias para ello y, en consecuencia, es de aplicación a los prestadores de determinados servicios de la sociedad de la información definidos en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, esto es, a cualquier servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición de un destinatario a título individual.

En concreto, el Reglamento debe aplicarse a los prestadores de servicios intermediarios, en particular los servicios intermediarios consistentes en servicios conocidos como de "mera transmisión", de "memoria caché" y de "alojamiento de datos", dado que el crecimiento exponencial del uso de dichos servicios, principalmente para todo tipo de fines legítimos y beneficiosos para la sociedad, también

ha incrementado su importancia en la intermediación y propagación de información y actividades ilícitas o de otras que también resultan nocivas[18].

Su principal finalidad es regular la forma en la que las empresas intermediarias de servicios digitales (por ejemplo, compartición de contenidos de usuarios, *marketplaces*, buscadores, plataformas de viajes, hoteles, etc.) colaboren para la retirada de contenidos ilícitos de Internet y la protección de los derechos fundamentales. En concreto 1) Confirma y aclara el régimen de responsabilidad introducido por la directiva de comercio electrónico; 2) Establece nuevas obligaciones de diligencia debida; 3) Crea nuevos mecanismos de supervisión y control; y, 4) Impone un nuevo régimen sancionador. Se trata de una evolución de los principios que ya introdujo a principios del milenio la Directiva de Comercio Electrónico (en España, la Ley de Servicios de la Sociedad de la Información) que, en lo fundamental, siguen siendo aplicables. Al adoptar forma de Reglamento disminuye el riesgo de fragmentación normativa y armoniza una normativa cada vez más dispersa, ayudando con ello a cohesionar el mercado único. Así, se mantiene en líneas generales el sistema de responsabilidad *ex post* de los prestadores intermediarios de servicios digitales; de forma que, solo serán responsables por los contenidos ilícitos que suben sus usuarios si tienen conocimiento efectivo de que, en efecto, se trata de contenidos ilícitos. Para facilitar estas denuncias, se exige que los prestadores implementen mecanismos de notificación y retirada. Por ejemplo, el titular de una marca puede notificar a un mercado digital (*marketplace)* que retire productos falsificados. Se exige además que se introduzcan mecanismos de apelación así como informes de transparencia. La principal novedad de la DSA es el establecimiento de obligaciones de diligencia debida que serán más gravosas dependiendo del tipo de servicios y del tamaño del prestador. Las más gravosas son las que aplicarán a las plataformas y buscadores de muy gran tamaño, esto es, con más de 45 millones de usuarios. Y sanciones más duras por incumplimiento.

Asimismo, el Reglamento vela por que todos los servicios digitales que utilizamos, especialmente las llamadas "plataformas en línea de muy gran tamaño" (VLOPs)[19], como Meta (Facebook, Instagram)[20], Snapchat, TikTok[21], X (Twitter), Amazon, o YouTube, así como los "motores de búsqueda en línea de muy gran tamaño"[22], como Google o Bing, apliquen más medidas para proteger los derechos de sus usuarios, garantizar nuestra seguridad y frenar la difusión de contenido ilícito o inapropiado. Y, engloba distintos tipos y tamaños de servicios en línea que cualquier persona en la Unión Europea puede utilizar, independientemente de dónde se ubique el servicio, y establece normas más estrictas para los servicios de mayor tamaño.

Tiene como objetivo contribuir al correcto funcionamiento del mercado interior de servicios intermediarios estableciendo normas armonizadas para crear un entorno en línea seguro, predecible y fiable que facilite la innovación y en el que se protejan efectivamente los derechos fundamentales amparados por la Carta, incluido el principio de protección de los consumidores (artículo 1.1); y, se aplicará a los servicios intermediarios ofrecidos a destinatarios del servicio que tengan su lugar de establecimiento o estén situados en la Unión, con independencia de donde los prestadores de dichos servicios intermediarios tengan su lugar de establecimiento (artículo 2.1). Por ende, no se aplicará a ningún servicio que no sea un servicio intermediario ni a ningún requisito que se imponga respecto de un

servicio de esa índole, con independencia de si el servicio se presta mediante el uso de un servicio intermediario; ni afectará a la aplicación de la Directiva 2000/31/CE (artículo 2.2 y 2.3).

En todo caso, este Reglamento ha de entenderse sin perjuicio de otros actos del Derecho de la Unión que regulan la prestación de servicios de la sociedad de la información en general, que regulan otros aspectos de la prestación de servicios intermediarios en el mercado interior o que precisan y complementan las normas armonizadas establecidas en el Reglamento, como la Directiva 2010/13/UE del Parlamento Europeo y del Consejo incluidas las disposiciones establecidas en ella por lo que se refiere a las plataformas de distribución de vídeos, los Reglamentos (UE) 2019/1148, (UE) 2019/1150, (UE) 2021/784 y (UE) 2021/1232 del Parlamento Europeo y del Consejo y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo y las disposiciones de Derecho de la Unión establecidas en un Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal y en una Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales. Análogamente, por motivos de claridad, el presente Reglamento ha de entenderse sin perjuicio del Derecho de la Unión en materia de protección de los consumidores, en particular los Reglamentos (UE) 2017/2394 y (UE) 2019/1020 del Parlamento Europeo y del Consejo, las Directivas 2001/95/CE, 2005/29/CE, 2011/83/UE y 2013/11/UE del Parlamento Europeo y del Consejo, y la Directiva 93/13/CEE del Consejo, y en materia de protección de los datos personales, en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Asimismo, este Reglamento también ha de entenderse sin perjuicio de las normas de la Unión en el ámbito del Derecho internacional privado, en particular las relativas a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, como el Reglamento (UE) nº 1215/2012, y a la ley aplicable a las obligaciones contractuales y extracontractuales. La protección de las personas físicas con respecto al tratamiento de los datos personales se rige exclusivamente por las disposiciones del Derecho de la Unión sobre esa materia, en particular el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE. Este Reglamento ha de entenderse, además, sin perjuicio del Derecho de la Unión en materia de condiciones laborales y del Derecho de la Unión en el ámbito de la cooperación judicial en materia civil y penal. No obstante, en la medida en que dichos actos jurídicos de la Unión persiguen los mismos objetivos que los establecidos en el Reglamento, las normas del mismo se deben aplicar a cuestiones que esos otros actos jurídicos no resuelven, o no resuelven por completo, así como a problemas para los que esos otros actos jurídicos dejan abierta la posibilidad de que los Estados miembros adopten determinadas medidas de ámbito nacional[23].

Partiendo de la premisa que, la protección de los menores es un objetivo político importante de la Unión se entiende que una plataforma en línea es accesible para los menores cuando sus condiciones generales permiten a los menores utilizar el servicio, cuando su servicio está dirigido a menores o es utilizado predominantemente por ellos, o cuando el prestador es consciente de que algunos de los destinatarios de su servicio son menores, por ejemplo, porque ya trata para otros fines datos personales de los destinatarios de su servicio que revelan su edad. Es,

por ello, que los prestadores de plataformas en línea utilizadas por menores deben adoptar medidas adecuadas y proporcionadas para proteger a los menores, por ejemplo, diseñando sus interfaces en línea o partes de estas con el máximo nivel de privacidad, seguridad y protección de los menores por defecto, cuando proceda, o adoptando normas para la protección de los menores, o participando en códigos de conducta para la protección de los menores. Deben tener en cuenta las mejores prácticas y las orientaciones disponibles, como las que ofrece la Comunicación de la Comisión titulada "Una década digital para los niños y los jóvenes: la nueva estrategia europea para una internet mejor para los niños (BIK+)". Además, los prestadores de plataformas en línea no deben presentar anuncios basados en la elaboración de perfiles mediante la utilización de datos personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor. En todo caso, de conformidad con el RGPD, en particular, en lo referente al principio de minimización de datos previsto en su artículo 5, apartado 1, letra c), esta prohibición no debe llevar al prestador de la plataforma en línea a mantener, obtener o tratar más datos personales de los que ya dispone para evaluar si el destinatario del servicio es un menor. Por lo tanto, esta obligación no debe incentivar a los prestadores de plataformas en línea a capturar la edad del destinatario del servicio antes de su uso. En consecuencia, esto debe aplicarse sin perjuicio del Derecho de la Unión en materia de protección de datos personales. En este contexto, el Reglamento obliga a las plataformas en línea a respetar nuestros derechos fundamentales, máxime si son menores o adolescentes cuando están en línea. De entre los enumerados en la Carta de los Derechos Fundamentales de la Unión Europea resultan más pertinentes con relación al Reglamento de Servicios Digitales y la protección de los menores en línea: 1. El principio del "interés superior del menor"; 2. El derecho a la protección del menor; 3. El derecho a la libertad de expresión; el derecho a no sufrir discriminación; 4. El derecho a la protección de los datos personales; y, 5. El respeto de un alto nivel de protección de los consumidores. Todos tenemos derecho a la intimidad y a mantener nuestros datos personales seguros. Además, de acuerdo con el Reglamento de Servicios Digitales, las plataformas en línea utilizadas por menores deben proteger la intimidad y la seguridad de sus usuarios. Para ello, es posible adoptar ajustes especiales de privacidad y seguridad por defecto, entre otras opciones. Efectivamente, las citadas plataformas deben ofrecer configuraciones predeterminadas que protejan la privación de los menores y evitar la recopilación excesiva de datos.

Por otra parte, los prestadores de servicios intermediarios incluirán en sus condiciones generales información sobre cualquier restricción que impongan en relación con el uso de su servicio respecto de la información proporcionada por los destinatarios del servicio[24]. Esta información deberá incluir datos sobre cualesquiera políticas, procedimientos, medidas y herramientas empleadas para moderar los contenidos, incluidas la toma de decisiones mediante algoritmos y la revisión humana, así como sobre las normas de procedimiento de su sistema interno de gestión de reclamaciones. Se expondrá en lenguaje claro, sencillo, inteligible, accesible al usuario e inequívoco, y se hará pública en un formato fácilmente accesible y legible por máquina. Asimismo, las condiciones deben redactarse y actualizarse de manera que resulten fácilmente comprensibles para todos, espe-

cialmente para los menores o adolescentes. Los servicios en línea utilizados por menores deben hacer un esfuerzo adicional para explicar las cosas claramente, de forma que los usuarios jóvenes puedan comprender para qué dan su acuerdo (artículo 14). En este contexto, las plataformas deben explicar sus condiciones de uso, políticas de privacidad y algoritmos de forma clara y comprensible, especialmente, si se trata de menores y adolescentes. Esto implica una mayor transparencia en el funcionamiento de los sistemas de recomendación y de toma de decisiones automatizadas.

Con relación a los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben evaluar en profundidad cuatro categorías de *riesgos sistémicos*. La primera categoría se refiere a los riesgos asociados a la difusión de contenidos ilícitos, como la difusión de materiales de abuso sexual de menores o delitos de incitación al odio, u otros tipos de usos indebidos de sus servicios para cometer delitos, y la realización de actividades ilícitas como la venta de productos o servicios prohibidos por el Derecho de la Unión o nacional, incluidos los productos peligrosos o falsificados o el comercio ilegal de animales. Por ejemplo, esa difusión o esas actividades pueden constituir un riesgo sistémico significativo cuando el acceso a contenidos ilícitos pueda propagarse rápida y ampliamente a través de cuentas con un alcance especialmente amplio o de otros medios de amplificación. Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben evaluar el riesgo de difusión de contenidos ilícitos, con independencia de que la información sea o no además incompatible con sus condiciones generales. Esta evaluación se entiende sin perjuicio de la responsabilidad personal del destinatario del servicio de plataformas en línea de muy gran tamaño o de los propietarios de sitios web indexados por motores de búsqueda en línea de muy gran tamaño ante la posible ilegalidad de su actividad con arreglo al Derecho aplicable. Una segunda categoría se refiere a los efectos reales o previsibles del servicio para el ejercicio de los derechos fundamentales, tal como los protege la Carta, entre ellos, la dignidad humana, la libertad de expresión y de información, incluidos la libertad de los medios de comunicación y su pluralismo, el derecho a la vida privada, el derecho a la protección de datos, el derecho a la no discriminación, los derechos del niño y la protección de los consumidores. Estos riesgos pueden derivarse, por ejemplo, del diseño de los sistemas algorítmicos utilizados por la plataforma en línea de muy gran tamaño o el motor de búsqueda en línea de muy gran tamaño o por el uso indebido de su servicio mediante el envío de notificaciones abusivas u otros métodos destinados a limitar la expresión u obstaculizar la competencia. Al evaluar los riesgos para los derechos del niño, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben tener en cuenta, por ejemplo, cuan fácil les resulta a los menores comprender el diseño y el funcionamiento del servicio, así como la manera en que los menores pueden verse expuestos, a través de su servicio, a contenidos que puedan perjudicar su salud y su desarrollo físico, mental y moral. Tales riesgos pueden surgir, por ejemplo, con interfaces en línea que estén diseñadas de manera que exploten intencionada o involuntariamente las debilidades y la inexperiencia de los menores o que puedan generar un comportamiento adictivo. Una tercera categoría de riesgos se refiere a los efectos negativos reales o previsibles sobre

los procesos democráticos, el discurso cívico y los procesos electorales, así como sobre la seguridad pública. Una cuarta categoría de riesgos se deriva de preocupaciones similares relacionadas con el diseño, el funcionamiento o la utilización, también mediante la manipulación, de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño, con un efecto negativo real o previsible en la protección de la salud pública, los menores y graves consecuencias negativas para el bienestar físico y mental de una persona, o en la violencia de género. Estos riesgos también pueden derivarse de campañas coordinadas de desinformación relacionadas con la salud pública, o del diseño de interfaces en línea que puedan estimular adicciones comportamentales de los destinatarios del servicio. Al evaluar dichos riesgos sistémicos, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben centrarse en los sistemas u otros elementos que puedan contribuir a los riesgos, incluidos todos los sistemas algorítmicos que puedan ser pertinentes, en particular sus sistemas de recomendación y de publicidad, dedicando atención a las prácticas conexas de recogida y uso de datos. También deben evaluar si sus condiciones generales y su cumplimiento son adecuados, así como sus procesos de moderación de contenidos, herramientas técnicas y recursos asignados. Al evaluar los riesgos sistémicos identificados en el Reglamento, dichos prestadores también deben centrarse en la información que no sea ilícita, pero que contribuya a los riesgos sistémicos identificados en el Reglamento. Por consiguiente, dichos prestadores deben dedicar especial atención a cómo se utilizan sus servicios para difundir o amplificar contenidos incorrectos o engañosos, incluida la desinformación. Cuando la amplificación algorítmica de la información contribuya a los riesgos sistémicos, dichos prestadores deben reflejarlo debidamente en sus evaluaciones de riesgos. Cuando los riesgos estén localizados o existan diferencias lingüísticas, dichos prestadores también deben tenerlo en cuenta en sus evaluaciones de riesgos. Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben evaluar, en particular, cómo contribuyen a tales riesgos el diseño y el funcionamiento de su servicio, así como la manipulación intencionada y, a menudo, coordinada y el uso de sus servicios, o la infracción sistémica de sus condiciones generales de servicio. Estos riesgos pueden derivarse, por ejemplo, del uso no auténtico del servicio, como la creación de cuentas falsas, el uso de bots o el uso engañoso de un servicio, y otros comportamientos total o parcialmente automatizados, que pueden dar lugar a la difusión rápida y extendida de información al público que sea un contenido ilícito o incompatible con las condiciones generales de una plataforma en línea o un motor de búsqueda en línea y que contribuya a campañas de desinformación. Con el fin de hacer posible que las evaluaciones de riesgos posteriores se completen mutuamente y muestren la evolución de los riesgos detectados, así como para facilitar las investigaciones y las medidas de ejecución, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben conservar todos los documentos justificativos relativos a las evaluaciones de riesgos que hayan llevado a cabo, como la información relativa a su preparación, los datos subyacentes y los datos sobre la realización de pruebas de sus sistemas algorítmicos.

Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben desplegar los medios necesarios para reducir diligentemente los riesgos sistémicos determinados en las evaluaciones de riesgos, respetando los derechos fundamentales. Cualquier medida que se adopte debe respetar los requisitos de diligencia debida del Reglamento y ser eficaz y apropiada para reducir los riesgos sistémicos específicos detectados. Deben ser proporcionadas a la luz de la capacidad económica del prestador de la plataforma en línea de muy gran tamaño o del motor de búsqueda en línea de muy gran tamaño y de la necesidad de evitar restricciones innecesarias al uso de su servicio, teniendo debidamente en cuenta los posibles efectos negativos en dichos derechos fundamentales. Dichos prestadores deben dedicar especial atención al impacto en la libertad de expresión. Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben considerar, entre esas medidas de mitigación, por ejemplo, la adaptación de cualquier diseño, característica o funcionamiento necesario de su servicio, como el diseño de la interfaz en línea. Deben adaptar y aplicar sus condiciones generales, según sea necesario y de conformidad con las normas del Reglamento relativas a las condiciones generales. Otras medidas adecuadas podrían incluir la adaptación de sus sistemas de moderación de contenidos y procesos internos o la adaptación de sus procesos y recursos de toma de decisiones, incluido el personal de moderación de contenidos, su formación y su experiencia local. Esto afecta, en particular, a la rapidez y la calidad del tratamiento de las notificaciones. A este respecto, por ejemplo, el Código de conducta para la lucha contra la incitación ilegal al odio en internet de 2016 establece un punto de referencia para tratar notificaciones válidas para la eliminación de la incitación ilegal al odio en menos de 24 horas. Los prestadores de plataformas en línea de muy gran tamaño, en particular las utilizadas principalmente para la difusión al público de contenidos pornográficos, deben cumplir con diligencia todas sus obligaciones en virtud del Reglamento en lo que respecta a los contenidos ilícitos que constituyen ciberviolencia, incluidos los contenidos pornográficos ilícitos, especialmente en lo que se refiere a garantizar que las víctimas puedan ejercer eficazmente sus derechos en relación con contenidos que representen el intercambio no consensuado de material íntimo o manipulado mediante el tratamiento rápido de notificaciones y la retirada de dichos contenidos sin dilación indebida. Otros tipos de contenidos ilícitos pueden requerir plazos más largos o más cortos para el tratamiento de las notificaciones, que dependerán de los hechos, las circunstancias y los tipos de contenidos ilícitos de que se trate. Dichos prestadores también pueden iniciar o aumentar la cooperación con alertadores fiables y organizar sesiones de formación e intercambios con organizaciones de alertadores fiables.

Ciertamente, en el diseño las plataformas deben aplicar el principio de "por diseño y por defecto" para proteger a sectores especialmente vulnerables como menores y adolescentes; y, asimismo, promover un diseño amigable y seguro para los menores, centrado en los mismos, evitando, por un lado, interfaces manipulativas (*dark patterns* o patrones engañosos que llevan al menor a hacer clic, suscribirse o aceptar sin plena conciencia); y por otro, evitar elementos que fomenten el uso compulsivo (*scroll* infinito, recompensas constantes) o dificulten el cierre de cuentas o la modificación de ajustes de privacidad. También, deben contar con

mecanismos efectivos que detecten, reporten y retiren contenido ilícito o peligroso para menores y adolescentes (pornografía, violencia, incitación al odio, entre otros); y, poner especial atención en la eliminación de contenidos que fomenten la autolesión, trastornos alimentarios, acoso, el suicidio, etc.

Los códigos de conducta deben facilitar la accesibilidad de las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño, de conformidad con el Derecho de la Unión y nacional, a fin de facilitar su uso previsible por las personas con discapacidad. En particular, los códigos de conducta podrían garantizar que la información se presente de forma perceptible, funcional, comprensible y sólida y que los formularios y las medidas facilitados en virtud del Reglamento estén disponibles de manera fácil de localizar y accesible para las personas con discapacidad.

De ahí que, el Reglamento pretenda que las plataformas aprendan buenas prácticas unas de otras y respeten las orientaciones pertinentes para garantizar la seguridad de los usuarios jóvenes. En todo caso, el artículo 28 establece que las plataformas en línea que puedan utilizar los menores deben asegurarse de que sus servicios ofrecen un alto nivel de privacidad, seguridad y protección a los usuarios jóvenes. De ahí que, no se permita la publicidad basada en el perfil de los menores, reduciendo el riesgo de manipulación comercial, a la par que se exige una mayor transparencia en la eliminación de contenido dañino y la implementación de medidas para evitar la exposición de los menores a material inapropiado. En esencia, se prohíbe la publicidad basada en datos personales sensibles, incluida la edad, respecto de menores de edad; por lo que, las plataformas no pueden usar perfiles de éstos para elaborar anuncios personalizados.

A tal fin, es preciso garantizar la seguridad de los usuarios, especialmente los niños y los jóvenes, ante peligros y riesgos en línea, como el acoso, el hostigamiento, la información falsa, el contenido ilícito o las personas que se hacen pasar por otras. A fin de evaluar los riesgos que presenta el servicio para los usuarios jóvenes, las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño deben tener en cuenta los siguientes aspectos: si los menores pueden comprender fácilmente cómo funciona el servicio (considerando número 81); si los menores corren el riesgo de verse expuestos a contenidos que puedan perjudicar "su salud y su desarrollo físico, mental y moral" (contenido inadecuado para su edad) (considerando número 81); de qué manera pueden causar adicción las características del diseño (considerandos números 81 y 83).

Por otra parte, los menores y adolescentes deben ser conscientes que, las citadas empresas pueden recopilar información sobre nuestras preferencias e intereses en las páginas web que visitamos, saber a qué le damos cuando pulsamos "me gusta", los enlaces que seguimos, así como la información personal que proporcionamos sobre nosotros mismos, como nuestra edad o nuestro lugar de residencia. Las plataformas utilizan algoritmos e inteligencia artificial en la elaboración de perfiles a partir de los datos para decidir qué anuncios mostrarnos y tener el mayor impacto posible en cada uno de nosotros. Algunas plataformas en línea obtienen dinero cada vez que compramos productos gracias a estos anuncios. De acuerdo con el Reglamento de Servicios Digitales (artículo 28) cuando las plataformas conozcan con una seguridad razonable que un usuario es menor, no podrán mostrarle anuncios basados en los perfiles creados. Se prohíbe a todas las

plataformas mostrar anuncios personalizados a menores, especialmente, si utilizan datos como la edad, ubicación, preferencias personales o comportamiento en línea. Esta prohibición viene a reforzar el principio que los menores y adolescentes deben estar protegidos contra cualquier forma de manipulación comercial, particularmente en entornos donde desconocen cómo funcionan los algoritmos o los intereses económicos que hay detrás de los contenidos.

De ahí que, el Reglamento de Servicios Digitales (artículo 39) exija que las plataformas en línea de muy gran tamaño hagan pública la información sobre sus anuncios, de manera que cualquiera pueda analizar sus posibles riesgos, especialmente los investigadores. Esta información debe incluir, entre otras cuestiones, elementos sobre el contenido del anuncio y quién lo ha pagado, especialmente cuando se dirige a menores.

El Reglamento de Servicios Digitales también promueve normas técnicas (artículo 44) y otros acuerdos para ofrecer a los usuarios una mejor experiencia en línea. En lo que se refiere a la protección de los menores, ya se están dando los primeros pasos con el Código de conducta de la Unión Europea sobre el diseño apropiado para la edad (artículo 45).

El Reglamento de Servicios Digitales (considerando número 67) también prohíbe las "interfaces engañosas" esto es, la forma en que estas interfaces en línea están diseñadas con el objetivo de persuadir y engañar para dirigirnos a realizar cosas, que quizá no deseemos hacer, como ciertas compras; o para influir en nuestras decisiones o dificultar la cancelación de los servicios suscritos.

Ahora bien, en cuanto a las obligaciones de diligencia debida para crear un entorno en línea transparente y seguro procede señalar: en primer lugar que, los prestadores de servicios intermediarios incluirán en sus condiciones generales información sobre cualquier restricción que impongan en relación con el uso de su servicio respecto de la información proporcionada por los destinatarios del servicio. Esta información deberá incluir datos sobre cualesquiera políticas, procedimientos, medidas y herramientas empleadas para moderar los contenidos, incluidas la toma de decisiones mediante algoritmos y la revisión humana, así como sobre las normas de procedimiento de su sistema interno de gestión de reclamaciones; y se expondrá en lenguaje claro, sencillo, inteligible, accesible al usuario e inequívoco, y se hará pública en un formato fácilmente accesible y legible por máquina. Si se trata de un *servicio intermediario dirigido principalmente a menores o es utilizado predominantemente por ellos*, el prestador de dicho servicio intermediario explicará las condiciones y cualesquiera restricciones del uso del servicio de manera que los menores lo puedan comprender. Por su parte, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño facilitarán a los destinatarios de los servicios un resumen sucinto, fácilmente accesible y legible por máquina de las condiciones generales, incluidas las medidas correctivas y los mecanismos de recurso disponibles, en un lenguaje claro e inequívoco. En fin, las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño publicarán sus condiciones generales en todas las lenguas oficiales de todos los Estados miembros en los que presten sus servicios.

En segundo lugar, respecto a las obligaciones de transparencia informativa de los prestadores de servicios intermediarios publicarán en un formato legible por

máquina y de forma fácilmente accesible, al menos una vez al año, informes claros y fácilmente comprensibles sobre cualquier actividad de moderación de contenidos que hayan realizado durante el período pertinente. Esos informes incluirán, en particular, información sobre lo siguiente, según proceda: a) En el supuesto de los prestadores de servicios intermediarios, el número de órdenes recibidas de las autoridades de los Estados miembros, incluidas las órdenes dictadas de conformidad con los artículos 9 y 10 del Reglamento, categorizadas según el tipo de contenido ilícito de que se trate, el Estado miembro que haya dictado la orden y el tiempo medio necesario para informar a la autoridad que haya dictado la orden, o a cualquier otra autoridad especificada en la orden, de su recepción, y para dar curso a la orden; b) En el caso de los prestadores de servicios de alojamiento de datos, el número de notificaciones enviadas de conformidad con el artículo 16 del citado Reglamento, clasificadas según el tipo de contenido presuntamente ilícito de que se trate, el número de notificaciones enviadas por alertadores fiables, toda actuación que se haya llevado a cabo en virtud de dichas notificaciones distinguiendo si esta se hizo conforme al Derecho o a las condiciones generales del prestador, el número de notificaciones tratadas únicamente por medios automatizados y el tiempo medio necesario para adoptar medidas; c) En el caso de los prestadores de servicios intermediarios, información significativa y comprensible sobre la actividad de moderación de contenidos realizada por iniciativa propia del prestador, incluido el uso de herramientas automatizadas, las medidas adoptadas para proporcionar formación y asistencia a las personas encargadas de la moderación de contenidos, el número y el tipo de medidas adoptadas que afecten a la disponibilidad, visibilidad y accesibilidad de la información proporcionada por los destinatarios del servicio y a la capacidad de los destinatarios para proporcionar información a través del servicio, y otras restricciones conexas del servicio. La información proporcionada se clasificará según el tipo de contenido ilícito o infracción de las condiciones generales del prestador del servicio de que se trate, según el método de detección y según el tipo de restricción aplicado; d) En el caso de los prestadores de servicios intermediarios, el número de reclamaciones recibidas a través de los sistemas internos de gestión de reclamaciones de conformidad con las condiciones generales del prestador y además, para los prestadores de plataformas en línea, de conformidad con el artículo 20 del Reglamento, la base de dichas reclamaciones, las decisiones adoptadas en relación con dichas reclamaciones, el tiempo medio necesario para adoptar dichas decisiones y el número de ocasiones en que dichas decisiones fueron revocadas; e) El uso de medios automatizados con fines de moderación de contenidos, incluyendo una descripción cualitativa, una especificación de los fines precisos, los indicadores de la precisión y la posible tasa de error de los medios automatizados empleados para cumplir dichos fines, y las salvaguardias aplicadas.

En tercer lugar, respecto a la obligación de transparencia en los sistemas de recomendación, los prestadores de plataformas en línea que utilicen tales sistemas de recomendación deberán establecer en sus condiciones generales, utilizando un lenguaje claro y comprensible, los parámetros principales utilizados en sus sistemas de recomendación, así como cualquier opción a disposición de los destinatarios del servicio para modificar o influir en dichos parámetros principales. Estos parámetros incluirán, como mínimo: a) Los criterios más significativos a la

hora de determinar la información sugerida al destinatario del servicio; y b) Las razones de la importancia relativa de dichos parámetros.

En cuarto lugar, en cuanto a la transparencia adicional sobre la publicidad en línea, los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda en línea de muy gran tamaño que presenten anuncios publicitarios en sus interfaces en línea deberán recopilar y hacer público, en una sección específica de su interfaz en línea, a través de una herramienta de búsqueda fiable que permita realizar consultas en función de múltiples criterios, y mediante interfaces de programación de aplicaciones, un repositorio que contenga la información que a continuación se detalla, durante todo el tiempo en el que presenten un anuncio y hasta un año después de la última vez que se presente el anuncio en sus interfaces en línea. Se asegurarán de que el repositorio no contenga ningún dato personal de los destinatarios del servicio a quienes se haya o se pueda haber presentado el anuncio y harán todos los esfuerzos que resulten razonables para garantizar que la información sea exacta y completa.

Así, el repositorio incluirá al menos toda la información siguiente: a) El contenido del anuncio publicitario, incluidos el nombre del producto, servicio o marca y el objeto del anuncio; b) La persona física o jurídica en cuyo nombre se presenta el anuncio publicitario; c) La persona física o jurídica que ha pagado por el anuncio publicitario, si es diferente de la persona física o jurídica a que se refiere la letra b); d) El período durante el que se haya presentado el anuncio; e) Si el anuncio estaba destinado a presentarse en particular a uno o varios grupos concretos de destinatarios del servicio y, en tal caso, los parámetros principales utilizados para tal fin, incluidos, en su caso, los principales parámetros utilizados para excluir a uno o más de esos grupos concretos; f) Las comunicaciones comerciales publicadas en las plataformas en línea de muy gran tamaño e identificadas con arreglo al artículo 26, apartado 2; y, g) El número total de destinatarios del servicio alcanzados y, en su caso, el número total desglosado por Estado miembro para el grupo o grupos de destinatarios a quienes el anuncio estuviera específicamente dirigido.

Ahora bien, en cuanto a la gestión de riesgos sistémicos los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño detectarán, analizarán y evaluarán con diligencia cualquier riesgo sistémico en la Unión que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios. Esta evaluación de riesgos será específica de sus servicios y proporcionada a los riesgos sistémicos, teniendo en cuenta su gravedad y probabilidad, e incluirá los siguientes riesgos sistémicos: a) La difusión de contenido ilícito a través de sus servicios; b) Cualquier efecto negativo real o previsible para el ejercicio de los derechos fundamentales, en particular los relativos a la dignidad humana amparada por el artículo 1 de la Carta, al respeto de la vida privada y familiar amparada por el artículo 7 de la Carta, a la protección de los datos de carácter personal amparada por el artículo 8 de la Carta, a la libertad de expresión e información, incluida la libertad y el pluralismo de los medios de comunicación, amparada por el artículo 11 de la Carta, a la no discriminación amparada por el artículo 21 de la Carta, a los derechos del niño amparados por el artículo 24 de la Carta y a un nivel elevado de protección de los consumidores, amparado por el artículo 38 de la Carta; c) Cualquier efecto negativo real o previsi-

ble sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública; y, d) Cualquier efecto negativo real o previsible en relación con la violencia de género, la protección de la salud pública y los menores y las consecuencias negativas graves para el bienestar físico y mental de la persona. En todo caso, conservarán los documentos justificativos de las evaluaciones de riesgos durante al menos tres años después de la realización de las evaluaciones de riesgos y se los comunicarán, previa solicitud, a la Comisión y al coordinador de servicios digitales de establecimiento.

En este contexto, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deberán aplicar: medidas de reducción de riesgos, razonables, proporcionadas y efectivas, adaptadas a los riesgos sistémicos específicos detectados, teniendo especialmente en cuenta las consecuencias de dichas medidas sobre los derechos fundamentales. Dichas medidas podrán incluir, cuando proceda: a) La adaptación del diseño, las características o el funcionamiento de sus servicios, incluidas sus interfaces en línea; b) La adaptación de sus condiciones generales y su ejecución; c) La adaptación de los procesos de moderación de contenidos, incluida la velocidad y la calidad del tratamiento de las notificaciones relacionadas con tipos específicos de contenidos ilícitos y, en su caso, la rápida retirada de los contenidos notificados, o el bloqueo del acceso a ellos, en particular en el caso de la incitación ilegal al odio o la ciberviolencia, así como la adaptación de los procesos de toma de decisiones pertinentes y los recursos específicos para la moderación de contenidos; d) La realización de pruebas y la adaptación de sus sistemas algorítmicos, incluidos sus sistemas de recomendación; e) La adaptación de sus sistemas publicitarios y la adopción de medidas específicas dirigidas a limitar o ajustar la presentación de anuncios publicitarios en asociación con el servicio que prestan; f) El refuerzo de los procesos internos, los recursos, la realización de pruebas, la documentación o la supervisión de cualquiera de sus actividades, en particular en lo que respecta a la detección de riesgos sistémicos; g) La puesta en marcha o el ajuste de la cooperación con los alertadores fiables de conformidad con el artículo 22 y la ejecución de las decisiones de los órganos de resolución extrajudicial de litigios en virtud del artículo 21; h) La puesta en marcha o el ajuste de la cooperación con otros prestadores de plataformas en línea o motores de búsqueda en línea mediante los códigos de conducta y los protocolos de crisis a que se refieren, respectivamente, los artículos 45 y 48; i) La adopción de medidas de concienciación y la adaptación de su interfaz en línea con el fin de proporcionar más información a los destinatarios del servicio; j) La adopción de medidas específicas para proteger los derechos de los menores, incluidas herramientas de comprobación de la edad y de control parental, herramientas destinadas a ayudar a los menores a señalar abusos u obtener ayuda, según corresponda; y, k) Garantizar que un elemento de información, ya se trate de imagen, audio o vídeo generado o manipulado que se asemeja notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puede inducir erróneamente a una persona a pensar que son auténticos o verídicos, se distinga mediante indicaciones destacadas cuando se presente en sus interfaces en línea y, además, proporcionar una funcionalidad fácil de utilizar que permita a los destinatarios del servicio señalar dicha información.

En cuanto, a la evaluación y reducción de riesgos: las plataformas en línea de muy gran tamaño (como Tik Tok, Instagram, Youtube, etc) y los motores de búsqueda en línea de muy gran tamaño (Google) deben cada año determinar y evaluar los posibles riesgos en línea para los niños y los jóvenes que utilicen sus servicios (artículos 34 y 35). De la misma manera que contamos con categorías de edad en las películas en el cine, ciertos contenidos y servicios en línea resultan inadecuados en el caso de los grupos de edad más jóvenes. Por eso, las plataformas también deben poner en marcha medidas para reducir esos riesgos, como (según proceda, en función de las plataformas): 1. Controles parentales: ajustes que ayuden a los padres y personas a cargo a, por ejemplo, supervisar o limitar el acceso de los niños a internet para protegerlos de los riesgos en línea y de los contenidos inadecuados; 2. Verificación de la edad: un sistema para comprobar la edad de los usuarios antes de que accedan al servicio, basándose, por ejemplo, en identificadores físicos u otras formas de identificación. Herramientas: para que los jóvenes puedan señalar los abusos u obtener ayuda.

Las plataformas como Snapchat, Google, Youtube, Instagram y Facebook ya no permiten a los anunciantes mostrar publicidad personalizada a los menores. Por su parte, TikTok y YouTube hacen automáticamente privadas las cuentas de los usuarios menores de 16 años de forma que solo los contactos conocidos puedan ver los vídeos que cargan. Y esto es solo el principio. La Comisión dispone de nuevas competencias para evaluar las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño y las medidas que adoptan para reducir los riesgos. La Unión Europea y los Estados miembros velarán por que las empresas respeten estas normas y podrán multar a estas últimas con hasta el 6 % de sus beneficios globales anuales si no lo hacen; o que no excedan del 1 % del total de sus ingresos o volumen de negocios anuales en todo el mundo del ejercicio fiscal anterior cuando, de forma intencionada o por negligencia: a) Proporcione información incorrecta, incompleta o engañosa en respuesta a una simple solicitud o a una solicitud de conformidad con lo dispuesto en el artículo 67; b) No responda a la solicitud de información mediante decisión en el plazo establecido; c) No rectifique, en el plazo determinado por la Comisión, la información incorrecta, incompleta o engañosa proporcionada por un miembro del personal, o no proporcione o se niegue a proporcionar información completa; d) Se niegue a someterse a una inspección con arreglo al artículo 69; e) No cumpla las medidas adoptadas por la Comisión con arreglo al artículo 72; o f) No cumpla las condiciones de acceso al expediente de la Comisión con arreglo al artículo 79, apartado 4. Si bien, para fijar el importe de la multa, la Comisión tendrá en cuenta la naturaleza, gravedad, duración y recurrencia de la infracción y, en el caso de las multas impuestas de conformidad con el apartado 2, la demora causada al procedimiento[25].

De todas formas, la Comisión dispone de nuevas competencias para evaluar las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño y las medidas que adoptan para reducir los riesgos. Asimismo, la Unión Europea y los Estados miembros velarán por que las empresas respeten estas normas y podrán multar a estas últimas con hasta el 6 % de sus beneficios globales anuales si no lo hacen.

En todo caso, como analizaremos España está elaborando una futura Ley Orgánica de Protección de las Personas menores en entornos digitales que busca

reforzar aún más la seguridad y el bienestar de los jóvenes en línea. Como veremos aborda aspectos como: 1. Uso responsable de la tecnología: se fomenta un acceso equilibrado y seguro a los entornos digitales; 2. Protección contra el ciberacoso: se establecen medidas para prevenir el acoso en línea y garantizar la seguridad de menores; 3. Derechos digitales: se reconoce el derecho de los menores a una navegación segura y a recibir información clara sobre los riesgos digitales.

En fin, atendiendo a la mencionada regulación de DSA, en concreto, ante la promoción de la alfabetización digital como herramienta clave de protección los centros escolares pueden: 1. Educar sobre derechos digitales y riesgos en las redes sociales; 2. Impulsar talleres/cursos sobre verificación de edad, privacidad y consentimiento; 3. Colaborar con las familias en la detección de señales de daño digital. Ente la exigencia de que las plataformas ofrezcan configuraciones seguras y comprensibles para menores y adolescentes que promueve el citado DSA, los padres/tutores deben llevar a cabo como acciones posibles: 1. Activar controles parentales y restricciones de tiempo; 2. Revisar el diseño de las apps utilizadas por los hijos, por si se diera el caso, que pudiesen crear adicción; 3. Denunciar contenido perjudicial.

Por otra parte, se impone a los Estado miembros designar un Coordinador de Servicios Digitales (*Digital Services Coordinators* —DSC—) encargado de verificar que se cumple el Reglamento. De ahí que los Gobiernos nacionales (autoridades digitales) a través del DSC deban: 1. Supervisar el cumplimiento del DSA; 2. Exigir auditorias de riesgos a las plataformas n línea de gran tamaño y motores de búsqueda; 3. Apoyar y promover campañas públicas, público-privadas sobre seguridad digital infantil; 4. Ordenar la eliminación del contenido o prácticas ilegales, nocivas y peligrosos; 5. Imponer multas de hasta el 6% del volumen global del negocio de una plataforma

En todo caso, ante la obligación directa del DSA a las plataformas grandes y medianas que operan en la Unión Europea. Deben: 1. Implementar mecanismo de verificación de edad confiables; 2. Desactivar anuncios personalizados para menores; 3. Realizar auditorías de impacto sobre los derechos de los menores y adolescentes.

Y, los menores y adolescentes deben tener también un papel activo. Como bien sabemos, el DSA incluye múltiples disposiciones explícitas e implícitas que buscan proteger a los menores y adolescentes frente a los riesgos digitales —desinformación, acoso, exposición a contenidos nocivos y dañinos y la explotación comercial—. Así deben denunciar contenido o perfiles dañinos o peligrosos; usar cuentas privadas y revisar las configuraciones de privacidad; y conocer sus derechos digitales, entre otros, el derecho a no ser perfilado con fines comerciales.

Recordemos que este Reglamento se complementa con el RGPD, con el RIA, con el artículo 24 de la Carta de Derecho Fundamentales de la Unión Europea y Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual (AVMSD).

Antes de realizar un breve análisis de la citada norma, señalar que la Comisión Europea publicó en 2013 el Libro Verde titulado "Preparación para la plena convergencia del mundo audiovisual: Crecimiento, creación y valores", en el que constataba que los servicios de comunicación audiovisual estaban convergiendo y que el modo de ofertar y consumir estos servicios estaba cambiando rápidamente en función de los avances tecnológicos.

Con el fin de actualizar el marco normativo bajo el ámbito de la "Estrategia para el Mercado Único Digital de Europa" aprobada el 6 de mayo de 2015, la Comisión Europea, asimismo, publicó el 25 de mayo de 2016 una propuesta legislativa para modificar la citada Directiva 2010/13/UE. Las negociaciones interinstitucionales tripartitas sobre la nueva redacción concluyeron el 6 de junio de 2018. El Pleno del Parlamento Europeo dio su apoyo a las nuevas normas el 2 de octubre de 2018 y, finalmente, el 6 de noviembre de 2018, el Consejo de Ministros Europeo votó la adopción de la Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual, habida cuenta de la evolución de las realidades del mercado. La Directiva 2018/1808, que esta Ley 13/2022 incorpora al ordenamiento jurídico español, fue publicada en el Diario Oficial de la Unión Europea el 28 de noviembre de 2018. Las principales innovaciones que la norma de la Unión Europea introduce en el ordenamiento jurídico son las siguientes: a) La modificación del límite cuantitativo respecto de la emisión de comunicaciones comerciales audiovisuales, que pasa de ser el veinte por ciento por hora a ser el veinte por ciento del tiempo entre las 6:00 y las 18:00 y el veinte por ciento del tiempo entre las 18:00 y las 24:00; b) La protección de los menores frente a los contenidos perjudiciales, aplicándose la misma regulación tanto a los servicios de radiodifusión tradicionales como a los servicios a petición; c) La extensión de las disposiciones aplicables a las obras europeas a los prestadores del servicio de comunicación audiovisual a petición, que deben velar por que las obras europeas representen, como mínimo, el treinta por ciento de sus catálogos y conferirles la prominencia que merecen; y d) La inclusión de los servicios de intercambio de vídeos a través de plataforma en el ámbito de la Directiva de servicios de comunicación audiovisual, con el fin de garantizar la protección de los menores frente a los contenidos perjudiciales también en ese entorno, así como proteger a los espectadores en general de contenidos que inciten a la violencia o al odio o bien que constituyan una provocación pública a la comisión de un delito de terrorismo.

Pues bien, tras referirse en su artículo 10 a la alfabetización mediática —la autoridad audiovisual competente, los prestadores del servicio de comunicación audiovisual, los prestadores del servicio de comunicación audiovisual comunitario sin ánimo de lucro y los prestadores del servicio de intercambio de vídeos a través de plataforma, en cooperación con todas las partes interesadas, incluidas las organizaciones, asociaciones, colegios y sindicatos profesionales del ámbito de la comunicación y el periodismo, adoptarán medidas para la adquisición y el desarrollo de las capacidades de alfabetización mediática en todos los sectores de la sociedad, para los ciudadanos de todas las edades y para todos los medios, y evaluarán periódicamente los avances realizados—; a la necesidad de aprobación de Código de conducta de autorregulación y corregulación (artículo 15); al tratamiento de datos personales de los menores recogidos o generados de otro modo por prestadores del servicio de intercambio de vídeos a través de plataforma de conformidad no podrán ser tratados con fines comerciales, como mercadotecnia directa, elaboración de perfiles o publicidad personalizada basada en el comportamiento (artículo 90); dedica el título VI de la Ley a las obligaciones de los ser-

vicios de comunicación audiovisual televisivos, tanto lineales como a petición. En concreto, el capítulo I se refiere a la protección de los menores, estableciendo obligaciones para la adecuada protección de los menores tanto en la forma en la que aparecen representados en los servicios de comunicación audiovisual televisivos, como en el uso que hacen de los servicios de comunicación audiovisual televisivos, en consonancia con la regulación contenida en el capítulo VIII del título III, relativo a las nuevas tecnologías, de la LOPIVI. Se incluye una referencia a los servicios de intercambio de vídeos a través de plataforma con el fin de prever que dichos servicios en España puedan sumarse a los acuerdos de corregulación que se adopten para garantizar una única descripción, señalización y recomendación por edades de los contenidos audiovisuales[26]; la calificación de programas audiovisuales (artículo 98)[27]; y en cuanto a los contenidos perjudiciales para el desarrollo físico, mental o moral de los menores: todos los prestadores del servicio de comunicación audiovisual televisivo lineal, abierto y de acceso condicional, y del servicio de comunicación audiovisual televisivo a petición tienen la obligación de facilitar a los usuarios información suficiente e inequívoca acerca de la naturaleza potencialmente perjudicial para el desarrollo físico, mental o moral de los menores de los programas y contenidos audiovisuales mediante la utilización de un sistema de descripción del contenido, advertencia acústica, símbolo visual o cualquier otro medio técnico que describa la naturaleza del contenido (artículo 99.1)[28]. Se incluyen, asimismo, los derechos de los menores en el ámbito audiovisual: los menores tienen derecho a que su imagen y su voz no se utilicen en los servicios de comunicación audiovisual sin su consentimiento o el de su representante legal, de acuerdo con la normativa vigente; también, está prohibida la difusión del nombre, la imagen u otros datos que permitan la identificación de los menores en el contexto de hechos delictivos, de emisiones en las que se discuta su tutela o filiación, o relativas a situaciones en las que menores hayan sido víctimas de violencia en cualquiera de sus manifestaciones; y, respecto a los datos personales de menores recogidos o generados de otro modo por prestadores del servicio de comunicación audiovisual televisivo de conformidad con lo previsto en este Capítulo no podrán ser tratados con fines comerciales, como mercadotecnia directa, elaboración de perfiles o publicidad personalizada basada en el comportamiento. Sin perjuicio de lo anterior, en todo caso el tratamiento de datos de menores quedará sometido a lo previsto en la normativa de protección de datos y, en particular, en lo establecido en el artículo 8 del RGPD, y al artículo 7 de la LOPDYGDD (artículo 95).

Y, el capítulo II, relativo a la accesibilidad de los servicios de comunicación audiovisual televisivos, regula las obligaciones de garantizar que se mejore de forma continua y progresiva la accesibilidad de los servicios para las personas con discapacidad. Como novedades destacan la introducción de requerimientos de calidad de las herramientas de accesibilidad y la consideración del Centro Español del Subtitulado y la Audiodescripción y del Centro de Normalización Lingüística de la Lengua de Signos Española como centros estatales técnicos de referencia en materia de accesibilidad audiovisual para personas con discapacidad (artículos 101 a 109).

La Comisión Europea ha presentado el 14 de julio de 2025 las Directrices sobre la protección de los menores y un prototipo de aplicación de verificación de la

edad (Guidelines on measures to ensure a high level of privacy, safety and security for minors on line, pursuant to Article 28 (4) of Regulation (EU) 2022/2065).

Estas Directrices garantizan que los niños dispongan de altos niveles de privacidad, seguridad y protección en las plataformas en línea. Esto está al día de hoy en un período de consulta amplio e inclusivo.

Entre otras medidas, las Directrices ofrecen recomendaciones para abordar: 1. El diiseño adictivo; 2. El ciberacoso; 3. El contenido nocivo; y 4. El contacto no deseado de extraños: en este ámbito, las directrices recomiendan que las plataformas establezcan cuentas de menores que sean privadas por defecto, es decir, que no sean visibles para los usuarios que no figuren en la lista de amigos, a fin de minimizar el riesgo que extraños se pongan en contacto con ellos en línea.

Las Directrices, asimismo, adoptan un enfoque basado en el riesgo, como hace la Ley de Servicios Digitales, que reconoce que las plataformas en línea pueden plantear diferentes tipos de riesgos para los menores, en función de su naturaleza, tamaños, finalidad y base de usuarios. En todo caso, las plataformas deben asegurarse que las medidas que se adopten, sean adecuadas y no restrinjan de manera desproporcionada o indebida los derechos de los niños.

Ahora bien, el prototipo de la aplicación de verificación de la edad resulta fácil de usar y proteger la privacidad estableciendo un "estándar de oro" en la garantía de edad en línea. Permitirá, por ejemplo, a los usuarios demostrar fácilmente que son mayores de 18 años cuando accedan a contenido restringido para adultos en línea, mientras mantienen el control total de cualquier otra información personal, como la edad o identidad exacta de un usuario. al respecto, nadie sería capaz de rastrear, ver o reconstruir qué contenido están consultando lo usuarios individuales.

En cuanto a la aplicación de verificación se probará y personalizará en colaboración con los Estados miembros, las plataformas en línea y los usuarios finales. En todo caso, las Directrices sobre la protección de los menores describen cuándo y cómo las plataformas deben comprobar la edad de sus usuarios. Igualmente, recomiendan la verificación de la edad para las plataformas de contenido para adultos y otras plataformas, que plantean altos riesgos para la seguridad de los menores. Especifican que los métodos de garantía de la edad deben ser precisos, fiables, sólidos, no intrusivos y no discriminatorios.

En fin, las Directrices y el plan de verificación de la edad tienen su base en los debates del grupo de trabajo sobre la protección de los menores, que forma parte del Comité Europeo de Servicios Digitales.

III. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: DERECHOS Y CONSENTIMIENTO DE LOS MENORES Y ADOLESCENTES.

3.1. En torno al contenido del Reglamento General de Protección de Datos.

Se establecen definiciones y conceptos marco, fundamentalmente en su artículo 4 y, sin dejar de remitir a dicho artículo, algunos de ellos los desarrollamos a continuación que son especialmente interesantes con relación a la IA. El artículo 1 del RGPD se refiere al objeto de la norma como es: la protección de derechos y

libertades fundamentales de las personas físicas, en particular con relación a la protección de datos de carácter personal.

El dato personal se define en el artículo 4.1 del RGPD como "toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

La seudonimización se conceptúa en el artículo 4.5 del RGPD como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable". La anonimización es el proceso que permite eliminar o reducir al mínimo los riesgos de reidentificación de un individuo a partir de sus datos personales eliminando toda referencia directa o indirecta a su identidad, pero manteniendo la veracidad de los resultados del tratamiento de los mismos. Es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

Las categorías especiales de datos se establecen en el artículo 9 del RGPD como aquellos datos que "que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos; datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física". El RGPD establece en dicho artículo la prohibición genérica a su tratamiento, prohibición que se amplía en el también artículo 9 de la LOPDGDD, salvo que se den una serie de circunstancias detalladas en los apartados 2, 3 y 4 del artículo 9 del RGPD y los apartados 1 y 2 del artículo 9 de la LOPDGDD.

En cuanto al tratamiento lo define el artículo 4.2 del RGPD: como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

La elaboración de perfiles y la toma de una decisión sobre una persona física son tratamientos según los Considerandos 24 y 72 del RGPD.

Así, el artículo 4.4 del RGPD define perfilado como una forma de tratamiento de datos personales que permite inferir más información acerca de una persona física, evaluando, analizando o prediciendo aspectos personales. Un tratamiento que implique la elaboración de perfiles se caracteriza por tres elementos: 1. Debe ser una forma automatizada de tratamiento, incluyendo aquellos tratamientos que tienen participación parcialmente humana; 2. Debe llevarse a cabo respecto

a datos personales; y, 3. El objetivo de la elaboración de perfiles debe ser evaluar aspectos personales sobre una persona física.

En cuanto a las decisiones automatizadas son las basadas únicamente en el tratamiento automatizado representan la capacidad de tomar decisiones por medios tecnológicos sin la participación del ser humano. El RGPD, en sus Considerandos 71 y 72 así como en su artículo 22 limita y establece derechos con relación a que los sujetos de los datos no sean sometidos a decisiones exclusivamente automatizadas, que tengan efectos jurídicos o que afecten significativamente al interesado. La elaboración de perfiles de forma automática se incluye en este marco de decisiones automatizadas

No obstante, ha de tenerse en cuenta que las decisiones automatizadas pueden llevarse a cabo con o sin elaboración de perfiles y la elaboración de perfiles puede darse sin realizar decisiones automatizadas.

Respecto a la figura de responsable de un tratamiento se define en el artículo 4.7 del RGPD como la persona que determine los fines y medios del tratamiento, y el ámbito de sus obligaciones, que se enmarcan en el artículo 24, incluye, entre otras, la de "aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento". También el RGPD introduce la figura del corresponsable del tratamiento en el artículo 26: como aquellos responsables (dos o más) que determinen conjuntamente los objetivos y los medios del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD; y del encargado del tratamiento como aquella persona que trate datos personales por cuenta del responsable, tal como se establece en el artículo 4.8 del RGPD, y el ámbito de sus obligaciones, que se enmarcan en el artículo 28, contempla, entre otras, que su relación con el responsable "se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable". En todo caso, en la necesaria interrelación entre RGPD y RIA los responsables del despliegue de SIAs, como indica JIMÉNEZ LÓPEZ "deben desplegar una especial diligencia, de manera que adopten las medidas necesarias, en su caso contractuales, para asegurar el cumplimiento del RGPD en el contexto de ciclo de vida y al cadena de valor, enervando por tanto el riesgo que supone la integración n mismos servicios no conformes con la norma, no sujetos a rendición de cuentas o carentes de documentación necesaria, pudiendo determinar incluso la no integración del servicio"[29].

Tras las consideraciones realizadas, de forma breve, el RGPD se desarrolla en 6 principios establecidos en el Capítulo II: 1. Licitud, lealtad y transparencia 2. Limitación de la finalidad (especificación del propósito) 3. Minimización de datos 4. Exactitud 5. Limitación del plazo de conservación 6. Integridad y confidencialidad En el mismo capítulo se establecen las condiciones para que un tratamiento de datos personales sea legítimo.

En el Capítulo III se establecen el conjunto de derechos que asisten a los sujetos de los datos, la obligación de garantizarlos y de implementar mecanismos efectivos para el ejercicio de estos, en particular los derechos de transparencia, información, acceso, rectificación, supresión, limitación, oposición, portabilidad y, uno más que tiene gran importancia en determinadas aplicaciones de IA como

son los derechos que tienen los ciudadanos con relación a la toma de decisiones automatizadas.

En el Capítulo IV se establece el modelo de responsabilidad y cumplimiento establecido basado en la "accountability", o responsabilidad proactiva, y cuyos elementos rectores son: 1. La identificación de una responsabilidad en el tratamiento; 2. El análisis del riesgo para los derechos y libertades; 3. El estudio de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; y, 4. El despliegue de medidas para la gestión del riesgo, medidas de privacidad por defecto y desde diseño, medidas de seguridad, de gestión de incidentes, etc.

Para terminar este breve resumen del contenido del RGPD, en el Capítulo V se establecen las condiciones para la ejecución de transferencias de datos personales a terceros países u organizaciones internacionales.

Con posterioridad a este RGPD la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital de 2023, proclamada por el Parlamento Europeo, el Consejo y la Comisión establece el derecho de todas las personas a acceder a tecnologías, productos y servicios digitales que sean seguros y protejan la privacidad desde el diseño. Esto incluye velar por que se ofrezca a todas las personas que viven en la Unión una identidad digital accesible, segura y fiable que permita acceder a una amplia gama de servicios en línea y fuera de línea, protegida contra los riesgos de ciberseguridad y los ciberdelitos, por ejemplo, la violación de la seguridad de los datos y la usurpación o la manipulación de identidad. En la Declaración también se afirma que toda persona tiene derecho a la protección de sus datos personales. Este derecho incluye el control de cómo se utilizan esos datos y con quién se comparten; y, el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024 por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento elDAS2) define las condiciones armonizadas de cara al establecimiento de un marco para las carteras europeas de identidad digital que deben proporcionar los Estados miembros. Todos los ciudadanos de la Unión, y los residentes en la Unión tal como se definen en el Derecho nacional, deben estar facultados para solicitar, seleccionar, combinar, almacenar, eliminar, compartir y presentar datos relacionados con su identidad y solicitar la supresión de sus datos personales de una manera sencilla y cómoda que esté bajo el control exclusivo del usuario y permita al mismo tiempo la divulgación selectiva de datos personales.

Pese a la aprobación de este Reglamento no existe obligación de las redes sociales y las plataformas en línea la obligación de autentificación de la edad mediante un sistema de identidad digital[30].

3.2. Derechos del interesado (titular de los datos personales) en el Reglamento de Protección de Datos (los conocidos como derechos ARCO).

La normativa de protección de datos permite a todo ciudadano de la Unión Europea ejercer ante el responsable del tratamiento los derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento,

portabilidad y de no ser objeto de decisiones individualizadas reconocidos en el RGPD (artículos 13 a 22) —y, asimismo, artículos 15 a 18 de la LOPDYGDD—.

El derecho de acceso permite obtener la siguiente información: 1. Una copia de tus datos personales que son objeto del tratamiento; 2. Los fines del tratamiento; 3. Las categorías de datos personales que se traten; 4. Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular, los destinatarios en países terceros u organizaciones internacionales; 5. El plazo previsto de conservación de los datos personales, o si no es posible, los criterios utilizados para determinar este plazo; 6. La existencia del derecho del interesado a solicitar al responsable: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento; 7. El derecho a presentar una reclamación ante una Autoridad de Control; 8. Cuando los datos personales no se hayan obtenido directamente de ti, cualquier información disponible sobre su origen; 9. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado; y, 10. Cuando se transfieran datos personales a un tercer país o a una organización internacional, tienes derecho a ser informado de las garantías adecuadas en las que se realizan las transferencias[31].

El derecho de rectificación: su ejercicio supone poder obtener la rectificación de tus datos personales que sean inexactos sin dilación indebida del responsable del tratamiento. Además, teniendo en cuenta los fines del tratamiento, se puede exigir el derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

El derecho de oposición implica, valga la redundancia, oponer a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos: 1. Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles: el responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones; y, 2. Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada: ejercitado, pues, este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines.

El derecho de supresión ("derecho al olvido"): se puede ejercitar este derecho ante la persona responsable solicitando la supresión de sus datos de carácter personal cuando concurra alguna de las siguientes circunstancias: 1. Si tus datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; 2. Si el tratamiento de tus datos personales se ha basado en el consentimiento que prestaste a la persona responsable, y retiras el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime; 3. Si te has opuesto al tratamiento de tus datos personales al ejercitar el derecho de oposición en las siguientes circunstancias: a) El tratamiento de la persona responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de tus datos; b) A que tus datos personales sean objeto de mer-

cadotecnia directa, incluyendo la elaboración perfiles relacionada con la citada mercadotecnia; 4. Si tus datos personales han sido tratados ilícitamente; 5. Si tus datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique a la persona responsable del tratamiento; y, 6. Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información)[32].

Ahora bien, el RGPD al regular este derecho lo relaciona con el "derecho al olvido"; de forma que, este derecho de supresión se amplíe de tal forma que la persona responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. No obstante, este derecho no es ilimitado, de tal forma que puede ser factible no proceder a la supresión cuando el tratamiento sea necesario para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la persona responsable, por razones de interés público, en el ámbito de la salud pública, con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

Por su parte, la LOPDYGDD en su artículo 94 regula el derecho al olvido en servicios de redes sociales y servicios de la sociedad de la información, permitiendo la supresión de datos personales publicados por el propio menor o por terceros durante su minoría de edad. Este derecho permite solicitar la supresión de datos personales publicados por el propio menor o por terceros durante su minoría de edad. Así se aplicará en los supuestos en que un menor haya publicado información personal en redes sociales o en otros servicios online, y luego desee suprimirla por diferentes motivos, como por ejemplo, porque la información ya no es relevante o porque considera que es inapropiada.

El derecho a la limitación del tratamiento: este nuevo derecho consiste en que obtengas la limitación del tratamiento de tus datos que realiza el responsable, si bien su ejercicio presenta dos vertientes: 1. Se puede solicitar la suspensión del tratamiento de tus datos: a) Cuando se impugne la exactitud de tus datos personales, durante un plazo que permita al responsable su verificación; b) Cuando se haya opuesto al tratamiento de tus datos personales que el responsable realiza en base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los tuyos; 2. Solicitar al responsable la conservación tus datos: a) Cuando el tratamiento sea ilícito y te has opuesto a la supresión de tus datos y en su lugar solicitas la limitación de su uso; y, b) Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones[33].

El derecho a la portabilidad de los datos: la finalidad de este nuevo derecho es reforzar aún más el control de tus datos personales, de forma que cuando el tratamiento se efectúe por medios automatizados, recibas tus datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable, y puedas transmitirlos a otro responsable del tratamiento, siempre que el tratamiento

se legitime en base al consentimiento o en el marco de la ejecución de un contrato. No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable.

Derecho a no ser objeto de decisiones individuales automatizadas: este derecho pretende garantizar que cualquier persona no sea objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ti o te afecte significativamente de forma similar. Sobre esta elaboración de perfiles: puede tratarse de cualquier forma de tratamiento de tus datos personales que evalúe aspectos personales, en particular analizar o predecir aspectos relacionados con tu rendimiento en el trabajo, situación económica, salud, las preferencias o intereses personales, fiabilidad o el comportamiento. No obstante, este derecho no será aplicable cuando: 1. Sea necesario para la celebración o ejecución de un contrato entre la persona titular de los datos y el responsable; 2. El tratamiento de tus datos se fundamente en tu consentimiento prestado previamente; y, 3. Esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado. A su vez, estas excepciones no se aplicarán sobre las categorías especiales de datos (artículo 9.1), salvo que se aplique el artículo 9.2.letra a) o g) y se hayan tomado las medidas adecuadas citadas en el párrafo anterior.

Derecho a la información: Cuando se recaban datos de carácter personal por el responsable del tratamiento debe cumplir con el derecho de información. Para dar cumplimiento a este derecho, la AEPD recomienda que esta información se te facilite por capas o niveles de manera que: 1. Se facilite una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan tus datos personales. 2. y, por otra parte, se remita el resto de las información, en un medio más adecuado para su presentación, compresión y, si se desea, archivo. La información a facilitar por capas o niveles sería la siguiente: 1ª Capa: Información básica (resumida): a) La identidad del responsable del tratamiento; b) Una descripción sencilla de los fines del tratamiento, incluyendo la elaboración de perfiles si existiese; c) La base jurídica del tratamiento; d) Previsión o no de cesiones. Previsión o no de transferencias a terceros países; y, e) Referencia al ejercicio de derechos. 2ª Capa: Información adicional (detallada): a) Datos de contacto del responsable. Identidad y datos del representante (si existiese). Datos de contacto del delegado de protección de datos (si existiese); b) Descripción ampliada de los fines del tratamiento. Plazos o criterios de conservación de los datos. Decisiones automatizadas, perfiles y lógica aplicada; c) Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo. Obligación o no de facilitar datos y consecuencias de no hacerlo; d) Destinatarios o categorías de destinatarios. Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables; e) Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de los datos, y la limitación u oposición a su tratamiento; f) Derecho a retirar el consentimiento prestado; y g) Derecho a reclamar ante la Autoridad de Control.

Estos derechos se caracterizan por lo siguiente: 1. Su ejercicio es gratuito; 2. Si las solicitudes son manifiestamente infundadas o excesivas (p. ej., carácter

repetitivo) el responsable podrá: a) Cobrar un canon proporcional a los costes administrativos soportados; y, b) Negarse a actuar; 3. Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más; 4. El responsable está obligado a informar sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio; 5. Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo; 6. Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control; 7. Se puede ejercer los derechos directamente o por medio de un representante legal o voluntario; y, 8. Cabe la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule.

En todo caso, el Marco de Privacidad de Datos UE-EE.UU. (EU-US Data Privacy Framework) garantiza a los particulares que sus datos personales se transmitan de forma segura a EE.UU. con un nivel de protección equivalente al que confiere el RGPD.

3.3. El consentimiento de menores de edad en el Reglamento General de Protección de datos y la Ley Orgánica 3/2018, de Protección de Datos y Garantía de Derechos Digitales.

El consentimiento de las personas físicas titulares de los datos personales representa una de las seis bases jurídicas para el tratamiento de datos personales que se enumeran en el artículo 6.1 del Reglamento y que determina la licitud del tratamiento. Asimismo, es una herramienta que posibilita a los interesados el control sobre sus datos personales y, en consecuencia, una capacidad de decisión y elección con respecto a si quiere que se traten o no sus datos. El papel fundamental del consentimiento está indicado en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Supone una herramienta que, permite a los interesados el control sobre sus datos personales van a ser o no tratados y, asimismo, su obtención no niega o disminuye en modo alguno la obligación del responsable del tratamiento de respetar los principios del tratamiento establecido en el Reglamento —en particular, los principios de lealtad, necesidad y proporcionalidad, así como la calidad de los datos (artículo 5)—. Se define en el artículo 4.11 como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Igual definición se contiene en el artículo 6.1 de la Ley Orgánica 3/2018 de Protección de Datos al disponer que "1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Este concepto básico que,

se contienen en ambas normas, es similar al establecido en la derogada Directiva 95/46/CEE que en su artículo 7 letra a) conceptuaba el consentimiento como "toda manifestación de voluntad libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan, que debe ser otorgado "de forma inequívoca" con el fin que el tratamiento de los datos sea legítimo".

Asimismo, se indica en el citado artículo 4 apartado 11 del Reglamento que, éste deberá ser "libre, específico, informado e inequívoco y el responsable del tratamiento de datos deberá probar que el "titular consistió el tratamiento de sus datos". Por tanto, lo elementos de un consentimiento válido son que la manifestación de voluntad que el interesado sea: libre, específica, informada e inequívoca, por la que el interesado acepta ya mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. El término manifestación de voluntad libre supone elección y control real por parte del interesado de sus datos y que no haya un vicio que lo invalide. Si el interesado no puede elegir libremente, o se siente obligado a dar el consentimiento, o, en fin, sufre consecuencias negativas, si no lo da, el consentimiento no será válido[34].

El considerando número 43 del Reglamento dispone que "para garantizar que el consentimiento se ha dado libremente, este no debe constituir fundamento jurídico valido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya prestado libremente en todas las circunstancias de dicha situación particular". De forma que, en este caso puede haber otras bases jurídicas que, sean más adecuadas para fundamentar el tratamiento de datos por las autoridades públicas como las previstas en el artículo 6.1 letra c) del citado Reglamento "para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"; o letra e) "para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento". Además, señala el considerando número 32 que "el consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos". Por lo que, si el responsable del tratamiento opera sobre varios fines para el tratamiento, y no ha intentado obtener el consentimiento para cada fin por separado, no puede considerarse que se haya prestado el consentimiento libre para todos los fines.

El consentimiento no es libre, si se causa perjuicio al interesado por el responsable del tratamiento. Perjuicio que, puede derivar, bien del engaño, intimidación, coerción o consecuencias negativas si un interesado no da su consentimiento, bien del coste que puede tener para el interesado, si se niega o retira el consentimiento. Por tanto, el responsable ha de demostrar que, el interesado prestó el consentimiento sin ningún tipo de vicio, y que puede negarse a prestarlo o retirarlo sin coste añadido, ni perjuicio alguno. El considerando número 42 del Reglamento señala, precisamente, que "el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno".

Otro de los requisitos del consentimiento es que, éste debe ser informado. El principio de transparencia relacionado con el de lealtad y licitud exige que, se facilite información a los interesados antes de obtener su consentimiento y resulta esencial para que el interesado pueda tomar decisiones informadas, comprenda lo que está autorizando. Si el responsable no proporciona información accesible, el consentimiento no constituirá una base válida para el tratamiento de los datos.

Esta información se debe facilitar, como hemos señalado, en un lenguaje claro y sencillo, esto es, debe ser comprensible para el ciudadano medio y sobre todo para los menores atendiendo a su grado de madurez y desarrollo. De conformidad, con el considerando número 32 del Reglamento, si el consentimiento se solicita por medios electrónicos, la información se podrá también facilitar de esta forma.

En fin, el consentimiento debe ser inequívoco esto es, aquel que se ha prestado mediante una manifestación del interesado mediante una clara acción afirmativa[35]. A tal fin, los responsables del tratamiento deben diseñar unos mecanismos claros para la prestación de consentimiento y garantizar que la acción mediante la que se presta el consentimiento se diferencia de otras acciones. En cualquier caso, el consentimiento siempre debe obtenerse antes que el responsable del tratamiento empieza a tratar los datos personales para los que se requiere el consentimiento.

Ahora bien, el consentimiento, además de inequívoco, debe ser explícito cuando se traten datos especialmente sensibles (artículo 9.2 a)); en caso de adopción de decisiones automatizadas, incluida la elaboración de perfiles (artículo 22), y en la transferencia internacional de datos (artículo 49.1 a) del Reglamento); y representan un supuesto de licitud o legitimidad del tratamiento de los datos personales (artículo 6.1 a) del Reglamento). De forma que, el consentimiento explícito se requiere en determinadas situaciones en las que existe un grave riesgo en la protección de los datos y se considera adecuado que, exista un mayor nivel de control sobre los datos personales. Además, se refiere a la manera en que el interesado expresa el consentimiento. Se requiere que el interesado realice una declaración expresa del consentimiento, lo que puede tener lugar mediante una declaración escrita o por vía electrónica —correo electrónico—, o mediante declaración verbales, si bien en todos los supuestos se requiere que el responsable pueda demostrar que se cumplieron todas las condiciones para el consentimiento explícito válido[36].

Centrándonos en el consentimiento de menores de edad, el artículo 8 del Reglamento dispone que: *"1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. 2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible. 3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño"*[37]. Por su parte, en esta línea,

el citado considerando número 38 del RGPD pone de manifiesto que "los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños"[38]. En todo caso, se posibilita a los Estado miembros establecer por ley una edad por debajo de los dieciséis, si bien nunca inferior a trece años. En la antigua regulación de protección de datos, el artículo 13.1 del drogado Real Decreto 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 d protección de datos de carácter personal establecía la edad de 14 años, por lo que se cumpliría con el parámetro legal fijado. La misma edad se establece en el artículo 7.1 de la LOPDYGDD al disponer que: "El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años" y añade el citado precepto que "Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento". La información que se facilita al menor ha de ser comprensible y proporcionarse en un lenguaje claro y sencillo con el fin de obtener el consentimiento informado[39]. El artículo 8 se aplica cuando el tratamiento esté relacionado con los servicios de la sociedad de la información —aunque no se excluye su aplicación a otros supuestos—[40] y, son ofrecidos directamente a los niños y, además que el tratamiento se base en su consentimiento[41]. Se opta en la LOPDYGDD, al igual que, el RGPD, por el criterio de la edad —presumiendo que el menor tiene capacidad natural para ello— y no por el de suficiente madurez contenido en el artículo 162.1 del Código Civil y en el artículo 3.1 de la Ley Orgánica 1/1982, de 5 de mayo de protección civil del derecho al honor, intimidad personal y familiar y a la propia imagen, para determinar la capacidad de los menores para consentir sobre el tratamiento de sus datos[42]. No obstante, no faltan quienes consideran que, atendiendo a una interpretación conjunta de los artículos 8.1 del Reglamento y 7 de la Ley Orgánica y el artículo 162.1 del Código Civil, también los menores de 14 años que, dispongan de suficiente madurez al respecto, podrán consentir[43]. Ciertamente, hay actos que los hijos menores de edad pueden realizar por si solos, bien porque la ley directamente les atribuye la posibilidad de ejercitarlos (derechos de la personalidad —artículo 162 del Código Civil—), o bien se fija una determinada edad para llevarlos a cabo, o, en fin, se lo permiten sus condiciones de madurez (actos de la vida corriente —artículo 1263 del Código Civil—). También hay actos de los hijos menores que, solo pueden realizar los padres como sus representantes legales, o pueden ser realizados por aquellos con el complemento o asistencia de sus padres[44]. En todo caso, el artículo 3.1 de la Ley Orgánica 1/1982 permite que, los menores puedan consentir la intromisión en sus derechos al honor, intimidad personal y la propia imagen, si sus condiciones de madurez lo permiten conforme a la legislación y el artículo 4.1 de la citada norma al regular las intromisiones

ilegítimas en tales derechos mediante la difusión de información o utilización de la imagen de menores en medios de comunicación, se puede considerar como tales las que supongan un menoscabo en su honor o reputación o sean contrarias a sus intereses "incluso si consta el consentimiento del menor o sus representantes legales" (artículo 4.3). Por lo que, sin perjuicio de las acciones de las que sean titulares los representantes legales, corresponde al Ministerio Fiscal su ejercicio que puede actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física o jurídica o entidad pública[45]. En cualquier caso, el menor tiene derecho a ser oído y escuchado tanto en el ámbito familiar como en cualquier procedimiento administrativo, judicial o de mediación en que esté afectado y que conduzca a una decisión que incida en su esfera personal, familiar o social, teniéndose debidamente en cuenta sus opiniones en función de su edad y madurez. La madurez habrá de valorarse por personal especializado, atendiendo tanto a su desarrollo evolutivo como a su capacidad para comprender y evaluar el asunto concreto a tratar en cada caso. Se considera, no obstante que, tiene suficiente madurez cuando tenga doce años cumplidos. El menor puede expresar su opinión verbalmente o a través de formas no verbales de comunicación (artículo 9.1 y 2 de la Ley Orgánica 1/1996)[46]. Por lo que, sobre tal base legal el menor podrá ser oído a partir de los doce años por las autoridades competentes, incluidas las autoridades de protección de datos, si tiene suficiente madurez. En todo caso, recordemos que, hay una excepción al consentimiento del menor mayor de catorce años para el tratamiento de sus datos, cuando la ley exija la asistencia de los titulares de la patria potestad o la tutela para la celebración de un acto o negocio jurídico, debiendo éstos consentir tal tratamiento (artículo 7.1 apartado segundo de la LOPDYGDD).

En todo caso, cuando se prestan servicios de la sociedad de la información a niños sobre la base del consentimiento, el responsable debe adoptar todas las medidas precisas para verificar que, el usuario tiene la edad exigida para prestar su consentimiento digital y estas medidas deben ser proporcionales a la naturaleza y riesgos de la actividad de tratamiento. Al respecto el artículo 8.2 del RGPD establece que "el responsable del tratamiento hará los esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible". En todo caso, la verificación de edad no debe conducir a un tratamiento excesivo de datos y debe conllevar una evaluación del riesgo del tratamiento propuesto. La inteligencia artificial puede servir para verificar la identidad y la edad de una persona[47]. Por lo que, si los riesgos son bajos bastará como que indique el año de nacimiento o rellene un formulario en la que declara que son o no menores. Si hay un mayor riesgo se deberán implementar otras medidas que, quizá exijan un mayor grado de intervención y de procedimientos para comprobar la edad; en todo caso, los mecanismos de verificación de la edad serán variados atendiendo al caso concreto y a la exigencia o no de comprobaciones adicionales. No se explica que se entiende por esfuerzos razonables, en todo caso, se puede comprobar la edad de los menores, solicitándoles una copia del DNI o certificación de nacimiento[48].

Ahora bien, la patria potestad se configura como una institución en beneficio o interés superior del hijo y el respeto a su personalidad y autonomía; de ejercicio conjunto por regla general; sometida al control y vigilancia judicial y, en su caso, de la Administración Pública —ante situaciones de riesgos y desamparo—; y, con

la posibilidad de dar audiencia a los hijos menores de edad, si tuvieren suficiente madurez antes de adoptar decisiones que les afecten (artículo 154 del Código Civil)[49].

En este contexto, si estamos ante el tratamiento de los datos de los menores de catorce años, solo será lícito el consentimiento, sí consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o de la tutela (artículo 7.2 de la LOPDYGDD) sobre la base de la obligación de velar por los hijos y de representarlos que, tienen quienes ejercen la potestad parental (artículo 154.1 y 2 del Código Civil) y, en el cumplimiento de las funciones tutelares en beneficio del tutelado que corresponde a los tutores (artículo 216 del Código Civil)[50]. Todo ello sin perjuicio que, cualquier conflicto de intereses que tenga lugar en este ámbito de actuación entre los padres y su hijo menor, pueda determinar el nombramiento de un defensor judicial, salvo que, el interés opuesto solo exista con respecto a uno de los progenitores, correspondiendo al otro representar al menor o completar su capacidad (artículo 163 del Código Civil)[51], o bien la intervención judicial ante cualquier decisión parental que, resulte perjudicial para el menor (artículo 158 del Código Civil). Ahora bien, ni el RGPD, ni esta LOPDYGDD establecen cómo se obtiene el consentimiento de los padres o quien tiene derecho a realizar dicha acción. En las Directrices sobre consentimiento el GT29 recomienda la adopción de un enfoque proporcionado, en consonancia con el artículo 8 apartado 2 y el artículo 5 apartado 1 letra c) del RGPD (minimización de datos). Un enfoque proporcionado puede centrarse en obtener una cantidad limitada de información, por ejemplo, los datos de contacto de un padre o tutor[52]. De todas formas, como norma general, los responsables del tratamiento deben evitar soluciones de verificación que conlleven una excesiva recogida de datos personales[53] y articular los procedimientos que garanticen la comprobación de la edad del menor y, como señalaba, el artículo 13.4 del derogado Reglamento de desarrollo de la Ley Orgánica 15/1999 la autenticidad del consentimiento prestado por los padres o tutores. Por su parte, BRITO IZQUIERDO propone tener en cuenta los criterios de verificación del consentimiento paterno, previstos en la normativa norteamericana de protección en línea del derecho a la privacidad de los niños, más conocida como COPPA (*Children's Online Privacy Protection Act* de 1998)[54].

Ahora bien, como regla general, la patria potestad se ejerce conjuntamente, por lo que, el consentimiento para el tratamiento de los datos de los hijos menores de 14 años han de prestarlo ambos progenitores o uno solo con el consentimiento expreso o tácito del otro. Así, pues, la regla general es el ejercicio conjunto de la patria potestad, ya sea mediante la concurrencia de ambos progenitores en el acto que se trate, procurando el interés del hijo, o mediante la actuación de uno de ellos con el consentimiento expreso o tácito del otro[55]. Además se prevé que, también serán válidos los actos llevados a cabo por uno de los progenitores conforme al uso social y a las circunstancias o en situaciones de urgente necesidad —que no admiten demora—[56]. En caso de desacuerdo, cualquiera de los dos podrán acudir al Juez, quien después de oír a ambos y al hijo, si tuviera suficiente madurez y, en todo caso, si fuera mayor de doce años, atribuir la facultad de decidir al padre o a la madre —esto es, la facultad de consentir o no el tratamiento de los datos de sus hijos menores de 14 años— (desacuerdos simples u ocasionales). La intervención judicial en estos casos consiste en atribuir la facultad de decidir a uno u otro

de los progenitores, bajo el criterio del interés del menor y el hijo habrá de ser oído, si tiene suficiente madurez y, en todo caso, fuera mayor de doce años. Si los desacuerdos fueran reiterados o concurriera cualquier otra causa que entorpezca gravemente el ejercicio de la patria potestad, se podrá atribuir la facultad de decidir total o parcialmente a uno de los padres, o distribuir entre ellos las funciones, entre las que se puede encontrar el consentir el tratamiento de los datos de sus hijos menores de catorce años (artículo 156 párrafo segundo del Código Civil). Por lo que, en este caso la decisión judicial implicará o bien la atribución total del ejercicio a uno de los padres, o atribución parcial del ejercicio a uno de los padres, esto es, el ejercicio de una o varias funciones que expresamente se atribuyen; o en fin, distribuir las funciones entre los padres, de manera que cada uno de los progenitores ejerzan individualmente las que se le hubiera asignado. Si bien, respecto de las actuaciones señaladas y con el objeto de proteger a los terceros que actúan de buena fe y han confiado en la apariencia, el artículo 156 apartado 1 del Código Civil establece una presunción *iuris et de iure* que cada uno de los progenitores actúa en el ejercicio ordinario de la patria potestad con el consentimiento del otro[57]. Ahora bien, si los padres viven separados, la patria potestad se ejercerá por aquel con quien el hijo conviva; si bien, se permite al Juez a solicitud fundada del otro progenitor y, en interés del hijo atribuir al solicitante la patria potestad para que la ejerza conjuntamente con el otro progenitor o distribuir entre el padre y la madre las funciones inherentes al ejercicio (artículo 156 párrafo 5 del Código Civil). En este caso, se atribuye al progenitor que conviva con el hijo el ejercicio de la patria potestad, dejando a salvo las medidas que pueda solicitar el otro progenitor. Por otra parte, si los padres viven separados (separación de hecho) y no decidieran de común acuerdo, el juez decidirá siempre en beneficio de los hijos, al cuidado de que progenitor quedan los hijos menores de edad. No obstante, el juez oirá antes de tomar esta medida, a los hijos que tuvieran suficiente juicio y, en todo caso, a los que fueran mayores de doce años (artículo 159 del Código Civil)[58]. Si, en fin, estamos ante un supuesto de separación, nulidad o divorcio, —aunque respecto al ejercicio habrá que estar a los establecido en convenio regulador o en la sentencia judicial de separación, nulidad o divorcio (en caso de procedimiento contencioso)—, en relación a la toma de decisiones relativas al tratamiento de datos de sus hijos menores de 14 años, habrá de consentir ambos conjuntamente al ser cotitulares de la patria potestad[59]. No obstante, en caso de privación de la patria potestad por ministerio de la ley, el progenitor privado de la misma no podrá en este supuesto consentir (artículo 170 del Código Civil). Asimismo, aun siendo la regla general el ejercicio conjunto de la patria potestad, el Código Civil contempla también determinados supuestos en los que el ejercicio de la patria potestad es individual: así en el caso de defecto, ausencia o imposibilidad de uno de los padres, la patria potestad se ejercerá de forma exclusiva por el otro, único legitimado, en consecuencia, para consentir (artículo 156 apartado 4 del Código Civil)[60]. Sobre tales bases, la sentencia del Tribunal Supremo, Sala de lo Civil de 14 de febrero de 2023[61] se entiende que no hay intromisión ilegítima en la intimidad y la propia imagen de la menor por parte de la gestora de una página web en la que se publicaron dos reportajes en los que aparecían sin pixelar imágenes de una menor: el primer reportaje cuyo objeto principal era la vida de la madre con sus dos hijas durante la época de confinamiento; lo cierto es que el uso social y las circunstan-

cias amparaban la validez del consentimiento prestado por la madre y ante la falta de oposición dirigida por el padre al medio, éste pudo presumir de buena fe que la actuación de la madre no se hacía contra la voluntad del padre; segundo reportaje en el que se da cuenta de la noticia de la pérdida de la guarda custodia por parte de la madre y se incluyen fotos de la niña. El medio demandado replico el enlace a la red social de la madre, accesible y disponible en internet. De ahí que, la prestación del consentimiento por parte de la madre para la publicación de la imagen de la niña en internet conlleva el consentimiento para la difusión de esa imagen cuando tal difusión por sus características, sea una consecuencia natural del carácter accesible de los datos e imágenes publicados en internet.

En todo caso, atendiendo a que, el derecho a la propia imagen en su dimensión constitucional se configura como un derecho de la personalidad que atribuye a su titular la facultad de disponer de la representación en su aspecto físico que permita su identificación (artículo 18.1 de la CE), y que la representación fotográfica de un menor constituye un dato de carácter personal, hay una tendencia actual socialmente aceptada por algunos padres de publicar constantemente imágenes de sus hijos menores en diferentes situaciones en redes sociales (Facebook, Instagram), lo que se conoce como "sharenting" o "oversharing" que, no es más que una continua exposición de los menores en actividades cotidianas, en encuentros familiares o en momentos especiales conformando lo que será su futura "identidad o huella digital", y aunque, en principio, las personas que acceden a tales imágenes, en la mayoría de las ocasiones, son familiares o amigos[62], ello no impide que, toda la información que se publique, esté completamente controlada y en consecuencia, se esté proporcionando una innecesaria información a terceros que puede ser aprovechada, precisamente, para la práctica de conductas delictivas, poniendo en peligro con ello la propia integridad física o psíquica del menor o, que, en sí mismos tales comportamiento parentales pueden llegar a constituir una vulneración de la intimidad y propia imagen del hijo o de su privacidad[63]. La cuestión se complica más cuando los padres están separados o divorciados, pues, se requiere el consentimiento de ambos —en cuanto cotitulares de la patria potestad— para que, cualquiera de ellos pueda subir una fotografía de sus hijos menores a Internet[64]. De todas formas, esta información que permanece en internet a lo largo del tiempo, el artículo 94.3 de la Ley Orgánica 3/2018 de Protección de Datos —de cuyo análisis nos ocuparemos en otro apartado de este estudio— posibilita el ejercicio del derecho al olvido en servicios de redes sociales y servicios equivalentes por el afectado respecto de los datos que hubieran sido facilitados al servicio por él o por terceros —por ejemplo, sus progenitores—, precisamente, durante su minoría de edad, debiendo el prestador proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2 del citado precepto.

A todo ello, procede, asimismo señalar que, esa continúa sobreexposición de los menores en redes sociales es fruto también de su propia actuación en internet, ellos mismos son los que proporcionan información, difunden sus imágenes, videos con el peligro que entraña esta sobreexposición y el compartir contenidos con los constantes reenvíos que realizan unos a otros que, pueden derivar en situaciones de acoso u en otras formas delictivas, a lo que, precisamente contribuye el fácil acceso a dispositivos como smartphone, tablets, ordenadores y ahora los

smartwatch sobre todo por el uso de estos últimos dispositivos a edades tempranas[65]. De ahí, la importancia del control parental y los dispositivos existentes para ello en la correspondiente proporcionalidad[66].

En todo caso, cualquier actuación y decisión habrá de tener en cuenta fundamentalmente el interés superior del menor que, ha de primar sobre cualquier otro interés que puede concurrir, las limitaciones a la capacidad de obrar de los menores se interpretarán restrictivamente y se ha de preservar su identidad, cultura, religión, convicciones, orientación e identidad sexual o idioma del menor, así como la no discriminación del mismo por éstas o cualesquiera otras condiciones, incluida la discapacidad, garantizando el desarrollo armónico de su personalidad (artículo 2 de la Ley Orgánica 1/1996, de 15 de enero de Protección Jurídica del Menor, de modificación del Código Civil y de la Ley de Enjuiciamiento Civil). De ahí que, la actitud permisiva de uno de los progenitores en cuanto la adición del menor a los videojuegos y a las redes sociales puede modificar el sistema de guarda y custodia[67]. Asimismo, como establece el artículo 84.1 de la LOPDYGDD: "Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales"; y añade en su apartado segundo que "La utilización y difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor". Por su parte, el artículo 92 párrafo primero de este misma LOPDYGDD amplía tal responsabilidad a los centros docentes al disponer que: "Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información"; y, además, del deber de las Administraciones educativas de contribuir a un uso responsable de las tecnologías mediante el diseño de un bloque de asignaturas de libre configuración que incluyan la competencia digital, así como elementos relacionados con situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red (artículo 83.1 apartado segundo de la LOPDYGDD). Ciertamente, la educación y la responsabilidad son instrumentos esenciales para la protección de datos de los menores y han de orientar la actuación de los padres y las políticas educativas que se acometan y se impartan en los centros docentes.

Ahora bien, el citado artículo 84.2 otorga un papel activo al Ministerio Fiscal en la protección de los menores en Internet, y remite a la LOPJM en cuanto a la adopción de medidas cautelares y de protección atendiendo siempre al interés superior del menor. De igual forma, el artículo 4.2 de la mencionada LOPJM prevé la intervención del Ministerio Fiscal frente a la difusión de información o utilización de imágenes o nombre de los menores en los medios de comunicación que, puedan implicar intromisión ilegítima en su intimidad, honra o reputación,

o que sea contraria a sus intereses. Asimismo, dicha intervención supone instar las medidas cautelares y de protección prevista en esta Ley, además de solicitar la correspondiente indemnización por los perjuicios causados. Por su parte, el artículo 4.3 de la LOPJM considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o nombre en los medios de comunicación que puede implicar menoscabo en su honra o reputación o que sea contraria a sus intereses, incluso si consta el consentimiento del menor o sus representantes legales[68]. Ciertamente, la operatividad de este precepto se centra en la protección de la imagen o nombre de los menores en los medios de comunicación —radio, prensa escrita y digital y televisión— y, determina que, aun existiendo consentimiento del menor o de sus representantes legales pueda entenderse intromisión ilegítima cualquier utilización de la imagen o nombre del menor, si va en contra de su interés y determina la necesaria actuación del Ministerio Fiscal que, puede ser de oficio o a instancia del propio menor o cualquier persona interesada, física o jurídica o entidad pública; mientras que, el artículo 84.2 tiene su campo de actuación en las redes sociales y servicios de la sociedad de la información equivalentes, por lo que no parece posible una traslación del contenido del citado artículo 4, vía la citada remisión y, en consecuencia, considerar que, esta remisión a la Ley Orgánica 1/1996 alcanza, esencialmente, a lo que representan las medidas cautelares y de protección necesarias para asegurar un adecuado amparo o protección del menor, valga la redundancia, atendiendo siempre a su interés superior. En todo caso, la intervención del Ministerio Fiscal ante la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes puede ser de oficio o a instancia de los propios menores —ante una eventual actuación "intensa" de sus padres en tales servicios de la sociedad de la información, en los términos apuntados, vulnerando su interés superior—[69], o de cualquier persona interesada, física o jurídica o entidad pública; y, a diferencia, de la previsión de actuación del Ministerio Fiscal que, contiene el artículo 4.3 respecto a los medios de comunicación, que tiene lugar aunque conste el consentimiento del menor o sus representantes legales, atendiendo siempre al interés superior del menor, no parece que, pueda ser trasladable el campo de operatividad de dicho precepto a la intervención también del Ministerio Fiscal en la utilización o difusión de imágenes o información personal de los menores en redes sociales y servicios de la sociedad de la información, al orientarse más la remisión a la adopción de medidas cautelares y de protección cuando resulten necesarias, como así lo establece el artículo 84.2 de la LOPDYGDD).

En este contexto, efectivamente resulta esencial que los datos referidos a menores de edad serán objeto de especial consideración y tratamiento, empleando para ello las medidas de seguridad que mejor se adapten y cubran las exigencias de protección y especial cuidado que, exigen este segmento de la población, especialmente vulnerable y, por ende, de realizar la correspondiente evaluación de impacto de las operaciones de tratamiento de los datos de tales menores frente a los riesgos que pueda entrañar para sus derechos y libertades (artículo 35.1 del RGPD). Igualmente, se ha de ser especialmente cuidadoso en el tratamiento de datos biométricos y de datos de geolocalización, respecto de los que, además de aplicarse el principio de proporcionalidad y minimización en la utilización de

estos datos, se debe informar a los menores de edad mayores de catorce años o a los padres o tutores en el caso de menores de catorce años y contar con el consentimiento expreso de los menores o de los padres o tutores, cuando éstos no puedan prestarlo[70]. Asimismo, se debe ser especialmente enérgico y eficaz en la protección de los menores cuando actúan en redes sociales.

3.4. El interés superior del menor, las redes sociales y plataformas digitales en línea de gran tamaño y motores de búsqueda.

La Ley Orgánica 8/2015 de 22 de julio ha reformado el artículo 2 de la Ley Orgánica 1/1996 que, con relación al interés del menor, después de indicar que, estamos ante un concepto jurídico indeterminado que, ha sido objeto de diversas interpretaciones a lo largo de estos años, lo define en su Preámbulo desde un contenido triple: como derecho sustantivo, como principio general y como norma de procedimiento. Respecto de esta triple dimensión, se indica además, en el citado Preámbulo que, el interés del menor tiene una misma finalidad: asegurar el respeto completo y efectivo de tales derechos del menor, así como su desarrollo integral y añade que, a la luz de estas consideraciones, es claro que la determinación del interés superior del menor en cada caso, debe basarse en una serie de criterios aceptados y valores universalmente reconocidos por el legislador que, deberán ser tenidos en cuenta y ponderados en función de diversos elementos y circunstancias del caso. Precisamente, los criterios a tener en cuenta en la interpretación y aplicación en cada caso del interés superior del menor se ponderarán teniendo en cuenta: a) La edad y madurez del menor; b) La necesidad de garantizar su igualdad y no discriminación por su especial vulnerabilidad; c) El irreversible efecto del transcurso del tiempo en su desarrollo; d) La necesidad de estabilidad de las soluciones que se adopten para promover la efectiva integración y desarrollo del menor en la sociedad, así como minimizar los riesgos que cualquier cambio de situación material y emocional pueda ocasionar en su personalidad y desarrollo futuro; e) La preparación del tránsito a la edad adulta e independiente, de acuerdo con sus capacidades y circunstancias personales; f) Aquellos otros elementos de ponderación que, en el supuesto concreto, sean considerados pertinentes y respeten los derechos de los menores. De concurrir el interés superior del menor con otro interés legítimo, deberán priorizarse aquellas medidas que, respondiendo a este interés, respeten también los otros intereses legítimos presentes. En el caso de no poderse respetar todos los intereses legítimos concurrentes, deberá primar el interés superior del menor sobre cualquier otro interés legítimo que pudiera concurrir[71].

FERNÁNDEZ ACEVEDO define las redes sociales *on line* como "estructuras sociales compuestas por un grupo de personas que comparten un interés común, relación o actividad a través de internet o de un canal de comunicación digital y en donde tienen lugar ciertas conexiones virtuales entre las personas que conforman dicho grupo, las cuales pueden ser recopiladas mediante una serie de informaciones que muestren las preferencias de consumo de información ya sea a través de una comunicación en tiempo real o ya sea a través de una comunicación diferida en el tiempo"[72]. Según el Dictamen 5/2009 sobre las redes sociales en línea,

elaborados, adoptado el 12 de junio de 2009 (WP 163) por el Grupo de Trabajo del Artículo 29 los servicios de redes sociales (SRS) pueden conceptuarse como "plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes". Asimismo, en este Dictamen el GT29 califica los servicios de redes sociales como servicios de la sociedad de la información que comparten determinadas características: "1. Los usuarios deben proporcionar datos personales para generar su descripción o "perfil"; 2. Los SRS proporcionan también herramientas que permiten a los usuarios poner su propio contenido en línea (contenido generado por el usuario como fotografías, crónicas o comentarios, música, vídeo o enlaces hacia otros sitios); 3. Las redes sociales funcionan gracias a la utilización de herramientas que proporcionar una lista de contactos para cada usuario, con las que los usuarios pueden interactuar"[73]. Los proveedores de redes sociales como responsables del tratamiento de datos, en cuanto proporcionan los medios que permiten tratar los datos de los usuarios, deben informar de forma clara y accesible a los usuarios —información por capas—[74], especialmente en el caso que se aporten datos sensibles o se refiera al tratamiento de datos de menores de edad, además de contar con el consentimiento del menor o sus representantes legales —consentimiento granular— (artículo 92.2 de la LOPDYGDD). Asimismo, han de facilitar el ejercicio de los derechos de acceso, rectificación —artículo 85 de la LOPDYGDD—; supresión o derecho al olvido —artículo 94 de la LOPDGDD—; portabilidad —artículo 95 de la LOPDYGDD—; limitación del tratamiento —artículo 16 de la LOPDYGDD—; y oposición a los usuarios de redes sociales. Todo ello sin perjuicio de las nuevas obligaciones de las redes sociales en cuanto prestadores de servicios de la sociedad de la información con respecto a los datos de personas fallecidas y, el acceso a sus datos o en su caso, a su rectificación o supresión que, en caso de fallecimiento de menores de edad, corresponde a los representantes legales, o el Ministerio Fiscal en el marco de sus competencia, bien de oficio o a instancia de cualquier persona física o jurídica interesada que, podrán dirigirse al responsable o encargado del tratamiento para solicitar tal acceso, o en su caso, la rectificación o supresión de los datos de sus hijos menores (artículos 3.3 y 96.1 c) de la LOPDYGDD).

En este sector se incluyen empresas como Alphabet (dueña de plataformas como YouTube, YouTube Kids Y Google Classroom), Meta (Facebook, Instragram,WhatsApp), Twitch (perteneciente a Amazon) y TikTok (propiedad de la empresa china ByteDance)[75]. Todas ellas controlan y recopilan una cantidad ingente de datos. Si bien, los menores y adolescentes desconocen el valor de sus datos; lo que, permiten a estas empresas, por una parte, mercantilizar con los mismos; crear perfiles que, entre otras cosas, les proporciona un conocimiento del comportamiento de la persona menor y adolescente en el momento actual como en el futuro (mediante predicciones sobre las tendencias que ofrece el mercado en su comportamiento —hábitos de consumo, influencia en sus decisiones); y, por otro, estas redes sociales y las plataformas digitales influyen en el comportamiento de los menores y adolescentes captando su atención a través de recompensas o generando emociones de todo tipo a través de la priorización de determinado contenidos que saben, van a tener una pronta respuesta de este colectivo[76]. Ante una cierta opacidad en cómo utilizan los datos, les permite obtener beneficios y orientar sus objetivos a lograr orientar el comportamiento, los hábitos y las emo-

ciones mediante instrumentos, como la publicidad en sus redes o plataformas, u ofreciendo productos o servicios adictivos.

Por su parte, los dispositivos móviles (smartphones y tabletas con sistema operativo Android e IOS, éstos último fabricado por Apple, además de otros sistemas operativos menores); relojes digitales (con sistema operativo de Google o Apple o sistemas operativos cerrados) permiten el acceso s aplicaciones móviles (APPS) que sirven entre otros fines, para la navegación en internet, para el entretenimiento —juegos, películas, música—, para las redes sociales y, en fin, para servicios basados en la localización entre otros. El Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes adoptado el 27 de febrero de 2013 (WP 202) define las aplicaciones como "programas informáticos generalmente concebidos para un cometido concreto y dirigido a un determinado conjunto de dispositivos inteligentes como teléfonos inteligentes, tabletas o televisiones conectados a internet". Las aplicaciones organizan la información de acuerdo con las características específicas del dispositivo y suelen interactuar con el soporte físico y las características del sistema operativo del mismo, además de posibilitar que, los dispositivos inteligentes puedan conectarse mediante interfaces de red wi-fi, bluetooth[77]. En dicho Dictamen, después de señalar que, los niños son ávidos usuarios de aplicaciones, ya sea en dispositivos propios o en dispositivos compartidos, existiendo al respecto un gran mercado de aplicaciones diversas destinadas a ellos y que, aquellos apenas conocen o comprenden el alcance y la sensibilidad de los datos a que dichas aplicaciones pueden acceder o el alcance de los datos compartidos con terceros para fines publicitarios, recomienda una serie de actuaciones a las partes que participan en el desarrollo, comercialización y explotación de las aplicaciones para alcanzar el máximo nivel de protección de la intimidad y protección de datos: así a los desarrolladores de aplicaciones que crean aplicaciones y/o las ponen a disposición de los usuarios finales, deben por lo que se refiere a las aplicaciones destinadas a niños; prestar atención al límite de edad que define a los niños o los menores de edad en las legislaciones naciones; escoger el enfoque más restrictivo del tratamiento de datos respetando íntegramente los principios de minimización de datos y limitación de la finalidad; abstenerse de tratar datos de niños para fines de publicidad compartamental, directa o indirectamente; de recoger a través de los niños datos de sus familiares y amigos; a las tiendas de aplicaciones donde se compran y descargan las aplicaciones y se registran los datos de inicio de sesión y el historial de aplicaciones compradas previamente deben: prestar especial atención a las aplicaciones dirigidas a los niños para protegerles contra el tratamiento ilícito de sus datos y, en particular, hacer cumplir la información pertinente de manera sencilla y con un lenguaje propio de las edades en cuestión; a los fabricantes de sistemas operativos y dispositivos que también como responsables del tratamiento de datos deben por un lado, garantizar la disponibilidad de mecanismos apropiados y los datos a que pueden acceder y, por otro, garantizar que todo acceso a una categorías de datos se refleja en la información del usuario antes de instalar la aplicación: las categorías presentadas deben ser claras y comprensibles; y, a las terceras partes, pues, muchas aplicaciones gratuitas se costean mediante publicidad —como cookies u otros identificadores del dispositivo o banner dentro de la aplicación o anuncios fuera de la misma— además de conocer y cumplir sus obligaciones como responsables del tratamiento de datos cuando procesen datos

personales sobre usuarios, debe abstenerse de tratar datos de niños para fines de publicidad compartamental directa o indirectamente y aplicar medidas de seguridad adecuadas. Esto incluye la transmisión segura y el almacenamiento cifrado de los identificadores únicos de dispositivo y de usuario y otros datos personales[78].

Pues bien, atendiendo a los derechos que cualquier persona física cuyos datos personales sean objeto del tratamiento puede ejercer (derecho de acceso del interesado, derecho de rectificación y supresión (derecho al olvido), derecho a la limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición y de decisiones individuales automatizadas, incluida la elaboración de perfiles), el artículo 94 de la LOPDYGDD se refiere al ejercicio del derecho al olvido en servicios de redes sociales y servicios equivalente y destaca al respecto que, toda persona tiene derecho a que sea suprimidos, a su simple solicitud, los datos personales que, se hubieran facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes. Y como supuesto específico señala que, si los datos se hubieran facilitado al servicio por el afectado o por terceros durante su minoría de edad, y el afectado ejercitase este derecho al olvido, el prestador de redes sociales o servicios equivalentes deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad que concurran las circunstancias contenidas en el apartado 2 del citado artículo —que los datos sean inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieran devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información—.

En todo caso, en aras del respeto a la autonomía del individuo, al libre desarrollo de su personalidad, una vez que, el interesado menor alcance la edad de consentimiento digital puede confirmar, modificar o retirar el consentimiento dado por el titular de la patria potestad o tutor o autorizado por dicho titular.

Por otra parte, el RGPD establece en su artículo 8.3 que las normas sobre requisitos de autorización parental con respecto a los menores no afectarán a las disposiciones generales del Derecho contractual de los Estados miembros, como normas relativas a la validez, formación o efectos de los contratos en relación con un niño". Por lo que, los requisitos de consentimiento válido para el uso de datos relativos a niños forman parte de un marco jurídico que debe considerarse independiente del Derecho contractual nacional. El Reglamento no incluye una armonización de las disposiciones nacionales del Derecho contractual. De todas formas, la regulación nacional y la europea pueden operar de forma simultánea. Asimismo, el considerando número 38 del citado RGPD establece que "(…). El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños".

Ahora bien, conviene precisar que, habitualmente, los fabricantes ponen a disposición sus propias herramientas de control parental en si sistemas operativos: tiempo y límites de uso y contenido, seguridad en las comunicaciones, preguntar antes de comprar, clasificación por edades en las tiendas de aplicaciones, centro de los dispositivos que usan menores. Respecto al diseño de las aplicaciones que ofrecen en las tiendas los distintos fabricantes, aquellas que se incluyen en la categoría de infantiles no permiten enlaces externos, ni recomendaciones y no

incluyen publicidad. En todo caso, los principales riesgos para los menores y adolescentes derivan del uso de algoritmos que recomienda determinados contenidos y aplicaciones en tiendas digitales, además de llevar a cabo un perfilado y recogida de datos on line. En este contexto, las videoconsolas suelen también incluir configuraciones que permiten usar herramientas de control parental. Y, además, la industria del videojuego cuenta con un sistema europeo de clasificación por edades (PEGI); si bien, es voluntario, pues está basado en la autorregulación.

De todas formas, a las herramientas de control parental, existen las medidas de bloqueo de contenidos inadecuados que pueden tener lugar tanto en los centros educativos como en las bibliotecas. Y, para las empresas aplicar además de sistemas de control de contenido, sistemas de verificación de la edad que garanticen el anonimato y la privacidad de los usuarios, como analizaremos.

Resulta un dato a tener en cuenta cómo es que los servicios que ofrecen estas empresas (redes sociales, plataformas de intercambio de videos, plataformas de video bajo demanda) son los que más impacto tienen en la seguridad digital de los menores y adolescentes; y, al ser multinacionales sus sedes están fuera de Europa (en concreto Estados Unidos o China); si bien, no es menos cierto que en cuanto al control y regulación de contenidos y servicios que ofrecen en Europa están sometidos además de los citados tres Reglamentos —RGPD, RIA y el Reglamento de Servicios Digitales—, el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

En fin, el aumento exponencial del uso de aplicaciones de IA generativa ha puesto sobre la mesa la existencia de otro riesgo, la posibilidad que tienen los menores y adolescentes de alterar la imagen de otro menor o adolescente, y combinándolo con otra de carácter pornográfico dar lugar a una nueva fotografía de alto contenido sexual protagonizado por sin menor sin quererlo (el caso de los menores de Almendralejo).

Si bien, en este contexto, de especial relevancia ha sido la creación, en 2019, del "Canal Prioritario", para solicitar la retirada urgente de contenidos sexuales o violentos publicados y/o difundidos en Internet sin el consentimiento de las personas afectadas, evitando que sean causa de graves daños y perjuicios. Cuenta con una línea específica para las denuncias de menores de edad, mayores de 14 años. Asimismo, es destacable la constitución, también en 2019, y a partir de la aplicación de la LOPDYGDD que incorpora el derecho a la educación digital, y del grupo de trabajo "Menores, salud digital y privacidad" dedicado a facilitar dicha educación y a analizar y estudiar las situaciones de riesgo de niños, niñas y adolescentes (NNA) en la red. En él se reúnen los agentes públicos y privados implicados en el interés superior del o de la menor. Cabe destacar su actividad en la prevención, detección y atención a las consecuencias del uso intensivo, problemático o adictivo de los dispositivos digitales por NNA, y el apoyo a las iniciativas científicas destinadas a proporcionar pautas y orientaciones que contribuyan a la salud y bienestar digital de NNA, como el "Plan Familiar Digital" y las "Recomendaciones" de la Asociación Española de Pediatría.

IV. EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL Y LA PROTECCIÓN DE MENORES DE EDAD Y ADOLESCENTES.

La inteligencia artificial (IA) es una tecnología que ha experimentado un avance espectacular en poco tiempo, gracias a tecnologías como el *big data*, el blockchain[79], la nube, el internet de las cosas, la robótica y la realidad virtual. Aunque la IA no es una invención reciente, ya que sus orígenes se remontan a hace más de 50 años, su impacto actual es enorme y afecta a casi todos los ámbitos de la vida. La IA está presente en multitud de aplicaciones.

Hoy en día estamos siendo testigos del crecimiento exponencial que ha experimentado la tecnología de aprendizaje automático (*machine learning*) y la inteligencia artificial (IA) en general y de la intención de la regulación europea de evitar consecuencias negativas sobre el estado de derecho. La regulación de la IA ha sido un imperativo de la evolución de estas tecnologías por parte de la Comisión Europea. Esta regulación representa un desafío complejo que requiere un enfoque multidisciplinar y una colaboración continua entre los diferentes actores involucrados. El RIA representa, por tanto, un avance significativo en este ámbito, pero su implementación efectiva dependerá de la capacidad de las organizaciones para adaptarse a las nuevas normativas y de la cooperación entre las autoridades reguladoras. Asimismo, este Reglamento establece un marco normativo para el desarrollo, comercialización y uso de sistemas de IA, con un enfoque basado en el análisis de riesgos, como veremos, y, por tanto, alineado con la interpretación que el propio RGPD hace de los posibles impactos que las tecnologías pueden tener sobre los derechos y libertades de las personas físicas.

Lo que define a los sistemas de IA es la capacidad de procesar datos e información y abarca generalmente aspectos de razonamiento, aprendizaje, creatividad o la capacidad de predecir o planear. Es un conjunto de técnicas que permiten a un sistema informático simular características que son propias de la inteligencia humana. De manera que, se automatizan ciertas actividades hasta ahora vinculadas exclusivamente con procesos del pensamiento humano, como pueden ser la toma de decisiones. Los sistemas de IA son capaces de analizar, pero también de trabajar de manera autónoma. Son tecnologías de procesamiento de la información que integran modelos y algoritmos con capacidad para aprender y realizar tareas cognitivas, dando lugar a resultados como la predicción y la adopción de decisiones en entornos materiales y virtuales. La ciberseguridad es otra cuestión relevante en este ámbito.

En el artículo 1 establece que el objetivo del RIA como es: 1. Mejorar el funcionamiento del mercado interior; 2. Promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA en la Unión así como prestar apoyo a la innovación; 3. Establecer normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión; 4. Prohibir determinadas prácticas de IA; 5. Concretar los requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas. 6. Disponer normas armonizadas

de transparencia aplicables a determinados sistemas de IA; normas armonizadas para la introducción en el mercado de modelos de IA de uso general; y, normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento; 7. Establecer medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes.

Asimismo, precisa el considerando núm. 1 del RIA: "el objetivo de este Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, proteger frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación".

En su artículo 3 define el sistema de IA como: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales; y el riesgo como: la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio. Supone la habilidad de un sistema informático para realizar tareas como las relacionadas con el aprendizaje, el razonamiento o la resolución de problemas, la percepción o el uso del lenguaje.

Por tanto, se trata de: 1. Un sistema basado en la máquina; 2. El sistema puede funcionar con distintos grados de independencia, desde la autonomía total hasta cierto nivel de supervisión humana; 3. La necesidad de supervisión humana para garantizar la seguridad, el cumplimiento ético y la responsabilidad; 4. El sistema procesa datos de entrada para generar resultados como predicciones, contenidos, recomendaciones o decisiones[80]. Esta definición se corresponde con la proporcionada por la OCDE (2019, revisado en 2023), que la RIA adopta con el objetivo de facilitar la convergencia de nociones a escala internacional. Quedan fuera de la misma y, por tanto, de la regulación, los sistemas de *software* de capacidades inferiores a las indicadas"[81]. Y por "riesgo" se considera: la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio (artículo 2.1 y 2 de la RIA).

La IA está presente en múltiples aplicaciones y funcionalidades de las que hacen uso tanto loa adultos como los menores. Es el caso de los chatbots y asistentes virtuales, videojuegos, plataformas educativas, chaptGPT y otros generadores de textos; DALL-E y generación de imágenes para el arte digital; filtros de contenidos, para fotos y videos en redes sociales; traductores automáticos; e internet de las cosas (IoT) —robots de limpieza o asistentes de voz, juguetes conectados—. Con la IA se puedes recopilar y analizar datos, lo que permiten la automatización de procesos y de toma de decisiones; pueden interactuar con el usuario, generando

un contenido más inmersivo; es una tecnología interactiva; permite la generación de imágenes; y, es un apoyo para diversas tareas —traductor de textos y videos—.

Al ser el RIA el primer instrumento legislativo del mundo sobre IA aplicable al mercado de la UE (*efecto Bruselas*), promueve un ecosistema tecnológico que beneficie a la sociedad sin comprometer la seguridad, ni los derechos humanos y establece una regulación única para proveedores, importadores, distribuidores, responsables del despliegue y particulares afectados por los sistemas de IA en el mercado europeo. Se entiende por proveedor: una persona física o autoridad pública que desarrolle (o para la que se desarrolle) un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado, o ponga en servicio el sistema de IA, con su propio nombre o marca; distribuidor: una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión; importador: una persona física o jurídica, ubicada o establecida en la Unión, que introduzca en el mercado un sistema de IA de un proveedor establecido fuera de la UE; y responsable del despliegue (deployer): una persona física o jurídica o autoridad pública que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. También se hace referencia al proveedor posterior como: un proveedor de un sistema de IA, también de un sistema de IA de uso general, que integra un modelo de IA, con independencia de que el modelo de IA lo proporcione él mismo y esté integrado verticalmente o lo proporcione otra entidad en virtud de relaciones contractuales (artículo 3.68 del RIA). Esta regulación no afecta a la innovación, ni la perjudica, pues, el Comité de Inteligencia artificial trabaja en la elaboración de normas y recomendaciones para garantizar que la IA sea segura, ética y beneficiosa para la sociedad; y permite adaptarse a las invocaciones que el sector va desarrollando en su aplicación. De todas formas, el Supervisor Europeo de Protección de Datos participa como observador en el Comité, asegundo que la IA respeta la privacidad y los derechos de las personas.

Ahora bien, el RIA sigue un enfoque basado en el riesgo; de modo que, la normativa se adapta al nivel de riesgo específico y opera mediante técnicas de *Compliance*, concretando los siguientes sistemas[82]: sistemas de riesgo inaceptable; sistemas de IA de alto riesgo; y, sistemas de IA de riesgo limitado[83].

En cuanto al riesgo inaceptable: El RIA establece una prohibición absoluta para varias prácticas que conllevan riesgos inaceptables, como veremos; al riesgo alto: El RIA clasifica como de alto riesgo determinados sistemas que plantean un riesgo significativo de daño para la salud, la seguridad o los derechos fundamentales; riesgo limitado: determinados sistemas de IA a los que se imponen requisitos específicos de transparencia; por ejemplo, cuando existe un riesgo claro de manipulación (v. gr., mediante el uso de chatbots). Los usuarios deben ser conscientes de que están interactuando con un sistema de IA; y, en fin, riesgo mínimo: todos los demás sistemas de IA pueden desarrollarse y utilizarse conforme a la legislación vigente sin obligaciones adicionales. Los proveedores de estos sistemas pueden optar voluntariamente por aplicar las directrices para una IA digna de confianza o adherirse a códigos de conducta voluntarios.

Así se consideran prácticas prohibidas. 1. El uso de técnicas subliminales, manipuladoras o engañosas para distorsionar el comportamiento de una perso-

na o un grupo de personas, haciéndoles tomar una decisión que de otro modo no habrían tomado, de una manera que probablemente les cause un perjuicio considerable; 2. La explotación de las vulnerabilidades de una persona física o un grupo de personas derivadas de su edad o discapacidad, o de una situación social o económica, con la finalidad o el efecto de alterar sustancialmente su comportamiento con una probabilidad razonable de causarles perjuicios considerables; 3. Puntuación ciudadana (social scoring): Sistemas de IA para la evaluación o clasificación de personas físicas o grupos de personas durante un periodo determinado en función de su comportamiento social o sus características personales, que pueden dar lugar a un trato perjudicial o desfavorable en contextos sociales no relacionados con aquellos en los que se recabaron los datos, o a un trato injustificado o desproporcionado; 4. Sistemas de IA para evaluar o predecir el riesgo de que una persona física cometa un delito, basándose únicamente en su perfil o sus rasgos de personalidad; 5. Sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión; 6. Sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando su uso esté destinado a fines médicos o de seguridad, 7. Sistemas de IA de categorización biométrica que clasifican individualmente a las personas físicas basándose en sus datos biométricos para deducir o inferir determinados datos sensibles; y, 8. Sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento de la ley, con ciertas excepciones sujetas a condiciones y garantías (artículo 5)[84].

En cuanto a los sistemas de alto riesgo el RIA distingue dos grupos: 1. Los sistemas vinculados a la legislación de armonización de la UE sobre seguridad de los productos, enumerada en el Anexo I del RIA, se clasificarán como de alto riesgo si se cumplen las dos condiciones siguientes: A) Que el sistema de IA sea un producto incluido en la legislación de armonización, o sea un componente de seguridad de estos productos. B) Que, en virtud de la legislación de armonización, el producto o componente deba someterse a una evaluación de la conformidad de terceros; 2. Sistemas enumerados en el Anexo III del RIA: se consideran de alto riesgo debido al ámbito en el que se utilizan y sus aplicaciones específicas. Biometría: incluidos los sistemas de identificación biométrica remota y la categorización biométrica basada en la inferencia de características sensibles o protegidas; Gestión de infraestructuras críticas: agua, gas, electricidad, transporte; Cumplimiento de la ley: sistemas de prevención e investigación de delitos, incluidos sistemas predictivos y de elaboración de perfiles; Educación y formación profesional: sistemas utilizados para determinar la admisión a centros educativos y de formación profesional, evaluar los resultados del aprendizaje, valorar el nivel de educación que recibirá una persona y supervisar y detectar comportamientos prohibidos de los estudiantes durante los exámenes; Migración, asilo y gestión del control fronterizo; Empleo, gestión de los trabajadores y acceso al autoempleo; Servicios privados esenciales y servicios y prestaciones públicos esenciales (seguros, banca, crédito, prestaciones...); y, Administración de justicia y procesos democráticos.

Los requisitos que han de cumplir tales sistemas son: 1. Sistema de gestión de riesgos: Implantar y mantener un sistema de gestión de riesgos durante todo el ciclo de vida del sistema; 2. Sistema de calidad, formación y pruebas: Garantizar

la calidad de los datos de entrenamiento, validación y prueba mediante prácticas adecuadas de gobernanza y gestión de datos; 3. Documentación técnica: Elaborar y mantener actualizada la documentación técnica del sistema; 4. Registro automático de acontecimientos: Permitir los archivos de registro/el registro automático de acontecimientos; 5. Instrucciones de uso: Proporcionar instrucciones de uso fáciles de entender para los responsables del despliegue; 6. Supervisión humana: Permitir una supervisión humana efectiva durante su uso; 7. Precisión/ciberseguridad: Alcanzar un nivel adecuado de precisión, solidez y ciberseguridad (artículos 6, 7, 8, 9, 11 y 12)[85].

Respecto a los modelos de IA de uso general. Además de sistemas de IA, el RIA contempla también determinados modelos de IA. Los modelos de IA se integran en sistemas, pero no constituyen en sí mimos un sistema. El concepto de modelos de IA de uso general debe definirse claramente y diferenciarse del concepto de sistemas de IA con el fin de garantizar la seguridad jurídica. La definición debe basarse en las características funcionales esenciales de un modelo de IA de uso general, en particular la generalidad y la capacidad de realizar de manera competente una amplia variedad de tareas diferenciadas. Estos modelos suelen entrenarse usando grandes volúmenes de datos y a través de diversos métodos, como el aprendizaje autosupervisado, no supervisado o por refuerzo. Los modelos de IA de uso general pueden introducirse en el mercado de diversas maneras, por ejemplo, a través de bibliotecas, interfaces de programación de aplicaciones (API), como descarga directa o como copia física. Estos modelos pueden modificarse o perfeccionarse y transformarse en nuevos modelos. Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen por sí mismos sistemas de IA. Los modelos de IA requieren que se les añadan otros componentes, como, por ejemplo, una interfaz de usuario, para convertirse en sistemas de IA. Suelen estar integrados en los sistemas de IA y formar parte de dichos sistemas[86].

El artículo 3.63 del RIA define como: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado; "capacidades de gran impacto": capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados.

Por otra parte, el RIA establece normas específicas para los modelos de IA de uso general y para los modelos de IA de uso general que entrañan riesgos sistémicos, que deben aplicarse también cuando estos modelos estén integrados en un sistema de IA o formen parte de un sistema de IA (artículo 51).

Los grandes modelos de IA generativa son un ejemplo típico de un modelo de IA de uso general, ya que permiten la generación flexible de contenidos, por ejemplo, en formato de texto, audio, imágenes o vídeo, que pueden adaptarse fácilmente a una amplia gama de tareas diferenciadas.

Cuando un modelo de IA de uso general esté integrado en un sistema de IA o forme parte de él, este sistema debe considerarse un sistema de IA de uso ge-

neral cuando, debido a esta integración, el sistema tenga la capacidad de servir a diversos fines. Un sistema de IA de uso general puede utilizarse directamente e integrarse en otros sistemas de IA[87].

También se clasifica la IA según los tipos de capacidad y función entre: 1. IA débil (o estrecha): diseñada para realizar tareas específicas sin conciencia ni comprensión más allá de su programación. Un ejemplo con los asistentes de voz como Siri o Alexa; 2. IA fuerte (o general): capaces de realizar cualquier tarea cognitiva como un ser humano, incluyendo la adaptación y el razonamiento. Aún no existe completamente, pero es un objetivo en el desarrollo de la IA; 3. La superinteligencia artificial: sería una IA que llegaría a superar la inteligencia humana en todos los aspectos. Asimismo, se pueden clasificar según su funcionalidad: 1. IA reactiva: no tiene memoria, solo responde a estímulos inmediatos. Son un ejemplo: Deep Blue, el ordenador de ajedrez de IBM; 2. IA con memoria limitada: aprende de experiencias recientes, pero no posee un conocimiento amplio y permanente. Por ejemplo, los automóviles autónomos; 3. Teoría de la mente: es la IA que entenderá de emociones y pensamientos humanos. Todavía está en proceso de desarrollo; 4. IA estrecha (ANI): sistemas diseñados para realizar una tarea específica, como reconocimiento de voz o juegos; y, 5. Autoconciencia: IA capaz de tener conciencia propia y autoconocimiento. De difícil aplicación ahora. Por el método de aprendizaje: 1. Aprendizaje supervisado: los algoritmos aprenden a partir de datos etiquetados; 2. Aprendizaje no supervisado: los algoritmos aprenden a partir de datos no etiquetados, identificando patrones; 3. Aprendizaje por refuerzo: los algoritmos aprenden a tomar decisiones para maximizar una recompensa. Por la estructura de la IA: 1. Redes neuronales artificiales: sistemas que imitan el funcionamiento del cerebro humano; y, 2, Deep learning: un tipo de red neuronal artificial que permite la extracción de patrones complejos de datos. En fin, por aplicación: 1. Sistemas expertos: Programas que imitan el razonamiento de expertos en un área específica; 2. Robótica: diseño y construcción de robots que pueden realizar tareas físicas; y3. Procesamiento del lenguaje natural; permite a las máquinas entender y generar lenguaje humano.

Ciertamente, la taxonomía de la IA es una herramienta para clasificar y organizar los diferentes tipos de IA, sus funcionalidades, aplicaciones y formas en que interactúan con el mundo. Con ello permiten comprender mejor la evolución y el potencial de la IA, así como facilitar la comunicación y el desarrollo en este campo. En esencia, la taxonomía de la IA no es solo estructura, sino que existen diferentes clasificación que se enfocan en diversos aspectos, como hemos visto en líneas precedentes.

En cuanto a las principales obligaciones de los proveedores de sistemas de IA de alto riesgo están: 1. Velar por que sus sistemas cumplan los requisitos anteriores y acreditar su conformidad, previa solicitud motivada de la autoridad competente: 2. Establecer un sistema de gestión de calidad sólido; 3. Conservar la documentación sobre el sistema y ponerla a disposición de las autoridades, incluyendo cualquier archivo de registro generado bajo su control; 4. Velar por que los sistemas se sometan a las evaluaciones de conformidad correspondientes, elaborar una declaración UE de conformidad y colocar el marcado CE en los sistemas; y, 5. Registrar el sistema en la base de datos de la UE de sistemas de alto riesgo. 6. Adoptar las medidas correctoras necesarias, incluida la suspensión o la

retirada de los sistemas en caso de no conformidad. Ahora bien, un operador será considerado proveedor, y por tanto sujeto a las obligaciones correspondientes, cuando: 1. ponga su nombre o marca comercial en un sistema de IA de alto riesgo previamente introducido en el mercado; y, 2. O lo modifique sustancialmente (artículos 16 y 17)[88].

Sobre estas bases, las principales obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo son: cualquier persona física o jurídica o autoridad pública que utilice un sistema de IA bajo su autoridad, excepto cuando se utilice para actividades personales de carácter no profesional, deberá, como responsable del despliegue: 1. Adoptar medidas técnicas y organizativas adecuadas para garantizar que dichos sistemas se utilizan con arreglo a las instrucciones de uso; 2. Garantizar que las tareas de supervisión humana son realizadas por personas con la competencia adecuada; 3. Asegurarse de que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema, en la medida en que los implantadores ejerzan el control sobre dichos datos; 4. Vigilar el funcionamiento del sistema e informar de cualquier riesgo e incidente a los proveedores, importadores, distribuidores y autoridades de vigilancia del mercado; 5. Conservar los archivos de registro generados bajo su control; 6. Informar a sus empleados y a los representantes de los trabajadores antes de implantar un sistema de IA de alto riesgo en el lugar de trabajo; 7. Informar a todas las personas que puedan verse afectadas por el uso de sistemas que tomen decisiones o colaboren en los procesos de toma de decisiones; 8. Cooperar con las autoridades competentes; y 9. Asegurarse de que los empleados y otras personas a quienes se encomiende en su nombre el manejo y el uso de los sistemas de IA tienen un nivel adecuado de alfabetización en materia de IA (artículo 26). En determinados casos, los responsables del despliegue deben llevar a cabo una evaluación de impacto en materia de derechos fundamentales[89].

Ahora bien, existen obligaciones de transparencia para determinados sistemas de IA, independientemente de si se consideran de alto riesgo: 1. Sistemas de IA destinados a interactuar directamente con personas físicas: Los proveedores deben diseñar el sistema de tal manera que las personas físicas afectadas estén informadas de que están interactuando con un sistema de IA; 2. Sistemas que generen contenido sintético de audio, imagen, video o texto: Los proveedores velarán por que la información de salida del sistema de IA esté marcada en un formato legible por máquina y que sea posible detectar que ha sido generada o manipulada de manera artificial; 3. Sistemas de reconocimiento de emociones o de categorización biométrica: Los responsables del despliegue deberán informar del funcionamiento del sistema a las personas físicas expuestas a él; y, 4. Sistemas que generen o manipulen imágenes o contenidos de audio o vídeo que constituyan una ultrafalsificación, y contenidos que informen sobre asuntos de interés público: Los responsables del despliegue deberán divulgar que el contenido se ha generado o manipulado de manera artificial (artículo 13).

Precisamente, en relación con los menores se opera en los riesgos asociados de la IA, especialmente, en el ámbito educativo, el entretenimiento y la seguridad digital; de ahí, la exigencia de requisitos específicos para los sistemas de IA de alto riego y normas de transparencia[90].

Recientemente, la Comisión europea ha puesto en marcha una consulta pública sobre los sistemas de IA de alto riesgo con la finalidad de recabar información sobre la aplicación de las normas del RIA relativos a estos sistemas, su funcionamiento y aplicación práctica. Está abierta a proveedores y desarrolladores de IA, empresas, autoridades públicas, instituciones de investigación, sociedad civil y ciudadanos en general hasta el 18 de julio de 2025. Las observaciones que se extraigan de la citada consulta se tendrán en cuenta para la elaboración de las próximas directrices de la Comisión sobre la clasificación de los sistemas de IA de alto riesgos, así como sus requisitos y obligaciones conexas.

Por otra parte, se regulan los modelos de IA de uso general se integran en sistemas de IA, pero no son sistemas en sí mismos. El RIA define los modelos de IA de uso general como aquellos que: 1. Tienen un grado considerable de generalidad; 2. Son capaces de realizar una gran variedad de tareas; y 3. Pueden integrarse en diversos sistemas o aplicaciones de IA. Son, esencialmente versátil, esto es, capaces de adaptar a múltiples propósitos sin necesidad de un entrenamiento específico para cada tarea y aunque algunos modelos pueden presentar rasgos sistémicos, están siendo de muy utilidades en diversos sectores, mejorando su eficiencia.

Los proveedores de estos modelos deben cumplir ciertas obligaciones, como: 1. Documentar el proceso de entrenamiento y sus resultados de evaluación; 2. Informar a los proveedores de sistemas de IA que tengan previsto integrar en sus sistemas el modelo de IA de uso general sobre sus características y requisitos legales; 3. Establecer una política de cumplimiento de la normativa de la UE sobre derechos de autor y derechos afines, especialmente en lo que respecta a la minería de textos y datos; y 4. Divulgar públicamente un resumen detallado del contenido utilizado para entrenar el modelo de IA de uso general (artículo 53).

Debido a sus capacidades de gran impacto, se considera que determinados modelos de IA de uso general plantean un riesgo sistémico. Para mitigar estos riesgos, los proveedores deben cumplir requisitos más estrictos: 1. Evaluar modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica; 2. Evaluar y mitigar los posibles riesgos sistémicos a escala de la Unión que puede derivarse del desarrollo, la introducción en el mercado o el uso de modelos de IA con riesgos sistémicos, así como el origen de dichos riesgos; 3. Vigilar, documentar y comunicar sin demora indebida, a la Oficina de IA y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctoras para resolverlos; y, 4. Velar por que se establezca un nivel adecuado de protección de la ciberseguridad para el modelo de IA de uso general con riesgo sistémicos y la infraestructura física del modelo (artículo 55)[91].

En este contexto, la Unión Europea está desarrollando un Código de Buenas Prácticas para modelos de IA de uso general, detallando normas sobre transparencia, derechos de autor y mitigación de riesgos. Precisamente, el 10 de julio de 2025 la Comisión Europea ha presentado el Código de Buenas Prácticas para modelos de Inteligencia Artificial de uso general (General Purpose Artifical Intelligence —GPAI—)

Tras esta breve referencia normativa sobre los tipos de IA y las obligaciones de los intervinientes en la misma a grandes rasgos, procede indicar que, la IA está presente en diversas aplicaciones accesibles para menores y adolescentes,

como asistentes virtuales, videojuegos, plataformas educativas. Asimismo que, la interacción entre menores y la IA plantea cuestiones importantes sobre la ética, privacidad, desarrollo cognitivo y educación. Desde el impacto de los algoritmos en la conformación de sus opiniones hasta la protección de sus datos.

En cuanto a los riesgos del uso de IA para los menores y adolescentes se señalan los siguientes: 1. Manipulación cognitiva de la realidad, influir en su comportamiento y desarrollo cognitivo de los menores; dicción —la IA puede generar contenido altamente personalidad y adictivo que, puede afectar el bienestar de los menores—; la falta de conocimiento de lo que representa su privacidad y seguridad en un entorno digital —introduciendo datos e información personal (fotos, videos, audios u otra información sensible)—; si bien, algunas plataformas como Instagram dentro de sus políticas de privacidad está el detectar perfiles de adolescentes que se hacen pasar por personas mayores de edad y configurar sus cuentas con protecciones adicionales; 2. Desinformación y la falta de credibilidad de la información: la IA puede influir en el comportamiento y las decisiones de los menores, a la par que, dificultan que el menor distinga lo que es real, de lo que no lo es. Confiar en las respuestas generales que ofrece la IA sin comprobar su veracidad. Lo que puede conllevar la difusión de información errónea y a una situación de dependencia por el uso excesivo de aplicaciones con IA; 3. Privacidad: la IA puede recopilar datos personales de los menores y adolescentes sin que ellos sean plenamente conscientes de ellos; planteando riesgos de seguridad; 4. Discriminación y exclusión a través de sesgos desarrollados por los algoritmos, afectando la percepción de los menores sobre ciertas materias y temas; 5. La exposición a contenido inapropiado o a información errónea: algunos sistemas de IA pueden generar o "recomendar" contenidos no adecuados para menores sin filtros efectivos; 6. La suplantación de su identidad o ciberacoso; 7. Riesgos de salud física, psicológicos y emocionales: un uso excesiva de IA puede afectar al desarrollo cognitivo y emocional de los menores y adolescentes. Además, la dependencia de asistentes virtuales y plataformas automatizadas pueden conllevar una disminución del pensamiento crítico y la creatividad en edades tempranas[92]; y, 8. El uso de algoritmos opacos y adictivos[93] y de patrones oscuros (Dark patterns) y adictivos[94]. La IA puede optimizar plataformas digitales para monitorizar el tiempo de uso; lo que puede generar adicción y afectar el bienestar de los menores.

De ahí que, como veremos en la tramitación normativa futura en España, las medidas para proteger a los menores en el ámbito de la IA y, en general, en lo que representa el entorno digital que deben incluir: 1. Control parental obligatorio: se deben incluir herramientas de control por defecto en dispositivos móviles, tablets; 2. Elevar la edad mínima en materia de protección de datos de 14 a 15; a la par que limitar el acceso de los menores a redes sociales sin supervisión previa de los progenitores; 3. Políticas de privacidad más estrictas en redes sociales; 4. Verificadores de edad por parte de las plataformas; 5. Regulación del contenido accesible para menores; sanciones penales por la creación de imágenes manipuladas con IA ("deepfakes") con fines vejatorios y sexuales; lo que exige modificar la normativa penal; 6. Lo que se conoce como alfabetización digital —educación digital— que posibilita que los menores aprendan a identificar los riesgos en internet y lleven a cabo un uso responsable de la tecnología: mediante el establecimiento de períodos específicos de uso de los dispositivos electrónicos —por ejemplo, establecer un

máximo diario para juegos y redes sociales—; 7. Promover el uso consciente de la tecnología, explicando a los menores y adolescentes los riegos de la sobreexposición a pantallas y el impacto en la salud mental; fomentar la autorregulación[95]; 8. Supervisar activamente el contenido: los padres y educadores deben monitorear el uso de la IA y establecer límites adecuados y efectivos. Así, por ejemplo, establecer límites de tiempo en el uso de dispositivos; revisar el contenido que consumen; y, fomentar el uso de plataformas seguras y educativas; 9. La transparencia: promover leyes que garanticen la seguridad de los menores y adolescentes en entornos digitales, exigir transparencia en los algoritmos e información a los operadores sobre cómo recopilan y usan los datos; 10. Reducir la dependencia digital empezando por los propios progenitores, pues, los menores toman como modelo e imitan el comportamiento de los adultos; 11. Procurar un uso responsable de la tecnología mediante normas claras sobre el uso de los dispositivos; fomentar el desarrollo de habilidades fuera del entorno digital; e integrar la IA en la educación de manera interactiva y supervisada; y, 11. Verificar la edad a través de sistemas de verificación de la edad (SVE)[96].

Frente a estos riesgos, procede señalar que el uso de la IA también ofrece múltiples oportunidades y ventajas a los menores y adolescentes: 1. Posibilita una educación personalizada: tutorías virtuales y proporcionar materiales ajustados al menor o adolescente a la par que permite crear planes de estudio adaptado a las necesidades individuales de cada estudiante —aplicaciones como plataformas de aprendizaje adaptativo pueden identificar áreas donde un alumno necesita más apoyo y ajustar los materiales a dicha circunstancia—[97]. Efectivamente, la IA permite adaptar el contenido y el ritmo de aprendizaje a las necesidades individuales de cada estudiantes, mejorando su comprensión y motivación; 2. Desarrollo de habilidades digitales: los menores y adolescentes pueden aprender a analizar datos, programación gracias a la IA —el conocimiento de IA y programación es cada vez más necesario en la sociedad actual; de forma que, herramientas como Scratch, Code.org y otras plataformas impulsadas por IA enseñan a los jóvenes a programar de manera interactiva y divertida; lo que ayuda a desarrollar pensamiento computaciones, resolución de problemas y habilidades lógicas—; 3. Seguridad en línea: los sistemas de IA puede detectar y bloquear contenidos inapropiados, ayudar a prevenir el ciberacoso y mejorar la privacidad en plataformas digitales —plataformas educativas utilizan filtros impulsados por la IA para evitar el acceso a información dañina, peligrosa y garantizar un entorno seguro en la red—; 4. Accesibilidad e inclusión: la IA puede facilitar el acceso a la educación para menores con discapacidad, mediante tecnologías como reconocimiento de voz, la conversión de texto en audio y herramientas de apoyo al aprendizaje —por ejemplo, estudiantes con dislexia pueden beneficiarse de lectores automatizados que les ayudan a comprender mejor los textos—; 5. Optimización del tiempo: puede ayudar en la organización de tiempo de estudio y mejorar su productividad; apoyo en la salud mental: aplicaciones de basadas en IA pueden ofrecer orientación emocional y detectar signos de ansiedad o depresión en menores y adolescentes —algunos chatbots pueden proporcionar consejos sobre bienestar mental y ayudar a gestionar emociones difíciles—; todo ello acompañado de la terapia en profesionales expertos en salud mental; y, 7. Fomento de la creatividad: herramientas de IA permiten a los jóvenes explorar su creatividad en diversas áreas como la música, escritura,

los idiomas, el deporte y el arte —a través de aplicaciones de composición asistida por la IA pueden ayudar a crear canciones; o permiten un diseño digital mediante ilustraciones generadas automáticamente; o en fin, como hace el Museo Nacional del Prado que a través del Proyecto FrAI Angelico muestra como la IA puede ayudar a acercar el patrimonio cultural a la ciudadanía y, en particular, a los menores y adolescentes: mediante sistemas de aprendizaje automático se puede reconocer el contenido de las pinturas y su contexto histórico e iconográfico—.

En todo caso, resulta necesario identificar el uso de la IA en aras de la transparencia y la confianza en las tecnologías —existen herramientas que permiten detectar si los textos se han generado por IA o si las imágenes o video ha sido creado mediante IA—. Ciertamente, el uso de inteligencia artificial generativa y su etiquetado se ésta incorporando paulatinamente —algunas plataformas optan por marcas de agua y otras por implementar un sistema de etiquetado disponible para los creadores de contenido—[98].

Y, para finalizar este apartado, nos parece oportuno indicar, por un lado, que en aras de conseguir una IA fiable se han presentado las Directrices éticas para una IA fiable por el Grupo de Expertos de Alto nivel sobre inteligencia artificial creado por la Comisión Europea en junio 2018 tiene como objetivo promover una inteligencia artificial fiable. La fiabilidad de la inteligencia artificial (IA) se apoya en tres componentes que deben satisfacerse a lo largo de todo el ciclo de vida del sistema: a) La IA debe ser lícita, es decir, cumplir todas las leyes y reglamentos aplicables; b) Ha de ser ética, de modo que se garantice el respeto de los principios y valores éticos; y c) Debe ser robusta, tanto desde el punto de vista técnico como social, puesto que los sistemas de IA, incluso si las intenciones son buenas, pueden provocar daños accidentales. Cada uno de estos componentes es en sí mismo necesario pero no suficiente para el logro de una IA fiable. Lo ideal es que todos ellos actúen en armonía y de manera simultánea. En el caso de que surjan tensiones entre ellos en la práctica, la sociedad deberá esforzarse por resolverlas. Estas directrices establecen un marco para conseguir una IA fiable. Dicho marco no aborda explícitamente el primero de los tres componentes expuestos de la inteligencia artificial (IA lícita). En lugar de ello, pretende ofrecer orientaciones sobre el fomento y la garantía de una IA ética y robusta (los componentes segundo y tercero). Las directrices, que van dirigidas a todas las partes interesadas, buscan ofrecer algo más que una simple lista de principios éticos; para ello, proporcionan orientación sobre cómo poner en práctica esos principios en los sistemas sociotécnicos. Las orientaciones se ofrecen en tres niveles de abstracción, desde el capítulo I (el más abstracto) al III (el más concreto). Concluyen con ejemplos de las oportunidades y preocupaciones fundamentales que plantean los sistemas de IA. El capítulo II ofrece orientaciones sobre cómo lograr una IA fiable, enumerando siete requisitos que deben cumplir los sistemas de IA para ello. Para aplicar estas orientaciones se pueden utilizar tanto métodos técnicos como de otro tipo. El capítulo III ofrece una lista concreta y no exhaustiva para la evaluación de la fiabilidad de la IA, con el objetivo de poner en práctica los requisitos descritos en el capítulo II. Dicha lista de evaluación deberá adaptarse al caso específico de utilización del sistema de IA.

Ahora bien, estas directrices pretenden ofrecer orientaciones sobre las aplicaciones de la IA en general y establecer una base horizontal para lograr una IA

fiable, las diferentes situaciones plantean desafíos distintos. Por lo tanto, se debería explorar si, además de este marco horizontal, puede ser necesario un enfoque sectorial dado que la aplicación de los sistemas de AI depende del contexto. En fin, estas directrices no aspiran a reemplazar ninguna política o reglamento actual o futuro, ni a impedir su introducción. Deben considerarse un documento vivo, que habrá de revisarse y actualizarse a lo largo del tiempo para garantizar que sigan siendo pertinentes a medida que evolucionen la tecnología, el entorno social y nuestros propios conocimientos. Este documento ha sido concebido como un punto de partida para el debate sobre "Una IA fiable para Europa". Más allá de Europa, las directrices también buscan estimular la investigación, la reflexión y el debate sobre un marco ético para los sistemas de IA a escala mundial.

España ha creado la Agencia Española de Supervisión de IA (AESIA) encargada de garantizar el uso ético y seguro de la IA en el país. Su misión es proteger la privacidad, la igualdad de trato, y los derechos fundamentales, promoviendo un desarrollo tecnológico responsable. En todo caso, aún no se ha aprobado la Ley correspondiente en la que se nombre la AEPD como autoridad de vigilancia del mercado a efectos de la RIA. No obstante, conviene precisar que, la citada AEPD es autoridad competente en materia de protección de datos personales; lo que supone incluir bajos sus labores de supervisión y control, a aquellos tratamientos realizados mediante inteligencia artificial. En consecuencia, la AEPD puede actuar y, asimismo, supervisar tratamientos de datos personales realizados mediante sistemas prohibidos, en la medida que afecten al derecho de protección de datos.

Y, por otro, reiterando, aunque sea brevemente, los numerosos delitos a los que se ven expuestos los menores y adolescentes en el entorno virtual y también en el presencial, inducidos por la información que obtienen en internet —en todo caso, pueden ser parte activa o parte pasiva (víctima)—: 1. Sexting: consiste en difundir imágenes o grabaciones íntimas sin el consentimiento de la persona afectada, se regula en el artículo 197.7 del Código Penal. Este delito se considera un tipo de descubrimiento y revelación de secretos, y castiga a quien, sin autorización, difunda, revele o ceda a terceros imágenes o grabaciones obtenidas con la anuencia de la persona afectada en un lugar privado. Estamos ante "conductas o prácticas entre adolescentes consistentes en la producción de cualquier tipo de imágenes digitales en las que aparezcan menores de forma desnuda o semidesnuda y en su transmisión a más menores, ya sea a través de la telefonía móvil o el correo electrónico, o mediante su puesta a disposición de terceros a través de internet"[99]. Pueden ser fotografías propias en posturas provocadoras o tratarse de desnudos; o bien fotos o vídeos en el momento de las relaciones sexuales que se envían a otras personas. Ahora bien, es importante destacar que el delito de *sexting* se aplica incluso cuando la imagen o grabación fue obtenida inicialmente con el consentimiento de la persona, pero luego se difunde sin su autorización. La pena es de prisión de tres meses a un año o multa de seis a doce meses. Como circunstancias agravantes: la pena se impondrá en su mitad superior en casos específicos como: 1. Si los hechos son cometidos por el cónyuge o una persona con relación afectiva; 2. Si la víctima es menor de edad o tiene una discapacidad; 3. Si los hechos se cometen con fines lucrativos; 2. Sextorsión: se trata del chantaje o amenaza de publicar contenido audiovisual o información personal sexual; en este caso, de un niño, niña o adolescente. No está tipificado en el Código Penal español con

esta denominación, pero su conducta se incluye en diferentes delitos; amenazas; explotación sexual; y, extorsión. Se diferencia del sexting en que, mientras éste supone el envío de materiales con connotación sexual a través de internet (imágenes, videos, mensajes, videollamadas), en la sextorsión la obtención de contenidos con connotación sexual de otra persona se hace a través del engaño, amenazas, extorsiones, coacciones, etc. Se entra en la dimensión online del chantaje que puede durar horas, meses o años, y que puede llevarlo a cabo una persona tanto conocida como desconocida por la víctima. Resulta poco probable que la persona que lo sufre pida ayuda, ya sea porque se siente avergonzada, culpable, o tenga miedo de que se difunda su material íntimo. En la mayoría de las ocasiones, el menor o adolescente teme que su círculo familiar y de amistades, descubran que ha compartido material sexual[100]; 3. Ciberacoso o cyberbullying: Es una violencia entre iguales que consiste en el hostigamiento hacia una víctima, a través de mensajes, imágenes, vídeos o comentarios, todos ellos con intención de dañar, insultar, humillar o difamar. Mientras que el bullying se produce principalmente en los centros escolares, el cyberbullying escapa de este espacio y puede darse entre menores de distintas escuelas, fuera del horario lectivo y extenderse indefinidamente en el tiempo. El contenido, una vez publicado digitalmente, puede ser reproducido y reenviado infinitas veces; 4. *Happy slapping*: la violencia que consiste en "la grabación de una agresión, física, verbal o sexual hacia una persona, que se difunde posteriormente mediante las tecnologías de la comunicación. La agresión puede ser publicada en una página web, una red social, una conversación a través del teléfono móvil, etc.". Así, el *happy slapping* consiste en la grabación de una agresión física, verbal o sexual y su difusión online mediante las tecnologías digitales (páginas, blogs, chats, redes sociales, etc.). Lo más común es que esta violencia se difunda por alguna red social y, en ocasiones, puede hacerse viral. La búsqueda de popularidad y de *likes* puede llevar a muchos jóvenes a cometer un delito contra sus compañeros e incluso, contra sus amigos. La persona que graba esta agresión, ocasional o planificada, cree que colgar la agresión en una plataforma digital puede ser "entretenido" o "divertido" para ganar popularidad en internet. Ahora bien, normalmente esta forma de violencia se relaciona con el *cyberbullying*. Sin embargo, en el *happy slapping* normalmente hay la intención previa de difundir el contenido, es decir, una grabación premeditada[101]; 5. *Online child grooming* o ciber acoso sexual a menores: se regula en el artículo 183 ter.1 y 2 del Código penal. Es un delito por el cual una persona adulta contacta electrónicamente con un menor o adolescente, ganándose poco a poco su confianza con el propósito de involucrarle en una actividad sexual. En ocasiones, los adultos, precisamente, se hacen pasar por menores en Internet o intentan establecer un contacto con niños y adolescentes que dé pie a una relación de confianza, pasando después al control emocional y, finalmente al chantaje con fines sexuales. Esta práctica tiene diversos objetivos: 1. Producción de imágenes y vídeos con connotación o actividad sexual, destinados al consumo propio de pederastas o a redes de abuso sexual a menores; 2. Encuentros en persona con el menor y abuso sexual físico; y, 3. Explotación sexual y prostitución infantil. Habitualmente el contacto entre ambas partes comienza a través de algún servicio de Internet, preferentemente redes sociales, plataformas de juego o comunidades online. Son servicios muy utilizados por los menores y todos ellos tienen funcionalidades de chat para conversar. El atacante

suele utilizar el engaño para facilitar ese primer contacto, creando perfiles falsos con edades y gustos similares a los del menor, de manera que le resulte atractivo e interesante, para que acepte su solicitud de amistad. Puede llegar a proponerle seguir conversando en privado por mensajería instantánea o videollamada, como por ejemplo WhatsApp o Skype. Esta conversación puede ir desde hablar de sexo y obtener material del mismo tipo, hasta mantener un encuentro sexual[102]. Aun cuando no se alcance este objetivo, también son considerados *online grooming* todos los actos materiales encaminados a conseguirlo[103]; 6. Ciberviolencia sexual (agresión sexual): obtener las grabaciones en las que la menor aparece realizándose tocamientos sobre el propio cuerpo, valiéndose el actor de amenazas que de no acceder a las conminaciones del victimario éste revelaría las imágenes a todos los contactos que la menor tenía en la red social y, denunciaría, además, a sus padres[104]; y, 7. Sharenting: como analizamos, es la práctica cada vez más habitual de madres y padres, en la que exponen pública y constantemente la vida de sus hijas e hijos en la red (cumpleaños, actividades, momentos de ocio, etc.). En principio, puede parecer una costumbre inofensiva, pero debemos ser conscientes de las consecuencias que puede tener para las vidas de las niñas y los niños. La huella digital es el rastro que dejamos cuando utilizamos internet y que no podemos eliminar. Para niñas y niños, esta huella se "genera" cada vez antes, debido a la publicación de información personal (fotos, vídeos, etc.) que realizan padres y madres.

V. EL PROYECTO DE LEY 121/000052 DE PROTECCIÓN DE LOS MENORES EN ENTORNOS DIGITALES.

El Consejo de Ministros de España aprobó el 2 de junio de 2024 el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, una de las medidas incluidas en el gran acuerdo de país que el Gobierno está impulsando para salvaguardar la salud, el bienestar y la seguridad de los niños, niñas y adolescentes de nuestro país; y, ha comenzado su tramitación como Proyecto de Ley en el Congreso de los Diputados[105].

El objetivo de esta norma es garantizar los derechos de los menores en el ámbito digital, especialmente el derecho a la intimidad, al honor y a la propia imagen, así como el derecho a la protección de sus datos personales y al acceso a contenidos adecuados para su edad. En este sentido, la ley contiene medidas para mejorar el conocimiento de los menores y de sus familias sobre los riesgos del entorno digital, sancionar de forma adecuada la vulneración de derechos que puede producirse en ese entorno —como, por ejemplo, la difusión de imágenes generadas por IA— e imponer obligaciones a grandes operadores e *influencers*, para garantizar la información y los derechos de los menores.

Esta Ley Orgánica tiene por objeto establecer medidas con la finalidad de garantizar la protección de las personas menores de edad en los entornos digitales (artículo 1).

Su principal objetivo es ofrecer entornos digitales seguros para la infancia y la adolescencia, con plena protección de sus derechos y libertades, a la vez que se fomenta un uso adecuado y respetuoso de las nuevas tecnologías. De acuerdo con lo anterior, el artículo 2 reconoce los derechos de las personas menores de edad

en este tipo de entornos, entre ellos los derechos a ser protegidas eficazmente ante contenidos digitales que puedan perjudicar su desarrollo, a recibir información suficiente y necesaria en una forma y lenguaje apropiado según la edad y el grado de madurez sobre el uso de las tecnologías y de los riesgos asociados al mismo, así como al acceso equitativo y efectivo a dispositivos, conexión y formación para el uso de herramientas digitales. Supone completar el marco normativo ya previsto en la LOPJM, LOPIVI, LOPDYGDD.

Las medidas que se recogen en la ley se despliegan desde una perspectiva amplia y multidisciplinar, alcanzando una protección integral de las personas menores de edad en el uso de dispositivos y medios digitales con una perspectiva preventiva, de atención e inclusión, con el fin de ofrecer a través de los canales adecuados herramientas accesibles que permitan anticiparse al desarrollo de problemas más graves, y fomentar entornos sin discriminación.

El entorno digital pone a disposición de la sociedad, en su conjunto, numerosas ventajas y beneficios, pero su uso ha de ser especialmente adecuado cuando los principales destinatarios de las nuevas tecnologías digitales son las personas menores de edad, que cada vez se enfrentan a mayores riesgos derivados de un consumo perjudicial. Es por ello que la presente ley contempla varias medidas en materia de protección de las personas menores de edad como consumidores y usuarios, que se recogen en el título I y también en la disposición final cuarta, que modifica de manera expresa el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.

Respecto de las medidas recogidas en el título I, el artículo 4 establece dos nuevas obligaciones dirigidas a los fabricantes de los equipos terminales digitales con conexión a internet a través de los cuales las personas menores de edad puedan acceder a contenidos perjudiciales para su desarrollo, que se encuentran en línea con lo previsto en el artículo 46, apartados 3 y 4, de la LOPIVI: una obligación de información en sus productos de los posibles riesgos derivados de un uso inadecuado, entre otros aspectos, y la obligación de que los equipos terminales digitales que fabriquen incluyan en su sistema operativo una funcionalidad de control parental que permita a sus usuarios restringir o controlar el acceso de dichas personas a servicios, aplicaciones y contenidos perjudiciales para menores, cuya activación debe producirse por defecto en el momento de la configuración inicial del equipo terminal. Como situación más específica, entre los consumos con un potencial perjudicial cabe mencionar los mecanismos aleatorios de recompensa (cajas botín o "lootboxes"), que forman parte de algunos videojuegos y que, sin el debido control de acceso en su activación, pueden suponer un riesgo para las personas vulnerables, en especial las más jóvenes a quienes van dirigidas y son los principales consumidores de este tipo de productos y servicios, tal y como pone en evidencia el estudio "Loot boxes in online games and their effect on consumers, in particular young consumers", encargado por la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo, en el que se llama la atención sobre los diferentes riesgos asociados a los mecanismos utilizados en las cajas botín en función de la fase de desarrollo de los niños y adolescentes.

En el caso de las personas menores de edad, es probable que el contacto con estos mecanismos aleatorios de recompensa constituya su primer encuentro con

un producto o funcionalidad en cuya mecánica de funcionamiento el azar tenga un papel preponderante y que guarda la citada similitud, tanto desde el punto de vista estructural como de las técnicas de marketing utilizadas para su comercialización, con ciertas modalidades propias del juego regulado. Por lo expuesto, el artículo 5 dispone una prohibición general de acceso a los mecanismos aleatorios de recompensa o su activación por personas que sean menores de edad, si bien reglamentariamente se podrán establecer supuestos en los que se determinen excepciones en las que se flexibilice la prohibición, siempre que se garantice la protección a la infancia.

Se aclara que la prohibición señalada no opera de manera general, sino que resulta de aplicación solo a los mecanismos aleatorios de recompensa que presentan un conjunto de caracteres que los hacen asimilables en mayor grado a ciertos productos de juegos de azar.

En coherencia con las medidas contempladas en el título I, la disposición final quinta modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, con el fin de incorporar la protección de las personas menores de edad, como personas consumidoras vulnerables, en relación con los bienes o servicios digitales. Además, se incide en la obligación por la parte empresarial de asegurarse de la mayoría de edad del consumidor y usuario con carácter previo a la contratación de bienes o servicios propios o ajenos o, internos o externos, destinados a personas mayores de edad, ya sea por su contenido sexual, violento o por suponer un riesgo para la salud física o el desarrollo de la personalidad; y se tipifica el incumplimiento por parte del empresario de dicha obligación de verificación y comprobación de edad como infracción leve en materia de defensa de los consumidores y usuarios.

El título II, compuesto por los artículos 6 y 7, incorpora las medidas dirigidas al ámbito educativo responde a la necesidad de mejorar la formación en esta materia tanto de los alumnos como del personal docente. Por una parte, se dispone el fomento de actuaciones de mejora de las competencias digitales del alumnado, con el fin de garantizar su plena inserción en la sociedad digital y el aprendizaje de un uso seguro, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, el trabajo y la participación en la sociedad, así como la interacción con estas. En línea con los principios pedagógicos que desarrolla la Ley Orgánica 2/2006, de 3 de mayo, de Educación, uno de los cuales es precisamente el desarrollo transversal de la competencia digital, y se vinculan también con el artículo 5 de la Ley Orgánica 1/1996, de 15 de enero, en relación con el derecho a la información, y el artículo 33 de la Ley Orgánica 8/2021, de 4 de junio, sobre formación en materia de derechos, seguridad y responsabilidad digital.

Por otra parte, se reconoce el papel fundamental del profesorado en el proceso de adquisición de las competencias digitales por parte del alumnado y en la detección de riesgos, y por ello se dispone que la planificación de la formación continua del profesorado no universitario incorpore actividades formativas que faciliten a los centros educativos el desarrollo de estrategias para el tratamiento, entre otros aspectos, de la seguridad y de los elementos relacionados con la ciudadanía digital, la privacidad y la propiedad intelectual, tomando para ello como referencia las áreas y competencias establecidas en el Marco de Referencia de la

Competencia Digital Docente y la regulación existente en materia de protección integral a la infancia y la adolescencia frente a la violencia, protección de datos personales y garantía de los derechos digitales.

Finalmente, de manera más específica a propósito del problema antes apuntado, el artículo 7 establece que los centros educativos, de acuerdo con las disposiciones que al efecto hayan aprobado las administraciones educativas, regulen como parte de sus normas de funcionamiento y convivencia el uso de dispositivos móviles y digitales en las aulas, en las actividades extraescolares y en lugares y tiempos de descanso que tengan lugar bajo su supervisión.

El título III contempla medidas en el ámbito de protección de las víctimas de violencia de género y violencias sexuales. Así, el artículo 8 establece que las víctimas de violencia de género o violencias sexuales facilitadas por entornos digitales tendrán la condición de víctimas a los efectos de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género y de la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, respectivamente. Por su parte, el artículo 9 garantiza que las personas menores de edad tendrán derecho a acceder a los servicios de información y orientación y, dado el caso, de atención psicosocial inmediata y asesoramiento jurídico, por vía telefónica y en línea, las 24 horas, todos los días del año. De igual forma, se reconoce el derecho a acceder a los servicios de acogida y asistencia psicológica y social destinados a las víctimas de violencia de género y de violencias sexuales y a los centros de crisis 24 horas. Además, se considera imprescindible considerar estos servicios como esenciales, ya que de ellos dependen la seguridad, la salud y el bienestar de la población afectada que es especialmente vulnerable.

El título IV aborda las medidas de carácter sanitario a adoptar por las Administraciones públicas. El impacto en la salud de los niños, niñas y adolescentes por el uso inadecuado de las tecnologías y entornos digitales constituye un motivo creciente de preocupación para las familias, educadores y profesionales de la salud. Así, existen evidencias de que pasar un tiempo excesivo frente a las pantallas y la exposición a contenidos inapropiados pueden afectar la salud mental y aumentar el riesgo de ansiedad, depresión, adicción, problemas de autoestima, trastornos del sueño, problemas en el desarrollo del lenguaje y habilidades sociales, así como en la capacidad de concentración y resolución de problemas. También se ha encontrado evidencia que las personas adolescentes con alta exposición a medios y entornos digitales podrían tener más probabilidad de desarrollar síntomas de trastorno por déficit de atención e hiperactividad. Además, los niños y niñas pueden exponerse a discursos de odio, violencia y contenidos que incitan a la autolesión o al suicidio, o que tienen un impacto negativo en su bienestar emocional y psicológico. Por otra parte, el tiempo excesivo frente a las pantallas contribuye a un estilo de vida sedentario y por tanto a sufrir trastornos musculoesqueléticos, obesidad infantil y a los problemas derivados de la misma, como las enfermedades cardiovasculares y endocrinas. Para ello, el artículo 10 promueve que, con base en el principio de salud en todas las políticas, se incorpore la dimensión sanitaria en los estudios que se promuevan por las Administraciones públicas sobre el uso de estas tecnologías y entornos digitales por las personas menores, con el objetivo de aumentar el conocimiento sobre los efectos en la salud y generar evidencia científica. Asimismo, incorpora actuaciones individuales y comunitarias en los

programas de prevención y promoción de la salud infantil y adolescente que se desarrollan desde la atención primaria, para la detección precoz de los problemas específicos relacionados con las tecnologías y entornos digitales, así como el establecimiento de programas coordinados con otras administraciones públicas, para el abordaje integral, tratamiento y rehabilitación, con una perspectiva biopsicosocial. Por otra parte, el artículo 11, promueve la atención sanitaria especializada para personas menores con conductas adictivas sin sustancia.

En cuanto, a las medidas en el sector público, reguladas en el título V, se fundamentan en la obligación de los poderes públicos de promover las condiciones de libertad e igualdad de las personas, tanto individualmente como en los grupos en los que se integran, para que sean reales y efectivas, suprimiendo los obstáculos que dificulten su plenitud y facilitando la participación ciudadana en la esfera social, política, cultural y económica, tal y como recoge el artículo 9.2 de la Constitución Española. Asimismo, en virtud del artículo 11 de la LOPJM, las Administraciones Públicas deberán tener en cuenta las necesidades de los menores al ejercer sus competencias especialmente, entre otros, en relación con las nuevas tecnologías. A través de las medidas de participación, información y sensibilización previstas en el artículo 12, en línea con lo previsto en la LOPIVI, se incide en la necesidad de incorporar acciones proactivas y eficaces en relación con la información y formación sobre entornos digitales seguros, dirigidas a personas menores de edad y a sus familias, garantizando el ejercicio efectivo del derecho de participación en los planes, programas y políticas que afecten a la infancia y la juventud. A tal efecto, el artículo 13 dispone el fomento de la colaboración público-privada y la corregulación, de forma que los proveedores del servicio de acceso a internet desde una ubicación fija aprueben un código de conducta que establezca los mecanismos y parámetros de configuración segura que se comprometen a aplicar en la prestación de sus servicios en lugares de acceso público en los que se presten servicios públicos, para evitar el acceso a contenidos inadecuados por parte de las personas menores de edad; el artículo 14 garantiza la especialización profesional en todos los niveles de la Administración de todo el personal que trabaje en contacto directo con personas menores de edad; y, el artículo 15 recoge la obligación del Gobierno, en colaboración con las comunidades autónomas, las ciudades de Ceuta y Melilla y las entidades locales, de elaborar una Estrategia Nacional sobre la protección de la infancia y la adolescencia en el entorno digital, en la que participarán el Observatorio de la Infancia, las entidades del tercer sector, la sociedad civil, y, de forma muy especial, con las niñas, niños y adolescentes. Esta Estrategia, que deberá definirse en consonancia con la Estrategia Estatal de los Derechos de la Infancia y de la Adolescencia, perseguirá la alfabetización digital y mediática, la difusión de información a las familias, y personas que habitualmente estén en contacto con menores, el uso seguro de dispositivos, la investigación y la creación de espacios de interacción y colaboración sobre cultura digital.

Por otra parte, la protección de las personas menores de edad en los entornos digitales puede requerir como último recurso la interrupción de un servicio de la sociedad de la información que ofrezca acceso sin límites a contenido que perjudica gravemente al desarrollo físico, mental y moral de los menores. De modo general, el artículo 8.1 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, permite que los órganos competentes para

su protección puedan adoptar las medidas necesarias para interrumpir la prestación de un servicio de la sociedad de la información o retirar los datos que este ofrezca. Dado que estas medidas restrictivas pueden llegar a afectar a derechos fundamentales como la libertad de expresión o el derecho de información, que gozan de protección constitucional, una orden para la interrupción de un servicio o la retirada de contenido debe contar con la correspondiente autorización judicial.

Concretamente, se modifican el artículo 95.e) de la Ley Orgánica 6/1985, de 1 de julio, y el artículo 9.2 de la Ley 29/1998, de 13 de julio, a fin de atribuir a la Sección de lo Contencioso-Administrativo del Tribunal Central de Instancia la competencia para autorizar la ejecución de los actos adoptados por los órganos administrativos competentes en la materia para que se interrumpa la prestación de servicios de la sociedad de la información o para que se retiren contenidos que vulneren cualquiera de los bienes jurídicos enumerados en el artículo 8 de la Ley 34/2002, de 11 de julio, no solo la propiedad intelectual, así como para la ejecución de los adoptados para la interrupción del acceso a un intermediario por el coordinador de servicios digitales con base en el artículo 51.3.b) del Reglamento de Servicios Digitales. Asimismo, se modifica el artículo 122 bis de la Ley 29/1998, de 13 de julio, con objeto de que el procedimiento de autorización judicial para la ejecución de estas medidas se generalice para todos los bienes jurídicos protegidos, no solo para salvaguardar la propiedad intelectual.

En lo relativo a la protección de las personas menores de edad en entornos digitales, la habilitación a los Juzgados Centrales de lo Contencioso-Administrativo para autorizar estas medidas permitirá que todas las autoridades competentes en la materia puedan solicitar la autorización judicial para la interrupción de servicios o retirada de contenidos que atenten contra la protección de la juventud y la infancia. Entre otros supuestos, esto permitiría a la Comisión Nacional de los Mercados y la Competencia solicitar la autorización de una orden de cese de actividad a una plataforma de intercambio de vídeos o a un servicio de comunicación audiovisual a petición con contenido para adultos que no incluya sistemas de verificación de edad que limiten su acceso a menores.

En la adaptación a las nuevas formas de criminalidad y, sin olvidar los principios limitadores del *ius puniendi* del Estado, permitan ejercer una protección eficaz frente a los nuevos delitos tecnológicos, se ha estimado conveniente la incorporación de cuatro tipos de modificaciones, que se articulan en la disposición final tercera en el Código Penal. En primer lugar, se incorpora la pena de alejamiento de los entornos virtuales, para un mejor cumplimiento de la prevención general y especial en el ámbito de los delitos tecnológicos. En concreto, se modifican los artículos 33, 39, 40, 45, 48, 56, 70 y 83 del Código Penal para incorporar la pena de prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual, cuando el delito se comete en su seno. De este modo, se vincula el contenido de la pena a la naturaleza del delito, y se establece una mayor protección de las víctimas, evitando la reiteración de conductas punibles.

De manera complementaria, se modifica el artículo 96.3 para que esta misma prohibición se pueda imponer como medida de seguridad; y la disposición final primera reforma el artículo 544 bis de la Ley de Enjuiciamiento Criminal a fin de que el juez de instrucción pueda adoptarla como medida cautelar. En segundo

lugar, se aborda específicamente el tratamiento penal de las denominadas ultrafalsificaciones, esto es imágenes o voces manipuladas tecnológicamente y extremadamente realistas. A tal fin se incorpora un nuevo artículo 173 bis que sanciona a quienes, sin autorización de la persona afectada y con ánimo de menoscabar su integridad moral, difundan, exhiban o cedan su imagen corporal o audio de voz generada, modificada o recreada mediante sistemas automatizados, software, algoritmos, inteligencia artificial o cualquier otra tecnología, de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorias. Además de que las ultrafalsificaciones generalmente se difunden en el ciberespacio, con la potencialidad de permanencia que ello implica, como se ha advertido respecto de los delitos tecnológicos de contenido, se produce un aumento de la lesividad en relación con otras modalidades de ataque por la enorme dificultad de distinguir entre el contenido falso y el real debido a la precisión de las nuevas tecnologías y por el mayor grado de veracidad que mantenemos respecto de materiales audiovisuales sobre materiales escritos. Técnicamente, se opta por la sanción de la difusión de las ultrafalsificaciones de contenido sexual (las llamadas deepfakes pornográficas) o especialmente vejatorio en sede de delitos contra la integridad moral porque, en virtud del principio de consunción, se abarcarían los supuestos de lesión de la integridad moral y también los ataques contra el honor, pues ha de tomarse en cuenta no solo la afectación a la autoestima y la heteroestima, sino también la cosificación e instrumentalización que se produce sobre el sujeto pasivo, generalmente mujeres y niñas, niños y adolescentes que son tratados como objetos de consumo. También hay que recordar que la motivación para llevar a cabo estas acciones no siempre se identifica con el *animus iniuriandi*, pues el hecho puede deberse a otras razones como el ánimo de lucro, si dichas imágenes se utilizan en páginas o aplicaciones de contenido pornográfico. En tercer lugar, dado que la ley tiene como objetivo específico tutelar los intereses de los niños, niñas y adolescentes, y existe una gran preocupación en relación con el acceso de los menores a contenidos pornográficos que pueden afectar a su desarrollo en la esfera afectivo sexual, se prevé la modificación del artículo 186 del Código Penal, con la finalidad de mejorar la protección del bien jurídico libertad sexual de los menores. En su actual redacción, el artículo 186 del Código Penal castiga a quienes "por medios directos", vendan, exhiban o difundan material pornográfico entre menores y personas con discapacidad necesitadas de especial protección. Tal redacción no protege suficientemente el bien jurídico de intangibilidad sexual de estos colectivos frente a la puesta a disposición indiscriminada de este tipo de material en medios en los que, conocidamente, va a ser accesible a los mismos. En consecuencia, se aborda la reforma de este precepto que tiene una especial repercusión en el ámbito de las personas de menor edad. Con la nueva redacción que se incorpora, se hace posible la punición de supuestos en los que el material pornográfico se pone a disposición de una colectividad indiscriminada de usuarios, de entre los que se tiene la clara representación de que va a haber menores de edad. Para ello, se contempla además un dolo específico reforzado. En cuarto lugar, en línea con el objetivo indicado, y tomando en consideración la incidencia de los supuestos de enmascaramiento de la propia identidad en este ámbito, también se introducen diferentes tipos agravados en los artículos 181, 182, 183, 185, 186, 188

y 189 que tienen que ver con el uso de identidades falsas a través de la tecnología, que facilitan la comisión de delitos contra las personas menores de edad[106].

Por otro lado, se modifica también la LOPDYGDD a través de la disposición final sexta para elevar a los 16 años la edad a partir de la cual las personas menores de edad pueden prestar consentimiento para el tratamiento de sus datos personales. Se considera necesario elevar la edad del consentimiento del menor en materia de protección de datos, armonizando el umbral con el establecido por la mayoría de los países de la Unión Europea, así como con el exigido en el ordenamiento jurídico nacional para los menores de edad en otras actividades o conductas.

Finalmente, esta Ley Orgánica, a través de su disposición final séptima, incorpora nueve modificaciones de la Ley 13/2022, de 7 de julio. En primer lugar, se modifica el artículo 3, relativo al ámbito de aplicación, para, por un lado, obligar a cumplir con lo establecido en los artículos 95 y 98.1, en los apartados 1, 2, 3 y 4 del artículo 99 y la sección 1.ª del capítulo IV del título VI de la Ley 13/2022, de 7 de julio, al prestador del servicio de comunicación audiovisual que, estando establecido en un país que no sea miembro de la Unión Europea o del Espacio Económico Europeo, dirija sus servicios específicamente al mercado español. Por otro lado, se obliga a cumplir con lo establecido en los artículos 88, 89, 90 y 91 de la Ley 13/2022, de 7 de julio, al prestador del servicio de intercambio de vídeos a través de plataforma que, estando establecido en un país que no sea miembro de la Unión Europea o del Espacio Económico Europeo, dirija sus servicios específicamente al mercado español, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables. En segundo lugar, con el fin de mejorar la efectividad de los canales de denuncia establecidos por la autoridad audiovisual de supervisión, se modifica el artículo 42.b) a fin de que los prestadores del servicio de comunicación audiovisual y los prestadores del servicio de intercambio de vídeos a través de plataforma incluyan en sus sitios web corporativos un enlace fácilmente reconocible y accesible al sitio web de dicha autoridad. Asimismo, se extiende de forma análoga esta obligación a los usuarios de especial relevancia que empleen servicios de intercambio de videos a través de plataforma, que deberán publicar dicho enlace en sus respectivos servicios. En tercer lugar, se modifica el artículo 89.1, relativo a las medidas para la protección de los usuarios y de los menores frente a determinados contenidos audiovisuales, con el fin de reforzar las medidas actualmente establecidas para evitar la exposición de las personas menores de edad a contenidos inapropiados a su edad. Concretamente, en el párrafo e) del citado precepto se dispone que los sistemas de verificación de la edad deberán garantizar la seguridad, la privacidad y la protección de datos, en particular, en cuanto a minimización de datos y limitación de la finalidad. Asimismo, en virtud de la modificación del artículo 89.1.f) se impone al prestador el establecimiento de sistemas de control parental controlados por el usuario final con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de las personas menores de edad.

Se modifica también el artículo 93.4 que prevé que el incumplimiento de las obligaciones previstas en el artículo 89.1.e) será constitutivo de la infracción tipificada en el artículo 157.8, sin perjuicio de la responsabilidad penal que pueda derivarse de dicha acción. A este respecto, se incluye una previsión para disponer expresamente que la Comisión Nacional de los Mercados y la Competencia (CNMC)

podrá adoptar las medidas previstas en los artículos 8 y 11 de la Ley 34/2002, de 11 de julio, de conformidad con lo dispuesto en dichos artículos, cuando dicho incumplimiento atente o pueda atentar contra el principio de protección de la juventud y de la infancia. La CNMC deberá valorar la procedencia de la adopción de tales medidas atendiendo al daño potencial en el desarrollo físico, mental o moral de los menores; al nivel de audiencia del servicio en España; o a la reincidencia en la conducta infractora. Por otra parte, se modifica el apartado 1 del artículo 94, relativo a las obligaciones de los usuarios de especial relevancia que empleen servicios de intercambio de vídeos a través de plataforma. Estos servicios que, en muchos ámbitos, son agrupados bajo el concepto de "videobloggers", "influencers" o "prescriptores de opinión", gozan de relevancia en el mercado audiovisual desde el punto de vista de la inversión publicitaria y del consumo, especialmente, entre el público más joven.

Ahora bien, desde la aprobación de la Ley 13/2022, de 7 de julio, han aparecido nuevos servicios de intercambio de videos a través de plataforma que ya no pueden ser considerados asimilables a los servicios a petición, ya que los usuarios de especial relevancia ofrecen contenidos audiovisuales en directo, mucho más parecidos a los servicios de comunicación audiovisual lineales. Por ello, a fin de garantizar una protección adecuada de los menores frente a su exposición a contenidos dañinos o perjudiciales se considera oportuno modificar el régimen establecido en el artículo 94.1 y extender a los usuarios de especial relevancia el cumplimiento de las obligaciones para la protección de los menores del contenido perjudicial previstas en los apartados 2 y 3 del artículo 99 en función de que el tipo de servicio que ofrezcan pueda considerarse lineal en abierto o de acceso condicional. Por otro lado, en la medida en que cada vez existe un mayor número de usuarios de especial relevancia que ofrecen a través de sus servicios contenidos audiovisuales de carácter informativo, se considera procedente que deban cumplir con el principio de veracidad de la información previsto en el artículo 9 de la Ley 13/2022, de 7 de julio. También, se establece que los usuarios de especial relevancia deberán emplear los sistemas de verificación de edad y de control parental previstos en las letras e) y f) del artículo 89.1, de acuerdo con la modificación expuesta anteriormente. En sexto lugar, se modifican los apartados 3 y 4 del artículo 99 obligando a los servicios de comunicación audiovisual televisivo lineal de acceso condicional y a los servicios de comunicación audiovisual televisivo a petición al establecimiento de sistemas de verificación de edad con respecto a los contenidos más nocivos, como la violencia gratuita y la pornografía, que puedan perjudicar el desarrollo físico, mental o moral de las personas menores de edad.

Además, se modifica el artículo 155 con el fin de que la CNMC supervise y controle el cumplimiento de lo previsto en la Ley 13/2022, de 7 de julio, salvo lo relativo a títulos habilitantes, y ejerza la potestad sancionadora, de conformidad con lo previsto en la Ley 3/2013, de 4 de junio, respecto de los prestadores del servicio de comunicación audiovisual televisivo y prestadores del servicio de intercambio de vídeos a través de plataforma establecidos en un país que no sea miembro de la Unión Europea o del Espacio Económico Europeo que dirigen sus servicios específicamente al mercado español. En octavo lugar, se modifica el artículo 160.1.c) con el fin de reforzar las competencias sancionadoras de la CNMC, permitiendo que este organismo pueda imponer como sanciones accesorias, por una parte,

el cese de la prestación del servicio y la pérdida de la condición de prestador del servicio de comunicación audiovisual televisivo adquirida a través de la comunicación previa, durante un periodo máximo de un año, cuando se hayan cometido las infracciones muy graves tipificadas en los apartados 13 y 14 del artículo 157, relativas a la obligación de establecer y operar sistemas de verificación de edad. Y por otra, el cese de la prestación del servicio por parte del prestador del servicio de intercambio de videos a través de plataforma, durante un periodo máximo de un año, cuando este haya cometido la infracción muy grave tipificada en el artículo 157.8, consistente en el incumplimiento de su obligación de establecer y operar sistemas de verificación de edad para los usuarios con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores que, en todo caso, impidan el acceso de estos a los contenidos audiovisuales más nocivos, como la violencia gratuita o la pornografía. Finalmente, se modifica el apartado 1 del artículo 164, para que, una vez iniciado el procedimiento sancionador por alguna de las infracciones muy graves tipificadas en los apartados 8 y 14 del artículo 157, se puedan adoptar como medidas provisionales las previstas en los artículos 8 y 11 de la Ley 34/2002, de 11 de julio, de conformidad con lo previsto en dichos artículos, que incluyen la interrupción del servicio infractor y la retirada de datos.

En este contexto, la IA se ha convertido en una de las tecnologías más disruptivas y transformadoras de nuestro tiempo. Con ella, tenemos acceso a aplicaciones capaces de realizar tareas que antiguamente requerían inteligencia humana. Además, la IA ha traído avances significativos los campos de la imagen, como la fotografía o el video. Por lo que, esta norma que está siendo objeto de tramitación supone un paso más en establecer medidas que garanticen la protección de las personas menores de edad en los entornos digitales. Se reconoce como derechos de las personas menores de edad: derecho a ser protegidas eficazmente frente a contenidos digitales que puedan perjudicar a su desarrollo, así como a su salud física y mental; a recibir información suficiente y necesaria en una forma y lenguaje apropiados según su edad y grado de madurez sobre el uso de las tecnologías, así como de sus derechos y de los riesgos asociados al entorno digital; derecho a que su seguridad y privacidad, así como su honor, intimidad e imagen se vean salvaguardados en el espacio digital y a un uso crítico, seguro y responsable de las tecnologías.

Asimismo, se disponen el cumplimiento de obligaciones por los fabricantes de equipos terminales digitales con conexión a internet, en concreto: 1. Los equipos terminales digitales deben disponer de un sistema operativo que tengan la capacidad de conectarse a internet y a través de dicha conexión pueda accederse a contenidos perjudiciales para las personas menores de edad, como es el caso de teléfonos móviles, tabletas electrónicas, televisores inteligentes, ordenadores de uso personal, consolas de videojuegos o gafas de realidad virtual o aumentada. 2. Los fabricantes de equipos terminales digitales proporcionarán información en sus productos, al menos en el embalaje y en el libro de instrucciones, manual de usuario o guía de uso del equipo, en la que se advierta, en un lenguaje accesible, inclusivo y apropiado para todas las edades, de los riesgos derivados del acceso a contenidos perjudiciales para la salud y el desarrollo físico, mental y moral de las personas menores de edad. La obligación de información comprenderá, como mínimo, el siguiente contenido: a) Las medidas de protección de datos y los riesgos

relacionados con la privacidad y la seguridad; b) El tiempo recomendado de uso de los productos y servicios, adecuado a la edad de la persona usuaria; c) Los sistemas de control parental; y, d) Los riesgos sobre el desarrollo cognitivo y emocional y la afección a la calidad del sueño de un uso prolongado de tales servicios. En todo caso se tendrá en cuenta la adaptación del lenguaje y elementos visuales y audiovisuales a las necesidades de las personas con discapacidad. 3. Los fabricantes estarán obligados a garantizar que los equipos terminales a los que se refiere este artículo incluyan en su sistema operativo una funcionalidad de control parental que permita a sus usuarios restringir o controlar el acceso de las personas menores de edad a servicios, aplicaciones y contenidos perjudiciales para ellas, cuya activación debe producirse por defecto en el momento de la configuración inicial del equipo terminal. La inclusión de la funcionalidad, su activación, configuración y actualización serán gratuitas para la persona usuaria. 4. Los fabricantes velarán por que los sistemas operativos instalados en sus equipos terminales incorporen la funcionalidad de control parental. El proveedor del sistema operativo, a petición del fabricante, garantizará y certificará al fabricante que el sistema operativo destinado a instalarse en el equipo terminal incorpora la funcionalidad de control parental.

Los datos personales de personas menores de edad recopilados o generados durante la activación de esta funcionalidad no podrán ser utilizados en ningún caso, incluso cuando la persona usuaria adquiera la mayoría de edad, con fines comerciales, como marketing directo, elaboración de perfiles y publicidad basada en el comportamiento.

En todo caso, los fabricantes deberán acreditar ante los importadores, distribuidores y comercializadores que los dispositivos suministrados cumplen los requisitos y condiciones expuestos y, los importadores, distribuidores y comercializadores deberán desarrollar actuaciones de verificación del cumplimiento de estos requisitos y condiciones.

El incumplimiento de tales obligaciones deriva en importantes sanciones. A tal efecto se considera que infracciones graves: a) la falta de información en sus productos por los fabricantes de equipos terminales digitales. b) La ausencia de la funcionalidad de control parental en los equipos terminales por los fabricantes de equipos terminales digitales. c) El diseño o fabricación errónea del equipo terminal o del sistema operativo que haga imposible activar la funcionalidad de control parental. d) La activación, configuración y actualización de la funcionalidad de control parental no gratuita para el usuario. e) La falta de certificación por el proveedor del sistema operativo al fabricante de que el sistema operativo destinado a instalarse en el equipo terminal incorpora la funcionalidad de control parental en los equipos terminales digitales. f) La falta de acreditación por los fabricantes ante los importadores, distribuidores y comercializadores que los equipos y dispositivos suministrados cumplen los requisitos y condiciones establecidos en este artículo; y, g) La ausencia de desarrollo por los importadores, distribuidores y comercializadores de actuaciones de verificación del cumplimiento de los requisitos y condiciones establecidos en este artículo. Las sanciones impuestas por cualquiera de las infracciones mencionadas podrán llevar aparejada la retirada o recuperación del mercado de los equipos o la prohibición o restricción de su

comercialización, hasta que se produzca el cumplimiento de los requisitos establecidos en este artículo.

En todo caso, por la comisión de las infracciones tipificadas en el apartado precedente se impondrá al infractor multa por importe de hasta dos millones de euros. La cuantía de la sanción que se imponga, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, lo siguiente: a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona; b) El daño causado; c) El cumplimiento voluntario de las medidas cautelares que, en su caso, se impongan en el procedimiento sancionador; d) La negativa u obstrucción a facilitar la información o documentación requerida; e) El cese de la actividad infractora, previamente o durante la tramitación del expediente sancionador; y, f) La colaboración activa y efectiva con la autoridad competente en la detección o prueba de la actividad infractora.

Resulta especialmente operativa la prohibición de acceso de los menores a los mecanismos aleatorios de recompensa o su activación por aquellos.

También resulta pertinente las medidas en el ámbito educativo, así, por un lado, las Administraciones educativas fomentarán en los centros que impartan enseñanzas de educación infantil, educación básica y educación secundaria postobligatoria, independientemente de su titularidad, el desarrollo de actividades encaminadas a la mejora de la competencia digital con el fin de garantizar la plena inclusión del alumnado en la sociedad digital y el aprendizaje de un uso seguro, saludable, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, el trabajo y la participación en la sociedad, así como la interacción con estas y la prevención de las violencias sexuales e incluirán, en su planificación de la formación continua del profesorado no universitario, de los coordinadores o coordinadoras de bienestar y protección, así como del personal de administración y servicios, actividades formativas que faciliten a los centros educativos el desarrollo de estrategias para incidir, entre otros aspectos, en la seguridad (incluido el bienestar digital y las competencias relacionadas con la ciberseguridad) y en asuntos relacionados con la ciudadanía digital, la privacidad y la propiedad intelectual. Y, por otro lado, los centros que impartan enseñanzas de educación infantil, educación básica y educación secundaria postobligatoria, independientemente de su titularidad, regularán, de acuerdo con las disposiciones que al efecto hayan aprobado las administraciones educativas y en el marco de lo previsto en el artículo 124 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, el uso de dispositivos móviles y digitales en las aulas, en las actividades extraescolares y en lugares y tiempos de descanso que tengan lugar bajo su supervisión.

Asimismo, las medidas en el ámbito sanitario en cuanto se promueve una atención especializada ante personas menores de edad con conductas adictivas sin sustancia, en la red especializada de atención a la salud mental, tanto en las Unidades de Atención a la Conducta Adictiva, como en los centros de salud mental infantojuveniles. También se establecerán procedimientos de atención sanitaria específicos para la atención integral de personas menores de edad víctimas de violencia a través del entorno digital.

Igualmente, medidas dirigidas al sector público: unas relativas a la participación, información y sensibilización de las Administraciones públicas desarro-

llando campañas y actividades de sensibilización, concienciación, prevención e información sobre los riesgos asociados al uso inadecuado de los entornos y dispositivos digitales, prestando especial atención al consumo de material pornográfico o de cualquier otro que pueda afectar a la integridad física o mental de las personas menores de edad o a su autoestima, y a la prevención, sensibilización y detección en materia de violencias sexuales. Dichas actividades prestarán especial atención a las situaciones de interseccionalidad.; a la par que, se impulsará con los proveedores de servicios de acceso internet para que aprueben códigos de conducta; y, la especialización profesional en todos los niveles de la Administración, a través de la formación inicial obligatoria y la formación continua.

En este contexto, los menores de edad que operen en entornos digitales se les consideran víctimas de violencia de género o violencias sexuales a los efectos de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género y de la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, respectivamente.

En cuanto al consentimiento para el tratamiento de datos personales: El texto del proyecto eleva de 14 a 16 años la edad de los/as menores para consentir el tratamiento de sus datos personales, lo que supone adecuar la legislación nacional a la normativa europea. Se trata de una modificación general de la edad en materia de protección de datos, una solución que el informe del CGPJ considera que favorece la seguridad jurídica al evitar que se establezcan regímenes especiales según el tipo de tratamiento de datos. No obstante, el dictamen señala que la elevación de la edad para consentir tratamientos de datos personales puede producir una disonancia entre la capacidad para el ejercicio del derecho a la protección de datos —para el que debe acreditarse haber cumplido los 16 años— y la capacidad exigida para ejercer otros derechos fundamentales como son los derechos a la intimidad y la propia imagen, para los que basta la suficiente madurez de juicio[107].

La norma proyectada, de carácter integral y transversal incluye modificaciones en el Código Penal: 1. Añade un nuevo párrafo l) al artículo 33.2 en relación con las penas graves[108]; también un nuevo párrafo m) al artículo 33.3 en relación penas menos graves[109]; y, un nuevo párrafo j) al artículo 33.4 relativa a las penas leves[110]; 2. Modifica el párrafo b) y se añade un nuevo párrafo k) al artículo 39 en cuanto penas privativas de derechos: *"b) Las de inhabilitación especial para empleo o cargo público; profesión, oficio, industria o comercio, u otras actividades, incluidas las que se desarrollen o exploten en espacios virtuales, sean o no retribuidas; o de los derechos de patria potestad, tutela, guarda o curatela, tenencia de animales, derecho de sufragio pasivo o de cualquier otro derecho"*; y *"k) La prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual"*; 3. Modifica el apartado 3 del artículo 40 en relación a la pena de privación del derecho a residir en determinados lugares o acudir a ellos que queda redactado como sigue: *"3. La pena de privación tendrá una duración de hasta diez años. La prohibición de aproximarse a la víctima o a aquellos de sus familiares u otras personas, o de comunicarse con ellas, tendrá una duración de un mes a diez años. La prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual tendrá una duración de un mes a diez años"*; 4. Modifica el artículo 45 respecto de la inhabilitación especial para profesión, oficio, industria o comercio u otras

actividades, incluidas las que se desarrollen o exploten en espacios virtuales, sean o no retribuidas, o cualquier otro derecho, que ha de concretarse expresa y motivadamente en la sentencia, que queda redactado: *"priva a la persona penada de la facultad de ejercerlos durante el tiempo de la condena. La autoridad judicial podrá restringir la inhabilitación a determinadas actividades o funciones de la profesión u oficio, retribuido o no, permitiendo, si ello fuera posible, el ejercicio de aquellas funciones no directamente relacionadas con el delito cometido"*; 5.

Modifican los apartados 2 y 4 y añade un nuevo apartado 5 al artículo 48 en cuanto a la prohibición de aproximarse a la víctima, o a aquellos de sus familiares u otras personas que determine el juez o tribunal: *"2. impide al penado acercarse a ellos, en cualquier lugar donde se encuentren, así como acercarse a su domicilio y a sus lugares de trabajo y a cualquier otro que sea frecuentado por ellos, aun cuando no se hallaren en ellos, quedando en suspenso, respecto de los hijos, el régimen de visitas, comunicación y estancia que, en su caso, se hubiere reconocido en sentencia civil hasta el total cumplimiento de esta pena"*; y en relación a la prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual *"4. Priva a la persona penada de la facultad del acceso o de comunicación a través de internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación durante el tiempo de la condena a los espacios virtuales que tengan relación directa con el delito cometido. En la resolución judicial deberá concretarse y motivarse expresamente el contenido o alcance de la prohibición"*; y, al respecto *"5. El juez o tribunal podrá acordar que el control de las medidas previstas en los apartados anteriores se realice a través de aquellos medios electrónicos que lo permitan"*; 6. En las penas de prisión inferior a diez años los jueces y los tribunales impondrán, atendiendo a la gravedad del delito, como penas accesorias algunas de las siguientes, modificando para ello el párrafo 3º y añadiendo un nuevo párrafo 4º al artículo 56.1 con el siguiente contenido: *"3º Inhabilitación especial para empleo o cargo público; profesión, oficio, industria, comercio, incluidos los que se desarrollen o exploten en espacios virtuales, sean o no retribuidos; ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento o cualquier otro derecho, la privación de la patria potestad, si estos derechos hubieran tenido relación directa con el delito cometido, debiendo determinarse expresamente en la sentencia esta vinculación, sin perjuicio de la aplicación de lo previsto en el artículo 579 de este Código. 4º. Prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual, cuando tengan relación directa con el delito cometido"*, Ciertamente, estamos ante la pena de alejamiento de los entornos virtuales —dentro del catálogo de penas privativas de derechos—; en concreto, la de prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro espacio virtual por un tiempo seis meses, cinco años o diez años dependiendo del delito; 7. Cuando se investigue un delito de los mencionados en el artículo 57 del Código Penal, el Juez o Tribunal podrá, de forma motivada y cuando resulte estrictamente necesario al fin de protección de la víctima, imponer cautelarmente al inculpado la prohibición de residir en un determinado lugar, barrio, municipio, provincia u otra entidad local, o Comunidad Autónoma. En las mismas condiciones podrá imponerle cautelarmente la prohibición de acudir a determinados lugares, tanto físicos como virtuales, barrios, municipios, provincias

u otras entidades locales, o Comunidades Autónomas, o de aproximarse o comunicarse con determinadas personas, con la graduación que sea precisa y a través de cualquier medio incluidas las redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual[111]; 8. En cuanto a la pena suprior o inferior en grado previsto por la ley para cualquier delito tendrá la extensión resultante de aplicación de las siguientes reglas: así se modifica el párrafo 6.º del artículo 70.3 que queda redactado: *"6.º Tratándose de privación del derecho a residir en determinados lugares o acudir a ellos, o de la prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual, la misma pena, con la cláusula de que su duración máxima será de veinte años"*; 9. El juez podrá condicionar la suspensión al cumplimiento de las siguientes prohibiciones y deberes cuando resulte necesario para evitar el peligro de comisión de nuevos delitos, sin que pueda imponerse deberes y obligaciones que resulten excesivas y desproporcionadas. Al respecto, se añade un nuevo párrafo numerado como 8ª bis al artículo 83.1, con el siguiente contenido: *"8ª bis. Prohibición de acceso o de comunicación a través de redes sociales, foros o plataformas virtuales cuando tengan relación directa con el delito cometido"*. 10. En cuanto a las medidas no privativas de libertad se añade un nuevo párrafo numerado como 7ª al artículo 96.3: *"7ª La prohibición de acceso o de comunicación a través de redes sociales, foros o plataformas virtuales cuando tengan relación directa con el delito cometido"*; 11. Ultrafalsificaciones: El proyecto da tratamiento penal a la ultrafalsificación (deepfake), término que emplea en su exposición de motivos para hacer referencia a los vídeos, fotos y audios que no son reales, pero lo parecen gracias a una manipulación extrema de imágenes y/o sonidos. Este delito se integra entre los cometidos contra la integridad moral de las personas, diferenciándolo de los cometidos contra la intimidad, el derecho a la propia imagen o contra el honor. A tal fin, el nuevo artículo 173 bis dispone que: *"Se impondrá la pena de prisión de uno a dos años a quienes, sin autorización de la persona afectada y con ánimo de menoscabar su integridad moral, difundan, exhiban o cedan su imagen corporal o audio de voz generada, modificada o recreada mediante sistemas automatizados, software, algoritmos, inteligencia artificial o cualquier otra tecnología, de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorias. La pena será de un año y seis meses a dos años, si la víctima es menor de edad o persona con discapacidad necesitada de especial protección. Se aplicará la pena en su mitad superior si dicho material ultrafalsificado se difunde a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías, de modo que aquel se hiciera accesible a un elevado número de personas en el espacio virtual. Las autoridades judiciales ordenarán la adopción de las medidas necesarias para la retirada de los contenidos a los que se refieren los párrafos anteriores, para la interrupción de los servicios que ofrezcan predominantemente dichos contenidos o para el bloqueo de unos y otros cuando radiquen en el extranjero"*.

La inclusión de este nuevo tipo delictivo cumple con el mandato contenido en la Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo sobre la lucha contra la violencia de género y de la violencia doméstica, que pretende garantizar que este tipo de conductas no queden impunes en los Estados miembros. La pena será de un año y seis meses a dos años, si la víctima es menor de edad o persona con discapacidad necesitada de especial protección. Se aplicará la pena en su mi-

tad superior si dicho material ultrafalsificado se difunde a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías, de modo que aquel se hiciera accesible a un elevado número de personas en el espacio virtual. Las autoridades judiciales ordenarán la adopción de las medidas necesarias para la retirada de los contenidos a los que se refieren los párrafos anteriores, para la interrupción de los servicios que ofrezcan predominantemente dichos contenidos o para el bloqueo de unos y otros cuando radiquen en el extranjero En España, uno de los incidentes con fotos manipuladas que más impacto tuvo en los medios de comunicación sucedió en septiembre del 2023. Varias chicas menores de edad denunciaron que había fotografías suyas desnudas, manipuladas con IA, que se encontraban circulando en internet. Todo ocurrió en Almendralejo (Badajoz), donde las madres de las víctimas (de entre 12 y 17 años) denunciaron la situación. La Policía Nacional detuvo a varios menores implicados en el caso. Para crear estas fotografías, los adolescentes habían utilizado una aplicación de IA que era capaz de hacer un montaje hiperrealista intercambiando el rostro o el cuerpo original de la víctima por el de otra persona; 12. Enmascaramiento de identidad: Así quien realice actos de carácter sexual con un menor de dieciséis años, será castigado con la pena de prisión de dos a seis años y con la pena de prisión correspondiente en su mitad superior cuando en la ejecución del delito, si la persona responsable haya utilizado una identidad falsa, ficticia o imaginaria, o se haya atribuido una edad, sexo u otras condiciones personales diferentes de las propias. Asimismo, quien contacte con un menor de dieciséis a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años con el fin de concertar un encuentro con el mismo para cometer cualquiera de los delitos sexuales, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación, engaño o empleando una identidad falsa, ficticia o imaginaria, o atribuyéndose el agresor una edad, sexo u otras condiciones personales diferentes a las propias. También, el que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años. Cuando el embaucamiento se lleve a efecto utilizando el agresor una identidad falsa, ficticia o imaginaria, o atribuyéndose edad, sexo u otras condiciones personales diferentes a las propias, la pena se impondrá en su mitad superior. A tal fin, se añade un nuevo párrafo i) al artículo 181.5 con el siguiente contenido: *"i) Cuando para facilitar la ejecución del delito, la persona responsable haya utilizado una identidad falsa, ficticia o imaginaria, o se haya atribuido una edad, sexo u otras condiciones personales diferentes de las propias"*; y también añade un nuevo apartado 3 al artículo 182, con el siguiente contenido: *"3. Si para facilitar la ejecución de las conductas definidas en los apartados anteriores la persona responsable hubiera utilizado una identidad falsa, ficticia o imaginaria, o se hubiera atribuido una edad, sexo u otras condiciones personales diferentes de las propias, la pena se impon-*

drá en su mitad superior"; 13. En cuanto a las agresiones sexuales a menores de 16 años: se modifica el artículo 183 con el siguiente texto: *"1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 181 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación, engaño o empleando una identidad falsa, ficticia o imaginaria, o atribuyéndose el agresor una edad, sexo u otras condiciones personales diferentes a las propias. 2. El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años. Cuando el embaucamiento se lleve a efecto utilizando el agresor una identidad falsa, ficticia o imaginaria, o atribuyéndose edad, sexo u otras condiciones personales diferentes a las propias, la pena se impondrá en su mitad superior"*; 14. Respecto al acoso sexual: se modifica el artículo 185 que queda redactado como sigue: *"El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de doce a veinticuatro meses. Cuando para facilitar la ejecución de la conducta la persona responsable hubiera utilizado una identidad falsa, ficticia o imaginaria, o se hubiera atribuido una edad, sexo u otras condiciones personales diferentes de las propias, la pena se impondrá en su mitad superior"*; y, también el artículo 186 que queda redactado: *"El que, a sabiendas, y por cualquier medio, vendiere, difundiere, exhibiere o pusiere a disposición, entre menores de edad o personas con discapacidad necesitadas de especial protección, material pornográfico, será castigado con la pena de prisión de seis meses a un año o multa de doce a veinticuatro meses. Cuando para facilitar la ejecución de la conducta la persona responsable hubiera utilizado una identidad falsa, ficticia o imaginaria, o se hubiera atribuido una edad, sexo u otras condiciones personales diferentes de las propias, la pena se impondrá en su mitad superior"*[112]; 15. El que induzca, promueva, favorezca o facilite la prostitución de un menor de edad o una persona con discapacidad necesitada de especial protección, o se lucre con ello, o explote de algún otro modo a un menor o a una persona con discapacidad para estos fines con la modificación del artículo 188.1:*"será castigado con las penas de prisión de dos a cinco años y multa de doce a veinticuatro meses. Si la víctima fuera menor de dieciséis años, se impondrá la pena de prisión de cuatro a ocho años y multa de doce a veinticuatro meses. Cuando para facilitar la ejecución de la conducta la persona responsable hubiera utilizado una identidad falsa, ficticia o imaginaria, o se hubiera atribuido una edad, sexo u otras condiciones personales diferentes de las propias, la pena se impondrá en su mitad superior"*; y, asimismo, el que solicite, acepte u obtenga, a cambio de una remuneración o promesa, una relación sexual con una persona menor de edad o una persona con discapacidad necesitada de especial protección *"será castigado con una pena de*

uno a cuatro años de prisión. Si el menor no hubiera cumplido dieciséis años de edad, se impondrá una pena de dos a seis años de prisión. Cuando para facilitar la ejecución de la conducta la persona responsable hubiera utilizado una identidad falsa, ficticia o imaginaria, o se hubiera atribuido una edad, sexo u otras condiciones personales diferentes de las propias, la pena se impondrá en su mitad superior" (modifica el apartado 4 del artículo 188); y, en fin, 16. Respecto al que captare o utilizare menores de edad o personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, se modifica el apartado 3 del artículo 189. Así se dispone que: *"Las penas correspondientes a los hechos a que se refiere la letra a) del párrafo primero del apartado 1 del presente artículo se incrementaran si concurre alguna de las circunstancias siguientes: a) Si en la comisión de los hechos se hubiera empleado violencia o intimidación, se impondrá la pena superior en grado a las previstas en los apartados anteriores. b) Si para facilitar la ejecución de los hechos el responsable hubiera utilizado una identidad falsa, ficticia o imaginaria, o se hubiera atribuido una edad, sexo o género u otras condiciones personales diferentes de las propias, se impondrá la pena prevista en los apartados anteriores en su mitad superior"*.

Pues bien, en este contexto, resulta esencial imponer sistemas de verificación de edad: el texto sometido a tramitación parlamentaria modifica la analizada Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual (LGCA) para establecer la obligación, por parte de los prestadores del servicio de intercambio de vídeos a través de plataforma, de establecer y operar sistemas de verificación de edad de los usuarios, en relación con los contenidos que puedan causar un perjuicio a las personas menores de edad, como la violencia gratuita o la pornografía. Estos sistemas deberán ser "por defecto" y deberán garantizar determinados niveles de seguridad y privacidad. El proyecto prevé también la posibilidad de interrumpir el servicio o de retirar contenidos, medidas que podrán ser acordadas por la Comisión Nacional de los Mercados y de la Competencia (CNMC) por incumplimiento de la obligación de establecer un sistema de verificación de la edad, siempre que ese incumplimiento atente o pueda atentar contra el principio de protección de la juventud y la infancia. Serán los Juzgados Centrales de lo Contencioso-Administrativo los competentes para autorizar judicialmente esas medidas, según el procedimiento previsto hasta ahora solo para la protección de la propiedad intelectual.

En fin, se elaborará una Estrategia Nacional sobre la protección de la infancia y adolescencia en el entorno digital en consonancia con la Estrategia Estatal de los Derechos de la Infancia y de la Adolescencia y la Estrategia Estatal para combatir las violencias machistas, y contará con la participación del Observatorio de la Infancia, el Observatorio Estatal de Violencia sobre la Mujer, las entidades del tercer sector, la sociedad civil, las organizaciones de consumidores y usuarios y, de forma muy especial, con las niñas, niños y adolescentes y con sus familias.

En este apartado procede, asimismo, indicar que, el Consejo de Ministros, en su reunión del 30 de enero de 2024, a propuesta de la Ministra de Juventud e Infancia, aprobó el acuerdo de creación de un comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. Al citado comité se le denominará como el "Comité de Personas Expertas". En dicho acuerdo, se estableció un plazo de seis meses para el Comité de Personas

Expertas elaborase un documento que, en materia de infancia, adolescencia y juventud: 1. Analizara las buenas prácticas en el entorno digital. 2. Señalara los principales riesgos y peligros a los que pueden enfrentarse en el entorno digital. 3. Formulara recomendaciones y actuaciones a implementar, distinguiendo entre las de corto, medio y largo plazo, que sirvan de hoja de ruta con el objetivo de que las distintas administraciones públicas garanticen, cada una en su ámbito competencial, el desarrollo integral de la infancia y la juventud. Lo cierto es que, la creación en 2024 del Comité de Personas Expertas para un entorno digital seguro de la juventud e infancia fue la plasmación políticamente más significativa de una demanda social, creciente desde hace algunos años. Tras la acelerada digitalización de los menores y adolescentes como consecuencia de las restricciones de movilidad de la pandemia de COVID-19, comenzó a cristalizar socialmente la preocupación sobre algunos aspectos de dicha digitalización. En ese largo camino, un punto clave fue, en 2023, la propuesta de Pacto de Estado en defensa de las y los menores en el entorno digital, la primera iniciativa de este calado en la que participaron las organizaciones más representativas de protección a la infancia. Como ya se ha dicho, la propuesta fue promovida por seis entidades de la sociedad civil —la Asociación Europea para la Transición Digital, promotora principal de la iniciativa, Save The Children, Fundación ANAR, iCMedia, Dale la Vuelta y UNICEF— y se enmarca en un contexto político muy concreto. Presentada en junio de 2023, pretendía sentar unas bases mínimas de consenso, más allá de los partidismos, ante las elecciones generales que se celebrarían en España un mes después, y el inicio del semestre de presidencia española de la Unión Europea, el 1 de julio. Las seis entidades promotoras compartían su preocupación sobre los riesgos que afrontan menores y adolescentes en los entornos digitales, al utilizar servicios diseñados para adultos, que pueden afectar a su socialización y potenciar posibles problemas de salud mental, como la ansiedad y la depresión, además de facilitar situaciones de violencia como el acoso escolar y sexual. Al mismo tiempo, señalaban cómo los dispositivos móviles se han convertido en una puerta a contenidos pornográficos, lo que genera una banalización de las relaciones sexuales, sexualización precoz y exposición a contenidos inapropiados. Por último, los firmantes también advertían sobre la captación masiva de datos de menores, con la perspectiva de ser perfilados para la venta a terceros con fines publicitarios.

Recientemente, se ha aprobado tal Informe sobre el desarrollo de un entorno digital seguro para la juventud y la infancia en el que se destaca: 1. La primacía del interés del menor. Recordemos que, El marco jurídico proporcionado por la UNCRC y la Observación General núm. 14 no solo establecen directrices claras para la toma de decisiones, sino que también impone una obligación legal a los Estados parte y a todos los actores involucrados en la protección de la infancia y la juventud. Esto refuerza la necesidad de políticas públicas y prácticas judiciales y administrativas que reflejen un compromiso firme con la promoción y protección de menores y adolescentes. Su interés superior abarca su desarrollo físico, emocional, educativo y social. Sin embargo, los intereses de otras personas (padres y madres, tutores, instituciones, etc.) pueden incluir derechos y obligaciones legales, así como intereses económicos, sociales o emocionales; 2. Desmitificar conceptos: "uso responsable", "nativo digital" y

"la regulación mata a la innovación" Desde los inicios de Internet han existido conflictos entre los que han defendido que la innovación tecnológica cambia —y debe cambiar— las relaciones entre las personas, las empresas y la forma de acceder a bienes y servicios. En última instancia, el acceso a Internet generaría sus propios sistemas de valores y normas. Del otro lado, se sostiene que los valores y normas que rigen el mundo de lo físico, y que son reglados por normas jurídicas, deben regir también en el ámbito digital. No debería haber unos principios para uno, y otros —o ningunos— para lo digital. El lenguaje no es neutro. Tal y como está ampliamente investigado por la psicología y la lingüística, tiene el poder de conformar nuestra realidad. Expresiones como "uso responsable", "nativos digitales", o "la regulación mata a la innovación", proliferan en el debate público, social, empresarial y político cuando se abordan las medidas de protección de niños, niñas y adolescentes (NNA) en el ámbito digital. En primer lugar, muchas de las plataformas que operan en Internet y los grupos de interés a los que han fidelizado con prácticas poco transparentes, ponen el acento en el "uso responsable" como la clave principal para evitar los efectos psicológicos, intelectuales y económicos generados por un abuso adictivo de las tecnologías. Pero, desgraciadamente, existen aplicaciones y plataformas que influyen de forma intencionada en el comportamiento de los usuarios (tanto personas adultas como NNA) mediante patrones oscuros, (dark patterns). Su objetivo es maximizar el tiempo de uso y el engagement, mediante notificaciones constantes, recompensas intermitentes (ej., los "me gusta", la utilización de emoticonos o los comentarios en redes sociales), el desplazamiento infinito, o los contenidos que apelan a la emoción de las o los adolescentes. De esta manera se crea una adicción que provoca comportamientos compulsivos de revisar el teléfono, las redes sociales o, directamente, no desconectarse de ellas. Es una cuestión especialmente preocupante en el caso de NNA, que aún no han desarrollado la capacidad de regular su uso, dado que su cerebro está en fase de maduración. El "uso responsable" solamente será eficaz si viene acompañado de políticas públicas, normas y sanciones para quienes las incumplan, estableciendo unos límites a la oferta de servicios de las empresas que contemplen los derechos de los ciudadanos digitales. Nativos digitales

En segundo lugar, se observa frecuentemente la aparición de la expresión "nativo digital". Esta justificaría que NNA actuales, cuentan de forma inherente con suficientes conocimientos para poder "navegar por las redes". Este término fue utilizado por primera vez en 2001 por el escritor y conferenciante Marc Prensky, en su artículo "Digital Natives, Digital Immigrants". Es importante resaltar, que, aunque el concepto se ha popularizado en el campo de la literatura académica (principalmente en el ámbito de la educación), no existe en su creación ningún fundamento científico o dato empírico que acredite que los NNA nacidos en la era digital posean capacidades y habilidades digitales innatas únicamente por haber crecido con la tecnología. Y menos aún que la facilidad y habilidad de acceso a las Tecnologías de la Relación, la Información y la Comunicación (TRIC) sea suficiente para implicar una navegación segura que proteja sus derechos de manera eficaz.

Este concepto de "nativo digital", además, puede fomentar una visión determinista de la tecnología, dando a entender que el simple acceso a dispositivos digita-

les garantiza ciertas habilidades y competencias. Pero no considera otros factores como la educación (habilidades digitales profundas o una comprensión crítica de la tecnología), el interés personal y el contexto social. La regulación mata a la innovación En tercer lugar, aparece la idea —repetida insistentemente desde el sector tecnológico— de que "la regulación mata a la innovación". Sin embargo, sectores como los de la alimentación, el farmacéutico o el de los contenidos culturales, son una clara muestra de cómo una exigente regulación, que vele por el bienestar de las personas y la seguridad jurídica, no desacelera la capacidad de innovar de las compañías. Por el contrario, ofrece garantías, controla riesgos y crea un marco justo para la competencia.

En tercer lugar, la mercantilización de los datos de NNA y el valor del dato. Igual que se mercantiliza con el dato en el mundo físico, sucede lo mismo en el mundo online. Pero en este último caso, muchas veces se hace de forma inadvertida. Numerosos productos o servicios que se ofrecen a NNA con apariencia de gratuitos, realmente no lo son. Lo cierto es que pagar con datos también es una forma de mercantilización. Sin embargo, el elemento más importante, el cálculo económico de la relación entre los datos que aporta el consumidor y la plataforma, todavía no ha sido abordado. Según el think tank europeo Epicenter, el hecho de que el consumidor no reciba ningún valor económico por sus datos no significa que este valor no exista. El precio que realmente está pagando, aunque no lo perciba, se denomina "valor en la sombra". En el mundo de los datos, este "valor en la sombra" es el beneficio adicional que un proveedor de servicios de mensajería instantánea o correo electrónico, las redes sociales, o las plataformas de intercambio de vídeos, entre otros, obtienen al utilizar los datos que cada usuario nuevo le facilita, así como cada dato adicional que el mismo usuario proporciona de forma gratuita. En otras palabras, es el coste de oportunidad que implica que el usuario no reciba una compensación económica a cambio del uso de sus datos. A más transacciones, más datos y más dinero para la big tech, o mayor su calidad, eficiencia o productividad. Un claro ejemplo de monetización —en este caso fallida— fue la iniciativa de la compañía estadounidense Meta al intentar usar datos personales de sus usuarios europeos para entrenar su inteligencia artificial[113].

En cuarto lugar: la prohibición de explotación; en quinto lugar: los neurodatos y las neurotecnologías: En los últimos años, ha sobrevenido un crecimiento en la utilización de neurotecnologías fuera del ámbito clínico, expandiéndose a áreas como la educación, el entretenimiento y la vigilancia. Este uso más amplio plantea preocupaciones éticas y legales, especialmente en lo que respecta a la privacidad y la protección de los derechos fundamentales. Los neurodatos podrían definirse como la información obtenida del cerebro y el sistema nervioso. Esta incluye los datos sobre la actividad cerebral y otras funciones neurológicas, que pueden recopilarse mediante diversas tecnologías, como electroencefalogramas o resonancias magnéticas funcionales. Pueden ser utilizados para distintos fines, desde la investigación médica hasta aplicaciones comerciales, pasando por el neuromarketing. En sexto lugar. La perspectiva de género. En séptimo lugar: el papel de la industria. En octavo lugar: los riesgos para la salud mental, Y, en noveno lugar: el consumo de pornografía; la violencia y los abusos sexuales.

VI. LAS AUTORIDADES DE CONTROL: EL PAPEL DE LA OFICINA EUROPEA DE INTELIGENCIA ARTIFICIAL Y LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS EN LA SEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD DE MENORES DE EDAD Y ADOLESCENTES.

La Oficina Europea de IA representa el centro de conocimientos especializados en materia de IA en toda la Unión Europea. Desempeña un papel clave en la aplicación del RIA, especialmente para la IA de uso general, fomentando el desarrollo y el uso de una IA fiable y la cooperación internacional. Apoya el desarrollo y el uso de una IA fiable, al tiempo que protege contra los riesgos de la IA. La Oficina de IA se creó en el seno de la Comisión Europea como centro de conocimientos especializados en IA y constituye la base de un sistema europeo único de gobernanza de la IA. Además, desempeña un papel clave en la aplicación de la Ley de IA al apoyar a los organismos de gobernanza de los Estados miembros en sus tareas. Hace cumplir las normas aplicables a los modelos de IA de uso general. Esto se sustenta en las competencias conferidas a la Comisión por la Ley de IA, incluida la capacidad de llevar a cabo evaluaciones de modelos de IA de uso general, solicitar información y medidas a los proveedores de modelos y aplicar sanciones. La Oficina de IA también promueve un ecosistema innovador de IA fiable para cosechar los beneficios sociales y económicos; y, en fin, garantiza un enfoque europeo estratégico, coherente y eficaz en materia de IA a escala internacional, convirtiéndose en un punto de referencia mundial.

Ahora bien, para una toma de decisiones bien informada, la Oficina de IA colabora con los Estados miembros y la comunidad de expertos en general a través de foros y grupos de expertos específicos. Estos combinan el conocimiento de la comunidad científica, la industria, los grupos de reflexión, la sociedad civil y el ecosistema de código abierto, asegurando que se tengan en cuenta sus puntos de vista y experiencia. Ciertamente, en una visión completa del ecosistema de IA, incluidos los avances en capacidades, despliegue y otras tendencias, la Oficina de IA fomenta una comprensión profunda de los posibles beneficios y riesgos.

La oficina de IA está compuesta por: 1. Unidad de Regulación y Cumplimiento que coordina el enfoque regulador para facilitar la aplicación y ejecución uniformes de la Ley de IA en toda la Unión, en estrecha colaboración con los Estados miembros. La unidad contribuirá a las investigaciones sobre posibles infracciones y a la gestión de las sanciones; 2. Unidad sobre seguridad de la IA centrada en la identificación de riesgos sistémicos de modelos de uso general muy capaces, posibles medidas de mitigación, así como enfoques de evaluación y ensayo; 3. Unidad de excelencia en IA y robótica que apoya y financia la investigación y el desarrollo para fomentar un ecosistema de excelencia. Coordina la iniciativa GenAI4EU, estimulando el desarrollo de modelos y su integración en aplicaciones innovadoras; 4. La Unidad de IA para el Bien Societal para diseñar y aplicar el compromiso internacional de la Oficina de IA en IA para el bien, como la modelización meteorológica, los diagnósticos del cáncer y los gemelos digitales para la reconstrucción; y, 5. Unidad de Innovación y Coordinación de Políticas en materia de IA que supervisa la ejecución de la estrategia de IA de la UE, supervisa las tendencias y la inversión, estimula la adopción de la IA a través de una red de centros europeos de innovación digital y la creación de fábricas de IA, y fomenta

un ecosistema innovador mediante el apoyo a espacios controlados de pruebas y pruebas en el mundo real.

Por su parte, la Comisión elaborará directrices sobre la aplicación práctica del presente Reglamento y, en particular, sobre: a) La aplicación de los requisitos y obligaciones a que se refieren los artículos 8 a 15 y el artículo 25; b) Las prácticas prohibidas a que se refiere el artículo 5; c) La aplicación práctica de las disposiciones relacionadas con modificaciones sustanciales; d) La aplicación práctica de las obligaciones de transparencia establecidas en el artículo 50; e) Información detallada sobre la relación entre el Reglamento y la lista de actos legislativos de armonización de la Unión enumerados en el anexo I, así como otras disposiciones de Derecho de la Unión pertinentes también por cuanto se refiere a la coherencia en su aplicación; y, f. La aplicación de la definición de sistema de IA que figura en el artículo 3 punto 1 del RIA (artículo 96.1).

En cuanto a la AEPD representa una de las instituciones que más ha impulsado y promovido el compromiso con la protección de los y las menores de edad en el entorno digital para garantizar sus derechos y libertades en relación con el tratamiento de sus datos personales. Desde 2015, con la adopción de su "Plan Estratégico", ha venido adoptando iniciativas y medidas en interés de NNA, como la creación del espacio temático "Educación y menores" en su web. Aquí incluye contenidos, materiales y recursos para fomentar el uso saludable, responsable y seguro de los dispositivos digitales y de los datos personales, además de un canal específico para consultas (WhatsApp, línea telefónica y correo electrónico). La Agencia también ha desarrollado acciones de sensibilización de familias y docentes con la realización sistemática de cursos de formación online, en colaboración con el Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado (INTEF) y el Instituto Nacional de Ciberseguridad (INCIBE), y campañas como las realizadas con UNICEF, "Un móvil es más que un móvil" y "La guía que no viene con el móvil". Estas contienen claves a tener en cuenta por las familias ante la entrega del primer móvil a sus hijos e hijas. Además, la AEPD convoca anualmente el premio a los centros educativos, personas y entidades que se distingan por su labor en pro del uso saludable y responsable de Internet por menores y adolescentes.

Asimismo, esta AEPD constituyó en 2019 un Grupo de Trabajo sobre "Menores, salud digital y privacidad" con el objetivo de estudiar y proponer iniciativas y medidas para proteger a los y las menores en el ámbito digital, en el que los servicios que se prestan y los contenidos que se ofrecen a través de redes sociales y servicios equivalentes requieren del tratamiento de datos personales para su operatividad. El Grupo de Trabajo, del que forman parte distintos actores implicados y comprometidos con la protección y salvaguarda del interés superior de los y las menores, del sector público y privado, como organizaciones profesionales y sociedades científicas, se viene reuniendo desde entonces para tratar sobre aquellos asuntos que afectan a su protección y seguridad en el mundo online. Los trabajos del Grupo han dado lugar a diversas iniciativas, entre las que cabe destacar, en materia de educación digital, el impulso y colaboración para la creación del portal Aseguratic, que contiene el más amplio repositorio de materiales, recursos y herramientas (catalogadas y ordenadas por materia, edades, fuente y destinatarios: docentes, familias, alumnos) disponible en la web del Instituto Nacional de Tecno-

logías Educativas y de Formación del Profesorado (INTEF); y en materia de salud digital impulsando la colaboración y elaboración de herramientas para prevenir y detectar usos inadecuados o adictivos a las TIC, como el Plan Digital Familiar de la Asociación Española de Pediatría. En este sentido, cabe destacar muy especialmente el Decálogo con los criterios y requisitos que han de reunir los sistemas de verificación de la edad en el acceso a contenidos online para adultos, de forma que sean eficaces y respetuosos con el marco de protección de datos y privacidad. Las diversas actuaciones realizadas por la Agencia para proteger a las personas en Internet han sido objeto de reconocimiento público en los últimos años, con 28 premios concedidos por parte de instituciones y entidades públicas y privadas, nacionales e internacionales.

Ante esta coyuntura, la Agencia establece las siguientes LÍNEAS ESTRATÉGICAS, que comprenden: 10 actuaciones prioritarias y 35 medidas.

La Agencia: 1. Apoya la iniciativa para la adopción de un Pacto de Estado promovida por organizaciones de la sociedad civil con medidas de consenso para la protección de la infancia y la adolescencia en Internet; 2. Colaborará, mediante la coordinación del Grupo de Trabajo de "Menores salud digital y privacidad", en el análisis jurídico y tecnológico de las propuestas y medidas de cara a la elaboración de un proyecto de Ley de protección integral a la infancia y adolescencia en los ámbitos en los que se han detectado necesidades (penal, procesal, administrativo, educativo, sanitario, de protección de datos —neurodatos y neuroderechos—, comunicaciones audiovisuales y consumo). 3. La Agencia ha elaborado un Decálogo con los principios y requisitos que han de observar los SISTEMAS DE VERIFICACIÓN DE LA EDAD para ser eficaces y respetuosos con la privacidad de quienes acceden a esos contenidos que, en un mundo globalizado, se proporcionan desde cualquier lugar. A este respecto: a. Impulsará la producción de apps que desarrollen estos sistemas conforme a los principios adoptados, colaborando en particular con la Comisión nacional de los Mercados y la Competencia (CNMC), la Fábrica Nacional de Moneda y Timbre (FNMT), el Ministerio del Interior y el Ministerio de Transformación Digital. b. Coordinará y promoverá la asunción de los principios y requisitos en el marco de la UE con la finalidad de que sirvan de referencia para el desarrollo de sistemas de verificación de la edad eficaces y garantistas en los Estados miembro. Para ello impulsará la adopción de una declaración por el Comité Europeo de Protección de Datos, y mantendrá contactos y reuniones con la Comisión Europea y el Parlamento Europeo a través de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE). c. Incentivará la adopción de los principios del decálogo en otros ámbitos internacionales, para lo que se presentarán a las autoridades en materia de privacidad y protección de datos reunidas en el seno de la Asamblea Global de Privacidad (GPA), a la Administración Federal de EEUU, la Federal Trade Commission y a la Autoridad de protección de datos del Estado de California (sede de la mayoría de los prestadores de servicios online), junto con la Red Iberoamericana de Protección de Datos (RIPD), cuya Secretaría ostenta la Agencia.

Para facilitar el papel de las familias, la Agencia intensificará la colaboración: 4. Con el Instituto Nacional de Ciberseguridad (INCIBE) para el análisis de las HERRAMIENTAS DE CONTROL PARENTAL y la actualización de las guías sobre privacidad y seguridad en Internet, y para la configuración de la privacidad en

redes sociales, aplicaciones de mensajería instantánea y principales navegadores. 5. Con el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) e INCIBE para proporcionar las familias educación, formación digital, recursos y materiales mediante módulos formativos. El ámbito escolar utiliza PLATAFORMAS EDUCATIVAS Y HERRAMIENTAS DIGITALES que tratan datos personales del alumnado, familiares y docentes que exige el análisis de su adecuación a la regulación del derecho a la protección de datos y su control como garantía de su cumplimiento, para lo que la Agencia: el refuerzo de las garantías de los derechos de los y las menores en internet El acceso y consumo de contenidos online inapropiados para menores exige la implantación de sistemas eficaces de verificación de la edad como garantía para la formación y desarrollo integral de los y las menores. 6. Colaborará activamente con las autoridades educativas para garantizar su adecuación a la regulación del derecho a la protección de datos y su control como garantía de su cumplimiento. 7. Llevará a cabo actuaciones de investigación a las plataformas, educativas y de aprendizaje, así como a las herramientas digitales que se utilizan en los centros escolares. 8. A través de los Consejos Generales de los Colegios Oficiales de Médicos, Psicólogos y Pedagogos, que participan en el Grupo de Trabajo, colaborará con las Administraciones educativas y sanitarias para fomentar la realización de evaluaciones de impacto en privacidad y salud digital en función de la edad y los riesgos para los y las menores. Lucha contra las prácticas ilícitas y nocivas que afectan a los y las menores en internet: La Agencia, como autoridad de control, está dotada de potestades de investigación y de sanción para supervisar el cumplimiento de la normativa de protección de datos. En el ejercicio de estas potestades ha iniciado actuaciones de investigación a páginas web de contenidos para personas adultas, así como a terceros de confianza en el ámbito de la verificación de la edad, que se han trasladado cuando ha sido necesario y cumpliendo lo establecido en el RGPD, a través del sistema de Información del Mercado interior (IMI) a las autoridades europeas de control en el marco de colaboración institucional y asistencia mutua. En este ámbito, la Agencia: 9. Priorizará el ejercicio de sus potestades de investigación a las páginas web de contenidos para personas adultas, en especial de pornografía, con respecto a la verificación de la edad para el acceso a dichos contenidos y al cumplimiento de la normativa de protección de datos de los y las menores. Actuando en cooperación con las autoridades de la Unión Europea cuando las páginas web no estén establecidas en España: y, 10. Realizará el análisis de los algoritmos y patrones adictivos que tienen como objetivo influir en el comportamiento y las decisiones de las personas usuarias, con relación a los datos y perfilados de los y las menores de edad, e impulsará la coordinación necesaria con el Comité Europeo de Protección de Datos.

En cuanto a la verificación de la edad: La protección de los menores en Internet es una de las prioridades no solo a nivel nacional, sino también desde Europa. El propósito es evitar que el acceso incontrolado de niños y niñas a contenidos inadecuados, que se materializa a través de la verificación de su edad. La AEPD cuenta con un decálogo de principios que deben guiar estos sistemas.

La verificación de edad es un sistema pensado para proteger a los menores de contenidos inadecuados en internet que, tal como sostiene, han de ser accesibles

para aquellas personas que deciden libremente consultarlas, siempre que cumplan con las condiciones de edad establecidas.

Pero, ¿qué se entiende como contenido inadecuado? Según la AEPD, este término se utilizará para aquellos sitios online restringidos solo a personas adultas, contenidos calificados para "mayores de 18 años" (pornografía, violencia extrema), sitios de Internet limitados al acceso por mayores de 14 años, y contenidos perjudiciales, adictivos o publicitarios prohibidos a personas menores de edad.

Los elementos que conforman los sistemas de verificación de la edad para proteger a los menores son cuatro: 1. Un mecanismo de verificación de edad, que proporcionará una información cierta sobre la autorización de acceso a contenidos orientados a personas adultas; 2. Unas políticas de calificación de sitios y contenidos por razones de edad. De este modo, se establece un criterio sobre qué sitios en Internet o qué contenidos en sitios generalistas se consideran orientados a adultos o tienen establecidos unos requisitos de limitación de acceso por edad; 3. Una calificación de los sitios, o de los contenidos, en función y aplicación de las políticas previamente establecidas. Esta calificación supone la aplicación de las políticas anteriores; y, Una ejecución de las políticas de acceso. De acuerdo con los elementos anteriores, se realizará el filtrado de los contenidos. En este aspecto están implicados no solo las entidades responsables de los sitios web y de las redes sociales, sino también los buscadores en Internet, las empresas de telefonía móvil y los fabricantes de videojuegos o dispositivos, entre otros.

En España, el entonces ministro para la Transformación Digital y de la Función Pública, José Luis Escrivá, presentó una Cartera Digital Beta, el "wallet" (portadocumentos digital) que incluye el sistema de verificación de la mayoría de edad en el acceso a contenidos para adultos, tras culminar la fase de diseño de la herramienta con la publicación de las especificaciones técnicas. Cartera Digital Beta será una aplicación móvil que almacenará de forma segura la credencial de mayoría de edad emitida por el Gobierno de España, que será presentada ante la plataforma de contenidos para adultos cuando se inicie la sesión. El sistema incorpora una doble autenticación para evitar que los menores accedan a través de los dispositivos de adultos. La aplicación incluirá otras funcionalidades desde su puesta en marcha e irá incorporando nuevas utilidades en el marco del ya mencionado Reglamento eIDAS2 relativo a la identidad digital europea.

Además, se ha diseñado una arquitectura de gobernanza basada en listas blancas de confianza que permite que los actores del sistema se identifiquen como tales. La lista blanca de plataformas para adultos gestionada por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, la lista blanca de aplicaciones de verificación gestionada por la Secretaría de Estado de Digitalización e Inteligencia Artificial y una última de emisores de credenciales gestionada por la Secretaría General de Administración Digital.

El Instituto Nacional de Ciberseguridad (INCIBE), por su parte, gestionará, con la colaboración de otros actores, un listado de páginas con contenido para adultos, no sometidas a la jurisdicción española, con el objetivo de que los navegadores puedan verificar la mayoría de edad antes de presentar sus contenidos.

Ahora bien, en la Memoria de la AEPD del año 2023 se destacó, como una de las principales preocupaciones de la Agencia es el acceso a los dispositivos móviles por parte de los menores en el entorno digital, así como el tiempo de uso

y los servicios de Internet a los que acceden, considerando los graves efectos perjudiciales para su salud (física, mental, psicosocial, sexual); su neurodesarrollo; su aprendizaje; sus relaciones familiares y sociales o a la monetización de sus datos. Por este motivo, las iniciativas adoptadas por la AEPD pueden dar respuesta a esta situación.

A principios de 2024, esta Agencia diseñó una nueva estrategia reforzada, constituida por 10 actuaciones prioritarias y 35 medidas, agrupadas en tres ejes estratégicos: la colaboración regulatoria, el refuerzo para garantizar los derechos de la infancia y la adolescencia y el ejercicio de las potestades de investigación y sanción, además de incluir dos grandes bloques centrados en la educación, y la salud y el bienestar digital.

En el marco de la labor de concienciación que le corresponde, la AEPD difundió, junto a la Fundación Atresmedia, la campaña "No a la barra libre digital", para alertar sobre los peligros del acceso de los y las menores a contenidos inadecuados a través del móvil y promover el acompañamiento en el uso de la tecnología en la infancia y adolescencia. Esta campaña recomendaba a las familias que retrasasen la entrega del móvil a sus hijos e hijas y los acompañasen en su interacción con el mundo digital, evitando así que accedieran a contenidos inapropiados y perjudiciales para su desarrollo, como contenidos pornográficos o violentos. La campaña comenzó a emitirse el 14 de noviembre bajo el hashtag #Noalabarralibredigital, y se difundió en todos los canales de televisión del Grupo Atresmedia: Antena 3, la Sexta, Nova, Neox, Mega y Atreseries, y en sus soportes multimedia, así como en la página web y redes sociales de la AEPD y la página web y las redes sociales de la Fundación Atresmedia. Otra de las acciones de sensibilización que divulgó esta Agencia en 2024 llevó por título "Hay más riesgos en Internet que en la vida real", relacionada con el acceso online por los y las menores a contenidos para personas adultas, en especial a la pornografía que, según los estudios e informes de organizaciones especializadas señalan que, se viene produciendo en torno a los 9 años, una edad en la que su desarrollo cognitivo no les permite entender lo que están viendo, pues su personalidad no está formada y genera importantes desórdenes en la concepción de las relaciones sexuales y del rol de la mujer. La campaña contó con la colaboración de Atresmedia, Mediaset España y RTVE, que se comprometieron a la difusión en sus respectivos canales, reforzando así su compromiso en la difusión de los derechos de la infancia y adolescencia en el entorno digital.

Asimismo, la AEPD continuó actualizando los contenidos de la sección específica de su página web dedicada al tratamiento de datos personales de menores y al ámbito educativo; del mismo modo que, mantuvo abierto el canal de atención y consulta específico para menores de edad, permitiéndoles tanto a ellos y ellas como a sus representantes, plantear dudas y obtener orientación sobre cuestiones relacionadas con la protección de sus datos en el entorno digital. También, durante 2024, la AEPD promovió el Pacto Digital para la Protección de las Personas, una iniciativa que busca involucrar a diferentes actores en la protección de los derechos de la ciudadanía en el entorno digital. Dentro de este mismo ámbito de protección de menores en el entorno digital, la Agencia, además de ofrecer recomendaciones para las familias a través del Plan Digital Familiar, proporcionando pautas y consejos prácticos para ayudar a los padres y madres a proteger a sus hijos e hijas en el entorno digital, también presentó dos informes sobre la influencia

de los patrones adictivos en Internet, especialmente en menores de edad, y cómo afectan a los derechos fundamentales. Ambos con el objetivo de concienciar sobre los posibles daños a la integridad física y mental que puede causar la exposición prolongada a estos patrones basados en sus datos personales. Una de las iniciativas más pioneras de la Agencia en los últimos años ha sido la relacionada con los sistemas de verificación de la edad. Esta propuesta fue presentada a finales de 2023 y experimentó un notable desarrollo tanto a nivel nacional como internacional, captando un interés relevante y siendo reconocida por su innovación y relevancia en el ámbito de la protección de la privacidad y la seguridad en línea.

Por otra parte, en una reunión celebrada en el plenario del Comité Europeo de Protección de Datos (CEPD) se adoptó un Dictamen sobre la determinación de la edad para el uso de servicios online que requieren de una edad mínima para poder acceder a ellos. En el contexto de la protección de los menores en Internet, se llevaron a cabo dos iniciativas fundamentales que destacaron por su carácter pionero y su relevancia en la creación de un entorno digital más seguro para los niños/niñas y adolescentes. La primera de ellas fue la publicación de un Informe sobre la influencia de los patrones adictivos en Internet, que aborda de manera profunda los efectos de los mecanismos y patrones diseñados para fomentar el uso continuo de Internet, en particular en lo que respecta a los y las menores de edad. Este informe examina cómo las plataformas digitales, mediante algoritmos y diseños de interfaces, pueden generar conductas adictivas que impactan negativamente en el bienestar de los y las menores, afectando tanto su desarrollo emocional como psicológico.

La segunda acción relevante fue la elaboración de una Nota Técnica titulada "Internet seguro por defecto para la infancia y el papel de la verificación de edad". Esta nota se centra en la necesidad de establecer medidas tecnológicas y legales que garanticen que los servicios y plataformas digitales ofrezcan una experiencia de navegación segura por defecto para los y las menores, reduciendo al mínimo los riesgos asociados al acceso a contenidos inapropiados o peligrosos. Además, subraya la importancia de la verificación de edad como una herramienta clave para proteger la privacidad y la seguridad de los niños/niñas y adolescentes en línea, asegurando que sólo puedan acceder a servicios adecuados a su edad y que se respeten sus derechos en el entorno digital. En el ámbito de las acciones de asesoramiento y el compromiso de la AEPD con la protección del menor, se colaboró con el Grupo Técnico de verificación de edad del Ministerio de Transformación Digital y Políticas Públicas y con el Comité de Expertos para la generación de un "entorno digital seguro para la juventud y la infancia".

Ahora bien, al igual que con la IA, van a ser de obligatoria referencia para la Agencia todas las cuestiones relacionadas con los espacios de datos. La disponibilidad de datos de alta calidad se constituye en un elemento clave para el entrenamiento de modelos de IA y su uso tiene el potencial de ser un factor de ayuda a la hora de mejorar la toma de decisiones y la personalización de servicios. Sin embargo, el acceso masivo a datos plantea retos significativos en términos de privacidad y protección de los derechos de las personas. En este contexto, los datos sanitarios, debido a su naturaleza especialmente sensible y otros tipos de datos provenientes de espacios de datos sectoriales, cobran especial relevancia por su sensibilidad y posible impacto sobre nuestra sociedad. La reutilización de datos

para fines distintos a aquellos para los que fueron recolectados originalmente es y será, un eje fundamental en la construcción de espacios de datos de calidad.

En relación con los neurodatos, durante la sesión del encuentro de la Red Iberoamericana de Protección de Datos (REDIPD) celebrada con motivo de su XX aniversario, la AEPD participó en la Declaración sobre neurodatos de la REDIPD aprobada por el Comité Jurídico Interamericano de la OEA. En dicha Declaración, se vino a subrayar que, si bien en el ámbito sanitario existe un marco jurídico específico que incorpora garantías adecuadas para los tratamientos de neurodatos, en otros ámbitos con tratamientos que conllevan fines distintos de los de salud, en los que existe monitorización de la actividad neuronal, se produce una ausencia de regulación sectorial específica que proporcione garantías adecuadas para dichos tratamientos; lo que viene a suscitar importantes preocupaciones éticas y jurídicas sobre el impacto final en principios, derechos y libertades fundamentales como la dignidad humana, el libre desarrollo de la personalidad, la identidad y la autonomía, el derecho a la intimidad, la libertad de pensamiento y de expresión, la integridad física y psíquica, la salud física y mental, etc. motivos por los que la Declaración crea un Grupo de Trabajo sectorial al objeto de analizar las bases jurídicas de los tratamientos en función de su finalidad, sus principios, límites y garantías aplicables en el marco de la normativa de protección de datos personales al tratamiento de neurodatos. A tal fin, la AEPD también ha impulsado la protección de los neuroderechos en el seno de las actividades del Grupo de Berlín, participando en la elaboración de varios documentos en los que se exploraron los riesgos que pueden presentar estas tecnologías combinadas con otras como la realidad extendida, los Grandes Modelos de Lenguaje (LLM) en IA. A estas acciones se suma también la participación de la AEPD en los grupos ISO donde se aporta la experiencia y el conocimiento en esta materia a modelos de normas que en el futuro puedan convertirse en estándares de los sectores de actividad en los que estas tecnologías tendrán aplicación. En definitiva, la AEPD entabló un diálogo activo con expertos en neurociencia, tecnología, ética y derecho, así como con representantes del sector privado y público, para comprender en profundidad las implicaciones del tratamiento de neurodatos y proporcionar directrices y orientaciones para abordar el principio de responsabilidad activa del RGPD. Estas colaboraciones permitieron recoger diferentes perspectivas y enriquecer el debate sobre cómo interpretar y aplicar el RGPD en este contexto tan complejo.

En definitiva, las cuestiones que se encuentran en desarrollo y que requerirán de un impulso mayor a lo largo del 2025, son las relacionadas con la IA, tanto en lo que afecta a la Decisión de la posible designación de la AEPD como Autoridad de Vigilancia de Mercado, como hacer un seguimiento de la implementación del tratamiento de incidentes graves de sistemas de IA, integrarse en los grupos de la Competent Authorities in Artificial Intelligence específicamente de notificación de incidentes y transparencias, participar en el EDPB interplay GDPR-AIA, colaborar en el desarrollo de los mecanismos de identidad digital con relación al eIDAS2 y la cartera digital europea, así como el desarrollo de orientaciones y la participación en organismos internacionales en lo relativo a neurodatos, datos genéticos o biométricos. Asimismo, es de enorme importancia la automatización de la gestión de brechas de datos personales para hacer frente al incremento de las notificaciones de forma eficiente, para servir de protección a los interesados y de apoyo a los

responsables; el impulso y actualización de las guías, orientaciones y herramientas de gestión del riesgo y evaluación de impacto, con un enfoque más práctico y desplegando un análisis formal de las amenazas en protección de datos, en línea con los estándares y la industria, así como actualizar las herramientas Notifica y Comunica Brecha para proporcionar una nueva herramienta inter-autonómica[114].

De todas formas, junto con el control parental, en los dispositivos con acceso a internet, se exige el desarrollo de herramientas de verificación de edad con el fin de garantizar un entorno digital más seguro. EEUU se han propuesto diversas normas para exigir la verificación de edad en plataformas con contenido para adultos (Texas, California, Utah). Y han aprobado leyes que obligan a plataformas como Apple store y Google Play a verificar la edad de los usuarios antes de permitir descargas las aplicaciones (Texas y Utah). Por su parte, en California, la Ley SB976 prohíbe que las plataformas digitales ofrezcan *feeds* adictivos a menores sin consentimiento parental. Además, a partir de 2027 será obligatorio para las plataformas implementar técnicas de verificación de dad para identificar usuarios menores y adoptan el contenido que les proporcionan. Exigen que os menores de 18 años cuentan con el consentimiento de sus padres para descargar aplicaciones o realizar compras en ellas.

Por su parte, China y la India han optado por técnicas de reconocimiento facial para verificar la edad de los usuarios, aunque ello pueda afectar a la privacidad.

En Alemania, la Comisión Alemana para la Protección de los Menores en los Medios de Comunicación ha aprobado el uso de tres sistemas de verificación de la edad mediante herramientas de Inteligencia Artificial, para evitar que los menores se vean expuestos a contenidos nocivos, según ha informado EURACTIV-Berlín.

Este organismo público alemán se ocupa de supervisar la protección de los menores en la televisión privada nacional y en Internet.

Los sistemas de IA aprobados por ese organismo estatal germano utilizan métodos de aprendizaje automático para analizar la edad de una persona en base a determinados parámetros biométricos.

Para tal fin, el organismo supervisor alemán ha estudiado tres sistemas diferentes de IA para la verificación de la edad. Se trata de programas informáticos de "estimación de la edad (mediante reconocimiento facial)", además de los programas informáticos "Age Verification" y "Yoti", objeto actualmente de análisis previo antes de darles la certificación de uso.

En todo caso, la autoridad de protección de la infancia ha previsto como mecanismo de seguridad para comprobar la edad real de aquellos niños o adolescentes que parecen mayores de lo que son, la existencia de un margen de error para la estimación de cinco años.

En España, además dos empresas españolas Bouncer Digital y Secture están trabajando en nuevos sistemas de conexión que protejan a los menores de contenido inadecuado con el desarrollo de una aplicación que utiliza biometría facial e IA, pues, representa su objetivo principal y misión proteger a los menores y, por ende, hacer de internet un lugar seguro para todos los usuarios. Esta solución está diseñada para cualquier web, e-commerce, app móvil o plataforma del mundo.

VII. LA RESPONSABILIDAD CIVIL DE LOS PROGENITORES, TUTORES Y CENTROS DOCENTES NO SUPERIORES.

El artículo 1903.2 del Código Civil establece que "los padres son responsables de los daños causados por los hijos que se encuentren bajo su guarda". El fundamento de la responsabilidad de los padres por los hechos dañosos de sus hijos que, están bajo su guarda se encuentra en la culpa *in vigilando* o *in educanda* de los propios padres, pues, como contenido de la patria potestad está en tenerlos en su compañía, educarlos y proporcionarles una educación integral (artículo 154 del citado cuerpo legal)[115]. Estamos ante una responsabilidad subjetiva o por culpa, directa, por culpa propia y por hecho ajeno[116]. Si bien, esta responsabilidad cesa cuando los padres prueben que emplearon toda la diligencia de un buen padre de familiar para prevenir el daño[117]; no obstante, en la mayoría de los casos no se admite tal exoneración de responsabilidad al no admitirse la prueba exoneratoria contemplada en el párrafo final del citado artículo 1903 del Código Civil, lo que ha llevado a la doctrina a considerar que, estamos ante un supuesto de responsabilidad cuasiobjetiva y, a la vez son muchas las resoluciones que destacan, precisamente, el matiz objetivo o cuasiobjetivo o calificándola de responsabilidad por semiriesgo[118]. Los sujetos responsables son ambos progenitores, que tienen al menor bajo su guarda —responsabilidad solidaria—[119]. Doble criterio de atribución, si bien, a diferencia de la responsabilidad de los tutores no se exige la convivencia del menor con sus padres[120]. Por lo que, atendiendo a tales criterios en caso de separación o divorcio la responsabilidad corresponde a quien tenga atribuida la guarda y custodia[121], sin perjuicio de exigir la responsabilidad al progenitor que está ejerciendo su derecho de visitas, precisamente, cuando el daño se produce durante ese periodo temporal, sin perjuicio de probar la responsabilidad también del otro progenitor por culpa *in educando*[122]. Igualmente, que en el caso de custodia compartida en la que se atribuye de forma alterna por periodos temporales determinados la guarda y custodia, atribuyéndose la responsabilidad al que tenga la guarda en el momento de producción del daño, salvo que, asimismo, se pruebe la responsabilidad de ambos por culpa *in educando* en cuanto que, la titularidad en ambos casos sigue siendo conjunta. Por otra parte, la responsabilidad de los padres puede concurrir con la de otras personas que, con su conducta contribuyeron a la causación del daño (guardador de hecho permanente no ocasional), moderándose su responsabilidad —reduciendo la cuantía—[123]. Señala YZQUIERDO TOLSADA como requisitos de esta responsabilidad parental: 1. Que el acto dañoso del hijo sea objetiva y comúnmente negligente; 2. Que los hijos se encuentren bajo su guarda; y 3. La culpa de los padres[124]. En cuanto el patrimonio que asume la deuda que se deriva de la responsabilidad, será en caso del régimen matrimonial de gananciales los bienes comunes (artículo 1367 del Código Civil)[125], salvo que, uno de los progenitores se exonere de responsabilidad probando su diligencia, siendo, en consecuencia, la deuda privativa (artículo 1373 del Código Civil). Si estamos ante un régimen de separación de bienes, de las obligaciones contraídas por las deudas comunes, responden ambas cónyuges, sin perjuicio del reparto interno entre cada uno en proporción a sus recursos económicos (artículo 1438 del Código Civil); y, en fin, el régimen de participación por la remisión del artículo 1413 del Código Civil se aplica las mismas reglas del régimen separación de bienes; no obstante,

si uno de los cónyuges abona la cantidad que corresponde asumir a ambos, aquél ostentará un crédito contra su consorte que, se computará en el patrimonio final del cónyuge acreedor y se deducirá del patrimonio del cónyuge deudor (artículo 1426 del Código Civil)[126].

En este contexto, los padres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales (artículo 84.1 de la LOPDYGDD). Lo que forma parte del ejercicio de la patria potestad (artículo 154 del Código Civil) y de la tutela (artículo 269 del Código Civil)[127]; y, por otro, los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información (artículo 92 de la citada LOPDYGDD).

Por lo que, cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes —páginas web del centro educativo o las personas físicas o jurídicas organizadoras de actividad o cualquier otro soporte publicitario digital— deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de la LOPDYGDD.

Ahora bien, con respecto a la responsabilidad penal de los menores de edad, el artículo 19 del Código Penal fija la edad penal en los dieciocho años, por lo que, los menores de dicha edad no serán responsables penalmente conforme tal Código, ni, en coherencia, los padres serán responsables civilmente por los actos delictivos cometidos por sus hijos menores de edad conforme, asimismo, lo previsto en el citado cuerpo legal. La mencionada Ley Orgánica 5/2000 de 2 de enero es la que regula la responsabilidad penal de los menores de dieciocho años. Así, por un lado, el artículo 3 de esta LORPM dispone que "cuando el autor de los hechos mencionados en los artículos anteriores sea menor de catorce años, no se le exigirá responsabilidad con arreglo a la presente Ley, sino que se le aplicará lo dispuesto en las normas sobre protección de menores prevista en el Código Civil y demás disposiciones vigentes". Por lo que, los menores de catorce años serán inimputables penalmente y la eventual responsabilidad civil en que incurran los padres se regirá por lo dispuesto en el Código Civil. Por otro lado, el artículo 61.3 de dicho cuerpo legal establece que "cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicio causados sus padres, tutores, acogedores y guardadores legales o de hecho por este orden. Cuando éstos no hubieran favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos"[128]. De forma que, serán imputables penalmente por los delitos o faltas cometidos por los menores mayores de catorce años conforme esta LORPM y, asimismo, se concreta quienes serán responsables civilmente. Como señala YZQUIERDO TOLSADA estamos ante una responsabilidad objetiva de los sujetos enumerados en el mencionado precepto y, añade que, hay varias cuestiones problemáticas "la primera hace referencia al propio diseño del consorcio

de los responsables solidarios, pues, la expresión "por este orden" provoca serias dudas. La segunda se refiere al alcance de la facultad de moderación del juez en los casos en los que no haya contribución dolosa o gravemente culposa de quienes aparecen en la norma respondiendo junto al menor". Ante lo que se pregunta "¿Es una moderación del *quantum* resarcitorio o solo una moderación *ad intra*, exclusivamente referida a la determinación de las cuotas?"[129].

En todo caso, este precepto establece la responsabilidad solidaria del menor mayor de catorce años y de sus padres, tutores, acogedores y guardadores legales o de hecho por este orden, sin exigir que concurra otra circunstancia y sin perjuicio de la facultad moderadora que corresponde al juez, cuando aquellos no hubieran favorecido la conducta del menor con dolo o negligencia. Aunque se dispone en el artículo 61.3 que se responde por este orden, la interpretación mayoritaria de la doctrina se inclina por entender que, no estamos ante un orden excluyente de personas, sino que responde en cada caso quien tenga la guarda del menor[130].

En el ámbito de la tutela, el artículo 1903.3 del Código Civil establece que los tutores son responsables "de los perjuicios causados por los menores e incapacitados que están bajo su autoridad y habitan en su compañía". En este caso, la convivencia es el criterio que determina la responsabilidad civil de los tutores, máxime si hay un tutor de la persona y otro del patrimonio (artículo 236.1 del Código Civil). Si son varios los tutores que conviven con el menor responden solidariamente[131]. Si el tutor es una persona jurídica privada el régimen de responsabilidad viene también determinado por lo previsto en el artículo 1903.4 del Código Civil —responsabilidad del empresario por los daños y perjuicio causados por su dependiente—; si se trata de persona jurídica pública les resulta aplicable lo previsto en el artículo 36.2 de la Ley 40/2015, de 1 de octubre de Régimen Jurídico del sector público que, prevé la repetición contra el personal al servicio de la Administración, si hubiera existido dolo o negligencia grave en su actuación.

Por otra parte, al igual que, sucede con la responsabilidad de los padres, el artículo 61.3 de la LORPM prevé también la responsabilidad civil de los tutores, si bien el juez puede moderar su responsabilidad, si no hubieran favorecido la conducta delictiva del menor con dolo o negligencia grave.

Por lo que, los padres y tutores responden civilmente por los daños ocasionados por sus hijos y tutelado sean o no imputables penalmente, tanto si la conducta dañosa ha tenido lugar en un entorno presencial o digital[132].

En todo caso, cabe que ante la intromisión ilegítima al derecho al honor de uno de los progenitores por parte de la hija, pueda estar legitimado pasivamente el otro progenitor y responder civilmente. Así la sentencia de la Audiencia Provincial de Tarragona, secc. 3ª, de 12 de diciembre de 2019[133] ante la publicación de la menor (hija del actor) en su cuenta de Instagram que su padre la había maltratado psicológicamente durante nueve años. Acreditado la falsada de la citada publicación y que le había provocado al actor un empeoramiento del trastorno depresivo y sintomatología ansiosa que venía padeciendo, se condena a la madre de la menor que ostenta la guarda y custodia a indemnizar en la cantidad de 1.000 euros por daños morales.

Respecto a los centros docentes de enseñanza no superior, el artículo 1903.5 del Código Civil señala que "las personas o entidades que sean titulares de un Centro docente de enseñanza no superior responderán por los daños y perjuicios

que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares, extraescolares y complementarias". La responsabilidad se fundamenta en la culpa *in vigilando* o deber de vigilancia que incumbe al Centro sobre sus alumnos menores de edad y en la culpa *in eligiendo* por la elección del personal docente o administrativo[134]. Esta responsabilidad subjetiva o por culpa no opera si logra probar que emplearon toda la diligencia de un buen padre de familia para prevenir el daño[135]. Los deberes de vigilancia de los padres de los menores se transfieren a los profesores del centro desde el mismo momento de la entrada en el mismo hasta la salida de él, una vez finalizada la jornada escolar[136]. Por su parte, el artículo 1904 párrafo 2 del Código Civil se refiere al derecho de repetición frente al personal docente "si éstos hubieren incurrido en dolo o culpa grave en el ejercicio de sus funciones que fueran causa del daño". Esta responsabilidad civil prevista en el Código Civil se aplica a los centros docentes privados y concertados; pues, si estamos ante centros docentes públicos procede la aplicación del régimen de responsabilidad de la Administración por el funcionamiento normal o anormal del servicio educativo. El artículo 9.4 de la LOPJ establece en estos casos como jurisdicción competente la contenciosa-administrativa en relación con las pretensiones que se deduzcan frente a la Administración del Estado o autonómica o municipal por el personal a su servicio, incluso si se ejercita frente a sujetos privados (compañía aseguradora).

Respecto a los ilícitos penales cometido por los alumnos menores mayores de catorce años; no obstante, la falta de mención a los Centros Docentes en el artículo 61.3, no impide que se le incluyan en la categoría de guardadores de hecho y, en consecuencia, responsables civiles ante la conducta delictiva de sus alumnos menores de edad[137].

En todo caso, como derechos de la era digital la LOPDYGDD hace referencia en su artículo 83, precisamente, al derecho a la educación digital. Así corresponde al sistema educativo garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje en el uso de los medios digitales que, sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Para ello, la Administración educativa deberá incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital, así como pos elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red. Asimismo, se prevé que, para conseguir la completa implementación de este derecho, el profesorado habrá de recibir las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos fundamentales y particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos. en cuanto a la enseñanza universitaria, se dispone, asimismo, que los planes de estudios de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado habrán de garantizar la formación en el uso y seguridad de los medios digitales y en la garantía de os derechos fundamentales en internet. Por otra parte, las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquellos en que habitualmente se

desempeñen funciones que impliquen el acceso a datos personales, materias relacionadas con la garantía de los derechos digitales y, en particular, en la protección de datos.

En todo caso, recordemos que, la utilización o difusión de imágenes o información personal de los menores en redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales, podrá determinar la intervención del Ministerio Fiscal que, instará al respecto las medidas cautelares y de protección previstas en el artículo 84.2 de la LOPDYGDD y el artículo 4 de la LOPJM. Al respecto, los centros docentes pueden limitar o incluso prohibir el uso de dispositivos electrónicos durante la jornada escolar, se trate de actividades escolares, extraescolares o complementarias; o, incluso controlar el uso que se haga de los mismos, previa información a los alumnos menores y sus padres. De no restringir el uso, el centro escolar asume los daños que se puedan derivar del uso indebido de los mismos, y, el acceso a través de los mismos a redes sociales donde se publiquen fotografías o se graben imágenes de otros alumnos o profesores durante la jornada escolar. Asimismo, puede aplicar las medidas tecnológicas precisas para evitar que los medios tecnológicos que los centros docentes aporten a los alumnos para el desarrollo de su actividad escolar, sean utilizados indebidamente mediante los controles adecuados.

Precisamente, en el cumplimiento del deber de proteger a los menores (alumnos) frente a cualquier situación de dañosa que sufra por la actuación de otro alumno y, máxime se trate de una situación de acoso o violencia que sufran aquellos en las instalaciones del Centro docente durante la jornada escolar desarrollando actividades escolares, extraescolares y complementarias, la sentencia de la Audiencia Provincial de Vizcaya, sección 5ª, de 25 de enero de 2019[138] ante la acción de responsabilidad frente al Centro escolar ejercitada por los padres de una alumna, la cual fue grabada desnuda mientras se duchaba en los vestuarios por una compañera con el teléfono móvil, difundiéndose las imágenes de la menor por Internet, considera la Audiencia que, el Centro escolar demandado sí incurrió en responsabilidad por tan lamentable suceso. La sentencia declara probado con la pericial practicada que, la captura y difusión de imágenes se produjo en el seno de una situación de acoso escolar que la hija menor ya venía padeciendo en el Centro escolar, con lo que el suceso que tuvo lugar el 15 de mayo de 2015 en las duchas de los vestuarios no puede calificarse de mera incidencia puntual o aislada. Por el contrario, es la culminación de un proceso de acoso escolar en sentido estricto, prologando en el tiempo aunque no haya presentado rasgos de fuerte o extrema violencia verbal o física, sí que se ha caracterizado por el desarrollo de una serie de conductas llevadas a cabo por algunas compañeras de la menor Lourdes de forma explícita en unos casos y en otros a través de mecanismos más sutiles de fustigación y de desprecio que han ido ocasionando en la afectada confusos y reiterados sentimientos de humillación, discriminación y exclusión precisamente en el patio y lugares de visitas programadas, sin que los responsables del Centro hubiese advertido lo que estaba ocurriendo. Las imágenes difundidas a través de redes sociales son nítidas y permiten identificar perfectamente a la alumna, lo que evidencia que su captación no fue una mera casualidad, sino fruto de ese contexto de acoso que sufría la menor. El suceso implica una total y absoluta negligencia en la actuación del centro escoñar en cuanto al

control del uso de los móviles, pues revela un fracaso total de los supuestos controles que se venían realizando para impedir un uso indebido de los teléfonos móviles, particularmente en un área especialmente delicada, y sensible como son las duchas y los vestuarios. La adopción de medidas que puedan considerarse adecuadas con posterioridad a producirse el suceso revela que las mismas podrán haberse aplicado con anterioridad y haber evitado que se captaran las imágenes de la hija de los demandantes. Concluye la Audiencia que una vez probada la responsabilidad del Centro escolar a la luz del artículo 1903 del Código Civil, debe estimarse la acción contra el mismo ejercitada por cuanto ha quedado acreditado el daño causado a la menor Lourdes y a su entorno, también como consecuencia de la actuación negligente del Centro educativo y se le condena al Centro a abonar a la parte actora la cantidad reclamada en la demanda de 6.320 euros.

VIII. BIBLIOGRAFÍA.

ABRIL CAMPOY, J.M. (2003). "La responsabilidad de los padres por los daños causados por sus hijos", *Revista Crítica de Derecho Inmobiliario, número 675, enero-febrero*, pp. 11-54.

ALAMILLO-DOMINGO, I. (2024). "La verificación de edad para el acceso a servicios digitales a la luz del nuevo marco de identidad del reglamento EIDAS 2", *LA LEY Derecho de familia, nº 44, octubre*, pp. 18-31.

ALMENAR PINEDA, FCO. (2024). "Nuevos escenarios para el Derecho y el Derecho Penal en la protección de los menores: el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales", *LA LEY Derecho de familia, nº 44, octubre*, pp. 65-71.

ANDREU MARTÍNEZ, Mª.B. y GRIMALT SERVERA, P. (2024). "Responsabilidad civil, consentimiento y difusión de datos de menores en entornos digitales", *LA LEY Derecho de familia, nº 44, octubre*, pp. 40-49.

ARRELLANO TOLEDO, W. y MERCHÁN MURILLO, A. (2024). "La obligación de conservar registros de los sistemas de alto riesgo en el Reglamento de Inteligencia Artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

ARGELICH COMELLES, C. (2025). "La proyectada Ley Orgánica para la protección de las personas menores de edad en los entonos digitales: del control parental defectivo a las obligaciones del fabricante", *Actualidad Civil, número 5, mayo*, pp. 1-12.

BARRIO ANDRÉS, M. (2024). "Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia artificial". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch.

BRITO IZQUIERDO, N. (2017). "Tratamiento de los datos personales de menores de edad en la nueva normativa europea protectora de datos personales", *Actualidad Civil, número 5, mayo, 2018*, pp.

— (2017). "Tratamiento de los datos personales de menores de edad: supuestos, límites, retos y desafíos", *LA LEY Derecho de Familia, Menores y Redes Sociales, número 14, abril-junio*, pp. 17-31.

CABALLERO, A. (2024). "Mercantilización de los datos de los menores por las plataformas de redes sociales", *LA LEY Derecho de familia, nº 44, octubre*, pp.10-17.

CAMPOS ACUÑA, C. (2024). "Las 15 claves del Reglamento Europeo de Inteligencia Artificial (AI Act) (1)", *El Consultor de los Ayuntamientos, de 15 de julio*, pp.

CASTÁN PÉREZ-GÓMEZ, J (2015). "La patria potestad". En: M. Garrido De Palma (coord.) *Instituciones de Derecho Privado,* T. IV Familia, vol. 2, 2ª ed., Cizur Menor (Navarra): Civitas Thomson Reuters.

CASTILLO PARRILLA, J.A. (2024). "Inteligencia artificial de uso general, modelos fundacionales (y "Chat GPT") en el Reglamento de Inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

CERNADA BADÍA, R. "Grandes plataformas y sistemas de inteligencia artificial destinados a la influencia política: la intersección entre la "Ley de Servicios Digitales" y el Reglamento de inteligencia artificial desde la perspectiva del riesgo". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

CHAVELI DONET, E. (2024). "La evaluación de impacto de derechos fundamentales por quienes despliegan sistemas de inteligencia artificial en el Reglamento". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

COTINO HUESO, L. (2024). "¿Qué es "inteligencia artificial" para el Reglamento?. Análisis, delimitación y aplicaciones prácticas". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

— (2024). "Alcance y delimitación de los sistemas de alto riesgo en el Reglamento de inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

DÍAZ ALABART, S. (1987). "La responsabilidad por los actos ilícitos dañosos de los sometidos a patria potestad y tutela", *Anuario de Derecho Civil, vol. XL, número 3,* pp. 795-894

DÍEZ GARCÍA, H. (2013). "Comentario al artículo 154 del Código Civil". En: R. Bervovitz-Rodríguez-Cano (coord.), *Comentarios al Código Civil,* T. I, Cizur Menor (Navarra): Thomson Reuters Aranzadi.

ESCAJEDO SAN-EPIFANIO, L. (2024). "El reconocimiento biométrico en el Reglamento de inteligencia artificial: exenciones, prohibiciones y especialidades de alto riesgo". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

FERNÁDEZ HERNÁNDEZ, C. (2024). "Comentario al artículo 6 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia, tirant lo blanch.

GARCÍA HERRERA, V. (2018). "El válido consentimiento para el tratamiento de los datos personales de los menores de edad en Internet. Especial referencia al

supuesto en que los representantes legales estén divorciados o separados (1)", *LA LEY Derecho de Familia, número 20, octubre-diciembre*, pp. 62-71.

GARCÍA MORALES, A. (2024). "Menores *influencers*, regulación legal actual en el ámbito laboral". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson.

GÓMEZ CALLE, E. (2016). "Comentario al artículo 1903 del Código Civil". En: A. Cañizares Laso, P. de Pablo Contreras, J. Orduña Moreno y R. Valpuesta Fernández (dirs.), *Código Civil comentado, vol. IV*, 2ª ed., Navarra: Civitas Thomson Reuters.

GONZÁLEZ MENESES GARCÍA-VALDECASAS, M. (2024). "Comentario al artículo 6 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch.

GÓRRIZ ROYO, E.M. (2016). "*On-line child grooming*" desde las perspectivas comparada y criminológica, como premisas de estudio del artículo 183 ter) 1º CP". En: Mª. L. Cuerda Arnau (dir.), *Menores y Redes sociales,* Valencia: tirant lo blanch.

GUADIX GARCÍA, N. (2024). "Los derechos de la infancia en la era digital", *LA LEY Derecho de Familia, número 44, octubre*, pp. 1-11.

GUTIÉRREZ MAYO, E. (2024), "La figura del Ministerio Fiscal en la defensa de los derechos digitales". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson.

JIMENEZ LÓPEZ, J. (2024). "El Reglamento de Inteligencia Artificial y el Reglamento general de protección de datos". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

MARTÍNEZ MARTÍNEZ, R. (2024). "El consentimiento en el tratamiento de los datos de carácter personal: un riesgo sistémico para los menores", LA LEY Derecho de Familia, número 44, octubre, pp. 1-16.

MARTÍNEZ MARTÍNEZ, R. y FERNÁNDEZ HERNÁNDEZ, C. (2024). "Publicidad digital y menores: una visión integrada de la Ley de Servicios Digitales y el Reglamento de Inteligencia Artificial (manipulaciones y conductas prohibidas, riesgos sistémicos en grandes modelos del lenguaje", *LA LEY Derecho de Familia, nº 44, octubre*, pp. 1-29.

MARTÍN CASALS, M. (2023). "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *Indret, núm. 3*, p.

MARTOS DÍAZ, N. (2019). "Principios (artículos 6-11 del RGPD. Artículos 4-10 de la LOPDGDD)". En: J. López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Barcelona: Bosch.

MESSÍA DE LA CERDA BALLESTEROS, J.A. (2017). "La protección del honor de los menores en las redes sociales", *LA LEY Derecho de Familia. Monográfico Menores y Redes Sociales, número 14, abril-junio*, pp. 32-42.

MUÑOZ GARCÍA, Mª.C. (2024). "Comentarios a los artículos 52 a 55 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch.

— (2024). "Taxonomía de los modelos de IA de uso general. Probabilidad de generar riesgos de alto impacto y las necesidades de identificarlos". En: J.A. Mo-

reno Martínez y P.J. Femenía López (coords.), *Inteligencia artificial y derecho de daños: cuestiones actuales*, Madrid. Dykinson

PALMA ORTIGOSA, A. (2024). "Régimen general de obligaciones de proveedores y responsables del despliegue en el Reglamento de inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

PARDO DE VERA, M.M. (2024). "La incidencia de la inteligencia artificial en los derechos de los menores. Regulación legal y problemática actual". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson.

PARRA LUCÁN, Mª Á. (2016). "Responsabilidad por hecho ajeno". En: C. Martínez de Aguirre Aldaz (coord.), *Curso de Derecho Civil, T. II, vol. II Contratos y responsabilidad civil,* Madrid: Edisofer.

PÉREZ ÁLVAREZ, M.Á. (2024). "La protección de los menores y las medidas de apoyo a las personas con discapacidad. La patria potestad". En: C. Martínez de Aguirre Aldaz (coord.), *Curso de Derecho Civil (IV) Derecho de Familia*, 7ª ed., Madrid: Edisofer.

PEÑA LÓPEZ, F. (2013). "Comentario al artículo 1903 del Código Civil". En: R. Bercovitz Rodríguez-Cano (dir.), *Comentarios al Código Civil, T. IX*, Valencia: tirant lo blanch.

POLVOROSA ROMERO, S. (2017). "El acoso escolar llevado a internet: los smartphone y los smarwatch", *LA LEY Derecho de Familia. Monográfico Menores y Redes Sociales, número 14, abril-junio*, pp. 85-94.

RAMÓN FERNÁDEZ, FCA. (2024). "Sistemas de gestión de calidad, documentación técnica y conservación en el Reglamento". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

RECIO GAYO, M. (2024). "Comentario al artículo 16 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch.

REYES MÉNDEZ D. (2019). "El acceso del menor a las redes sociales y el problema de su autentificación: la necesidad de una respuesta tecnológica", *Diario La Ley, número 9335, sección Tribunal, 11 enero,* p

RODRIGUEZ, A. (2024). "El derecho de imagen y a la intimidad de los NNA. Derechos de los menores e hijos de padres mediáticos o relevantes en el mundo digital". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson.

SIMÓN CASTELLANO, P. (2024). "El resto de los sistemas de inteligencia artificial prohibidos o inaceptables en el Reglamento de Inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

-(2024). "Los sistemas de gestión de riesgos como obligación específica para los sistemas de inteligencia artificial de alto riesgo en el artículo 9 del Reglamento". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi.

TINTORÉ GARRIGA Mª.P. (2017). "Sharenting y la responsabilidad parental", *LA LEY Derecho de Familia. Monográfico Menores y Redes Sociales, número 14, abril-junio*, p. 43-50.

VALDECANTOS, M. (2018). "El consentimiento como base legitimadora del tratamiento en el Reglamento Europeo de Protección de Datos", *Actualidad Civil, número 5, mayo*, p.

VIDAL HERRERO-VIOR, Mª. S. (2024). "Casuística y regulación legal de la responsabilidad penal de menores infractores en delitos relacionados con la tecnología". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson.

YZQUIERDO TOLSADA, M. (2015). *Responsabilidad civil extracontractual. Parte General. Delimitación y especies. Elementos. Efectos o consecuencias*, 3ª ed., Madrid: Dykinson.

ZABALGO, P. (2024). "El derecho de la infancia y la adolescencia al acceso a Internet y el derecho a la información contra el derecho a la infancia a la salud y a la seguridad. Interés superior del menor en el entorno digital". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, coordinadora, Madrid: Dykinson.

IX. ÍNDICE DE RESOLUCIONES

- STEDH, secc. 3ª, de 20 de junio de 2017.
- STC, de 4 de mayo de 1998.
- STC, de 30 de noviembre de 2000.
- STS, Sala de lo Civil, de 23 de julio de 1987.
- STS, Sala de lo Civil, de 17 de septiembre de 1996.
- STS, Sala de lo Civil, de 31 de diciembre de 1996.
- STS, Sala de lo Civil, de 8 de marzo de 2002.
- STS, Sala de lo Civil, de 9 de julio de 2002.
- STS, Sala de lo Civil, de 7 de noviembre de 2002.
- STS, Sala de lo Civil, de 5 de noviembre de 2003.
- STS, Sala de lo Civil, de 9 de julio de 2004.
- STS, Sala de lo Civil, de 10 de noviembre de 2006.
- STS, Sala de lo Civil, de 5 de junio de 2012.
- STS, Sala de lo Penal, de 24 de febrero de 2015.
- STS, Sala de lo Civil, de 30 de junio de 2015.
- STS, Sala de lo Civil, de 25 de noviembre de 2015.
- STS, Sala de lo Penal, de 10 de diciembre de 2015.
- STS, Sala de lo Contencioso-administrativo, de 2 de noviembre de 2016.
- STS, Sala de lo Contencioso-administrativo, de 20 de septiembre de 2018.
- STS, Sala de lo Penal, de 15 de enero de 2020.
- STS, Sala de lo Penal, de 15 de septiembre de 2020.
- STS, Sala de lo Penal, de 21 de enero de 2021.
- STS, Pleno de la Sala Segunda, de 2 de junio de 2022.
- STS, Sala de lo Penal, de 18 de mayo de 2023.
- STS, Sala de lo Penal, de 10 de julio de 2023.
- STS, Sala de lo Contencioso-administrativo, de 20 de diciembre de 2023.
- STS, Sala de lo Contencioso-administrativo, de 4 de marzo de 2024.
- STS, Sala de lo Contencioso-administrativo, de 6 de noviembre de 2024.

- STS, Sala de lo Penal, de 31 de octubre de 2024.
- ATS, Sala de lo Penal, de 30 de enero de 2025.
- STS, Sala de lo Penal, de 5 de febrero de 2025.
- SAN, Sala de lo Contencioso-administrativo, de 29 de noviembre de 2018.
- STSJ Navarra, Sala de lo Civil y Penal, de 4 de diciembre de 1995.
- ATSJ Cataluña, Sala de lo Civil y Penal, secc. 1ª, de 14 de junio de 2012.
- SAP Murcia, secc. 1ª, de 27 de febrero de 1996.
- SAP Valencia, secc. 6ª, de 22 de julio de 1996.
- SAP Sevilla, secc. 5ª, de 2 de octubre de 1998.
- SAP Vizcaya, secc. 1ª, de 8 de febrero de 1999.
- SAP Ávila, de 18 de junio de 1999.
- SAP Las Palmas, secc. 1ª, de 22 de junio de 1999.
- SAP Murcia, secc. 1ª, de 18 de enero de 2000.
- SAP Asturias, secc. 5ª, de 16 de marzo de 2004.
- SAP Barcelona, secc. 1ª, de 27 de enero de 2010.
- SAP Cádiz, secc. 5ª, de 2 de febrero de 2010.
- SAP Málaga, secc. 6ª, de 26 de enero de 2012.
- SAP Madrid, secc. 19ª, de 21 de febrero de 2013.
- SAP Alicante, secc. 6ª, de 14 de mayo de 2014.
- SAP Madrid, secc. 24ª, de 4 de junio de 2014.
- SAP Huelva, secc. 3ª, 8 junio 2014.
- SAP Granada, secc. 1ª, de 5 de junio de 2014.
- SAP Cáceres, secc. 1ª, de 3 de mayo de 2016.
- SAP Lugo, secc. 1ª, de 12 de mayo de 2016.
- SAP Guipúzcoa, secc. 2ª, de 27 de mayo de 2016.
- SAP Barcelona, secc. 1ª, de 1 de marzo de 2017.
- SAP Madrid, secc. 9ª, de 3 de mayo de 2017.
- SAP Madrid, secc. 12ª, de 6 de julio de 2017.
- SAP Valladolid, sección 3ª, de 31 de mayo de 2018.
- SAP Toledo, sección 1ª, de 5 de julio de 2018.
- SAP Santa Cruz de Tenerife, secc. 1ª, de 6 de julio de 2018.
- AAP La Rioja, secc. 1ª, de 5 de diciembre de 2018.
- SAP Vizcaya, secc. 5ª, de 25 de enero de 2019.
- SAP Valencia, secc. 7ª, de 27 de septiembre de 2019.
- SAP Vizcaya, secc. 3ª, de 20 de septiembre de 2024.
- SAP Cantabria, secc. 2ª, de 13 de enero de 2020.
- SAP Navarra, secc. 3ª, de 26 de febrero de 2020.
- SAP Murcia, secc. 1ª, de 27 de abril de 2020.
- SAP Cantabria, secc. 2ª, de 17 de mayo de 2021.
- SJPII, número 2, de Aoiz/Agoitz de 8 de febrero de 2021.

NOTAS

[1] En esta línea, ZABALGO, P. (2024). "El derecho de la infancia y la adolescencia al acceso a Internet y el derecho a la información contra el derecho a la infancia a la salud y a la seguridad. Interé s superior del menor en el entorno digital". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, coordinadora, Madrid: Dykinson, p. 69.

[2] RODRIGUEZ, A. (2024). "El derecho de imagen y a la intimidad de los NNA. Derechos de los menores e hijos de padres mediáticos o relevantes en el mundo digital". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson, p. 77.

[3] Vid., sobre el concepto de *influencer* o usuario de especial relevancia, vid., GARCÍA MORALES, A. (2024). "Menores *influencers*, regulación legal actual en el ámbito laboral". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson, pp. 97-103.

[4] Vid., la sentencia de la Audiencia Provincial de Barcelona, secc. 1ª, de 27 de enero de 2010 (JUR 2010,82805) responsabilidad del centro docente por acoso escolar a menor. No consta la adopción de ninguna medida de prevención, ni que se ideara un plan de actuación y seguimiento que permitiera conocer y valorar la situación de hostigamiento que estaba sufriendo el hijo de los actos y de la que tenía constancia tras una agresión sufrida por el mismo en el patio por la que fueron sancionados los responsables; la sentencia de la Audiencia Provincial de Guipúzcoa, secc. 2ª, de 27 de mayo de 2016 (AC 2016,1329) responsabilidad de los padres y del centro docentes por lesiones causadas por menor a la profesora. Inserción en red social de comentarios vejatorios terriblemente graves contra la citada docente. Asimismo, la sentencia de la Audiencia Provincial de Barcelona, secc. 1ª, de 1 de marzo de 2017 (AC 2017,607) responsabilidad del centro docente por un supuesto de acoso escolar. No se adoptaran por parte del Centro todas las medidas a su alcance para poner fin a la situación, no constado la vigilancia, atención o cautela no sólo con relación al menor, sino que incluyera a los compañeros que protagonizaron los conflictos con aquél, a fin de frenar la existencia de los mismos; la sentencia de la Audiencia Provincial de Vizcaya, secc. 5ª, de 25 de enero de 2019 (JUR 2019,98124) responsabilidad del colegio por los daños derivados de una situación de acoso escolar que culminó con la grabación de la alumna acosada mientras se duchaba en los vestuarios del colegio y la posterior difusión de las imágenes en internet; y la sentencia de la Audiencia Provincial de Valencia, secc. 7ª, de 27 de septiembre de 2019 (AC 2019,1819) existencia de una fotografía de la menor desnuda mientras se hallaba en los vestuarios duchándose tras un partido de futbol, tomada por otra menor y difundida por vía de WhatsApp. Responsabilidad del club deportivo que no extremo las medidas para que el móvil no se utilizara en los vestuarios y de los padres de las menor infractora.

[5] Unos datos preocupantes: 7 de cada 10 adolescentes consuman pornografía de forma regular en España; y, el primer acceso resulta entre los 9 y los 11 años. Asimismo, según los datos del Ministerio del Interior y del Ministerio de Juventud e Infancia, el acceso a estos contenidos se realiza fundamentalmente a través del teléfono móvil, bien por mensajería instantánea, páginas web o redes sociales.

[6] En la sentencia de la Audiencia Provincial de Vizcaya, secc. 3ª, de 20 de septiembre de 2024 (LA LEY 328230,2024) se condena a un menor por difundir por Instagram fotos íntimas de otro menor. La Sala estima acreditado que fue el menor demandado quien, desde la dirección de IP correspondiente al router del domicilio en el que residía con sus abuelos, creó los perfiles de Instagram desde los que se enviaron las fotografías y los mensajes n los que se amenazó a la víctima con difundir fotografías íntimas si no se enviaban más imágenes de él y de terceros. dichos hechos se realizaron de manera continuada y a los lato del tiempo. De las declaraciones d loa agentes que instruyeron las diligencias penales resulta que l único morador de la vivienda que hacía un uso continuado del wifi y que tenía conocimientos suficientes para crear los perfiles era el demandado.

[7] El RGPD se complementa con el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que

se,modifica el Reglamento (UE) 2918/1724 (Reglamento de Gobernanza de Datos), también conocido como Data Governance Act (DGA), es un marco legal que busca facilitar la reutilización de datos en la UE, aumentar la confianza en los servicios de intermediación de datos y promover el uso de datos en la economía y la sociedad. Tienen como objetivos: 1. Facilitar la compartición y reutilización de datos, especialmente aquellos del sector público, bajo ciertas condiciones; 2. Aumenta la confianza n los servicios de intermediación de datos que, ayudan a conectar a quienes necesitan datos con quien los poseen; 3. Promueve el uso de datos para la innovación y el desarrollo económico, impulsando la economía digital europea; 4. Garantiza que los datos se utilicen de manera responsable, respetando los derechos de las personas y cumpliendo con la normativa de protección de datos. Y, asimismo, con Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) también conocida como "Ley de Datos" o la "Data Act". Se trata de una norma clave en la Estrategia europea de Datos y que, se espera, contribuya significativamente al objetivo de la Década Digital de la Unión Europea (UE), complementando las medidas ya dispuestas de forma previa por la Ley de Gobernanza de datos. Esta nueva norma resulta aplicable tanto a datos no personales como personales y, por consiguiente, interactúa con el RGPD, siendo plenamente aplicable y prevaleciendo en tanto ley especial, el RGPD frente a la Data Act cuando se traten datos de carácter personal. Esta Ley de Datos o Data Act pretende potenciar una distribución justa del valor de los datos mediante el establecimiento de normas claras y justas para acceder a los datos ante la eclosión, sobre todo, del Internet de las Cosas (IoT), los dispositivos conectados y los servicios relacionados en estos casos. Y es que, con este Reglamento, los productos y servicios conectados tendrán que diseñarse y fabricarse de manera que los usuarios (empresas y consumidores) puedan acceder, utilizar y compartir los datos generados (datos de los productos y de los servicios relacionados, incluidos los metadatos pertinentes necesarios para interpretar y utilizar dichos datos) en múltiples sectores de forma fácil y segura, utilizando, por tanto, nuevas bases legales al efecto que lo posibilitan e imponen.

[8] El 2 de febrero empezaron a ser aplicables las disposiciones del Reglamento (UE) 2024/1689, de 13 de junio de 2024 (Reglamento de IA) incluidas en los Capítulos I (Disposiciones Generales) y II (Prácticas de IA Prohibidas) del mismo. Así, además de la obligación de alfabetización en materia de IA (artículo 4 del RIA) —que afecta a todos los proveedores y responsables del despliegue de sistemas de IA, independientemente de su nivel de riesgo— también resultan ya aplicables las disposiciones del Capítulo II del RIA, cuyo artículo 5 prohíbe ciertas prácticas en materia de IA.

Con la finalidad de esclarecer la interpretación y alcance de las anteriores disposiciones, así como del ámbito de aplicación del RIA, la Comisión Europea ha publicado recientemente los siguientes documentos: 1. Un repositorio vivo sobre prácticas de alfabetización en materia de IA el 16 de abril de 2025: entre las principales prácticas compartidas destacan: A. Realizar sesiones de formación organizadas según la complejidad técnica y el nivel de implicación de los empleados en el uso o desarrollo de sistemas de IA; B. Ofrecer cursos de e-learning; C. Compartir ejemplos de uso real en operaciones diarias; o D. Implementar guías detalladas para el desarrollo, uso y supervisión de sistemas de IA; 2. Unas directrices sobre la definición de los sistemas de IA el 6 de febrero de 2025: que aclaran qué constituye un sistema de IA y por tanto, a qué sistemas resultaría de aplicación el Reglamento de IA; y, 3. Unas directrices sobre prácticas prohibidas aprobadas el 4 de febrero de 2025: En relación con las prácticas prohibidas, la Comisión proporciona en sus Directrices una guía interpretativa detallada sobre los elementos a considerar para determinar si un sistema de IA se encuadra en las prohibiciones establecidas por el artículo 5 del Reglamento de IA. Así, por ejemplo: A. La práctica prohibida del art. 5.1.a): abarca aquellos sistemas que usen técnicas subliminales, manipulativas o engañosas (por ejemplo, el uso de imágenes subliminales, el aprovechamiento de sesgos, la manipulación sensorial para alterar el humor o la creación de mensajes persuasivos altamente personalizados en base a datos personales), que tengan como objetivo

distorsionar, o que puedan resultar en la distorsión del comportamiento de una persona o grupo. Y dicho comportamiento distorsionado debe causar, o ser probable que cause, un daño significativo (incluidos daños físicos, psicológicos o económicos) a esa persona, otra persona o un grupo de personas. Asimismo, la Comisión establece los criterios para valorar el carácter significativo del daño, como el contexto, la intensidad, la irreversibilidad del daño o la vulnerabilidad de las personas afectadas.; y B. En relación con la práctica prohibida del art. 5.1.f), esta se refiere a sistemas de IA utilizados para la inferencia emociones de un individuo en el lugar de trabajo o en instituciones educativas, excepto cuando su uso esté justificado por razones médicas o de seguridad. Según la Comisión el término "lugar de trabajo" debe interpretarse de forma amplia, incluyendo cualquier espacio físico o virtual específico en el que las personas realicen funciones asignadas por su empleador o por la organización a la que estén afiliadas, por ejemplo, en caso de trabajo por cuenta propia. En relación con la "inferencia de emociones", las Directrices también abogan por una interpretación amplia. No obstante, no abarca la inferencia de estados físicos como el cansancio o el dolor, ni aquellos sistemas que se limiten a detectar expresiones o gestos (como una sonrisa o el movimiento ocular) pero que no identifiquen emociones o intenciones.

Ahora bien, el 9 de julio de 2024 entró en vigor el Reglamento EuroHPC JU modificado, que permite la creación de Fábricas IA. El día 10 de diciembre de 2024 se seleccionaron siete consorcios para establecer Fábricas IA, seguidos de seis consorcios adicionales el 12 de marzo de 2025. También se ha aprobado un Plan de Acción del Continente IA por parte de la Comisión Europea el 9 de abril de 2025 con el fin de impulsar la capacidad de innovación en IA en la Unión Europea.

[9] RTC 94,1998.

[10] RTC 292,2000.

[11] El considerando número 48 del RIA establece, a tal efecto que: "La magnitud de las consecuencias adversas de un sistema de IA para los derechos fundamentales protegidos por la Carta es especialmente importante a la hora de clasificar un sistema de IA como de alto riesgo. Entre dichos derechos se incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, el derecho a la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, la igualdad entre hombres y mujeres, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración. Además de esos derechos, conviene poner de relieve el hecho de que los menores poseen unos derechos específicos consagrados en el artículo 24 de la Carta y en la Convención sobre los Derechos del Niño de las Naciones Unidas, que se desarrollan con más detalle en la observación general número 25 de la Convención sobre los Derechos del Niño de Naciones Unidas relativa a los derechos de los niños en relación con el entorno digital. Ambos instrumentos exigen que se tengan en consideración las vulnerabilidades de los menores y que se les brinde la protección y la asistencia necesarias para su bienestar. Cuando se evalúe la gravedad del perjuicio que puede ocasionar un sistema de IA, también en lo que respecta a la salud y la seguridad de las personas, también se debe tener en cuenta el derecho fundamental a un nivel elevado de protección del medio ambiente consagrado en la Carta y aplicado en las políticas de la Unión". Y, el considerando número 76 del RIA dispone que: "el derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. Las medidas adoptadas por los proveedores para garantizar el cumplimiento de estos principios podrán incluir no solo la anonimización y el cifrado, sino también el uso de una tecnología que permita llevar los algoritmos a los datos y el entrenamiento de los sistemas de IA sin que sea necesaria la

transmisión entre las partes ni la copia de los datos brutos o estructurados, sin perjuicio de los requisitos en materia de gobernanza de datos establecidos en este Reglamento".

[12] CABALLERO, A. (2024). "Mercantilización de los datos de los menores por las plataformas de redes sociales", *LA LEY Derecho de familia, nº 44, octubre*, p. 4 indica que "hay dos etapas claves en el neurodesarrollo. La primera que se produce en la fase de 0 a 2 años, momento de máxima plasticidad neuronal; la segunda tiene lugar gran parte del proceso de sinapsis (interconexión neuronal en base a experiencias vividas con el objetivo de adaptarse de forma óptima al entorno); y, la tercera supone la mielización (en la que se potencian las redes neuronales las utilizadas en función de la información que reciban las neuronas)".

[13] Asimismo, el artículo 15 se refiere a las obligaciones de transparencia informativa de los prestadores de servicios intermediarios. Así, los prestadores de servicios intermediarios publicarán en un formato legible por máquina y de forma fácilmente accesible, al menos una vez al año, informes claros y fácilmente comprensibles sobre cualquier actividad de moderación de contenidos que hayan realizado durante el período pertinente; igualmente notificaran la sospecha de delito cuando un prestador de servicios de alojamiento de datos tenga conocimiento de cualquier información que le haga sospechar que se ha cometido, se está cometiendo o es probable que se cometa un delito que implique una amenaza para la vida o la seguridad de una o más personas, comunicará su sospecha de inmediato a las autoridades policiales o judiciales del Estado miembro o Estados miembros afectados y aportará toda la información pertinente de que disponga (artículo 18). También, los prestadores de plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño detectarán, analizarán y evaluarán con diligencia cualquier riesgo sistémico en la Unión que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios. También los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño aplicarán medidas de reducción de riesgos razonables, proporcionadas, efectivas, y adaptadas a los riesgos sistémicos específicos detectados, teniendo especialmente en cuenta las consecuencias de dichas medidas sobre los derechos fundamentales (artículo 34). En cuanto a los sistemas de recomendación los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño que utilicen sistemas de recomendación ofrecerán al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles (artículo 38); respecto a la transparencia adicional sobre la publicidad en línea, los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda en línea de muy gran tamaño que presenten anuncios publicitarios en sus interfaces en línea recopilarán y harán público, en una sección específica de su interfaz en línea, a través de una herramienta de búsqueda fiable que permita realizar consultas en función de múltiples criterios, y mediante interfaces de programación de aplicaciones, un repositorio, durante todo el tiempo en el que presenten un anuncio y hasta un año después de la última vez que se presente el anuncio en sus interfaces en línea (artículo 39), Y, en fin, la Comisión y la Junta fomentarán y facilitarán la elaboración de códigos de conducta voluntarios en el ámbito de la Unión para contribuir a la debida aplicación del presente Reglamento, teniendo en cuenta en particular las dificultades concretas que conlleva actuar contra diferentes tipos de contenidos ilícitos y riesgos sistémicos, de conformidad con el Derecho de la Unión en particular en materia de competencia y de protección de los datos personales (artículo 45).

[14] El considerando número 46 dispone, asimismo, que: "Los prestadores de servicios intermediarios que estén dirigidos principalmente a menores, habida cuenta, por ejemplo, del diseño o la comercialización del servicio, o que sean utilizados predominantemente por menores, deben realizar un esfuerzo especial para que la explicación de sus condiciones generales pueda ser comprendida con facilidad por los menores".

Para un análisis más detallado de la publicidad digital y menores, vid., MARTÍNEZ MARTÍNEZ, R. y FERNÁNDEZ HERNÁNDEZ, C. (2024). "Publicidad digital y menores: una visión integrada de la Ley de Servicios Digitales y el Reglamento de Inteligencia Artificial

(manipulaciones y conductas prohibidas, riesgos sistémicos en grandes modelos del lenguaje", *LA LEY Derecho de Familia, nº 44, octubre*, pp. 1-29.

[15] Vid., la Propuesta de Guía sobre Generación de datos sintéticos, publicada por la Comisión de Protección de Datos Personales de Singapur (PCPC Singapore) el 15 de julio de 2024, pp. 1-38.

[16] Esta propuesta de Directiva parte de la responsabilidad civil subjetiva o por culpa; si bien, facilta la carga de la prueba de manera muy específica y proporcionada mediante el uso de la exhibición y las presunciones refutables (*iuris tantum*). Asimismo, para aquellas solicitudes de indemnización de daños y perjuicios establece la posibilidad de obtener información sobre los sistemas de IA de alto riesgos que deben registrarse o documentarse de conformidad con el RIA.

[17] Se imponía na necesaria revisión de la Directiva 85/374/CEE, por un lado, ante los avances relacionados con las nuevas tecnologías, incluida la IA; y, por otro, los nuevos modelos de negocio de economía circular y las nuevas cadenas de suministros mundiales, además de la propia carencia del concepto "producto".

En todo caso, para garantizar que el régimen de responsabilidad por productos defectuosos de la Unión sea exhaustivo "la responsabilidad será objetiva por daños causados por productos defectuosos y deberá aplicarse a todos los bienes muebles, incluidos los programas informáticos, incluso cuando estén integrados en otros bienes muebles o instalados en bienes inmuebles" (considerando número 6).

Si bien, con el fin de lograr un reparto equitativo del riesgo, una persona que reclame una indemnización por los daños causados por un producto defectuoso debe soportar la carga de la prueba del daño, el carácter defectuoso de un producto y el nexo de causalidad entre ambos, de conformidad con el nivel de prueba aplicable con arreglo al Derecho nacional No obstante, para evitar la asimetría informativa "resulta necesario facilitar el acceso de los demandantes a las pruebas que vayan a utilizarse en los procedimientos judiciales. Tales pruebas incluyen los documentos que el demandado deba crear *ex novo* mediante la compilación o clasificación de las pruebas disponibles. Al examinar la solicitud de exhibición de pruebas, los órganos jurisdiccionales nacionales deben garantizar que ese acceso se limite a lo necesario y proporcionado, entre otras cosas, para evitar búsquedas indiscriminadas de información que no sea pertinente para el procedimiento y para proteger la información confidencial, como la información que entra en el ámbito de aplicación del secreto profesional y los secretos comerciales de conformidad con el Derecho de la Unión y nacional, en particular la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo". Además, "teniendo en cuenta la complejidad de determinados tipos de pruebas, por ejemplo, las pruebas relativas a productos digitales, los órganos jurisdiccionales nacionales deben poder exigir que dichas pruebas se presenten de manera fácilmente accesible y comprensible, siempre que se cumplan determinadas condiciones" (considerando número 42).

[18] El artículo 3 letra g) señala como "servicio intermediario": uno de los siguientes servicios de la sociedad de la información: i) un servicio de "mera transmisión", consistente en transmitir, en una red de comunicaciones, información facilitada por el destinatario del servicio o en facilitar acceso a una red de comunicaciones; ii) un servicio de "memoria caché", consistente en transmitir por una red de comunicaciones información facilitada por el destinatario del servicio, que conlleve el almacenamiento automático, provisional y temporal de esta información, prestado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de estos; iii) un servicio de "alojamiento de datos!, consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este. En cuando al contenido ilícito el citado artículo 3 letra h) lo define como" toda información que, por sí sola o en relación con una actividad, incluida la venta de productos o la prestación de servicios, incumpla el Derecho de la Unión o el Derecho de cualquier Estado miembro que cumpla el Derecho de la Unión, sea cual sea el objeto o carácter concreto de ese Derecho".

[19] Artículo 3 letra i) "plataforma en línea" es: "un servicio de alojamiento de datos que, a petición de un destinatario del servicio, almacena y difunde información al público, salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento".

[20] Instagram (Meta) ha hecho desde 2023-2024 cambios en el diseño para menores. En concreto: 1. Cuentas privadas por defecto para menores; 2. Limitación de mensajes directos entre adultos y menores que nos e siguen mutuamente; 3. Reducción del contenido "·potencialmente dañino" en la *feed de Explore* para adolescentes; y 4. Meta ha publicado informes sobre el impacto de sus algoritmos en menores, incluyendo temas relativos a la autoestima o la salud mental.

[21] La Comisión Europea en abril de 2024 inicio una investigación formal contra Tik Tok ante posibles infracciones de la DSA relacionadas, precisamente, con menores. Se comprobó: 1. Una insuficiente verificación de la edad: Tik Tok no garantizaba que los usuarios menores de 13 años no accedieran a la plataforma; 2. Publicidad personalizada: había sospechas que Tik Tok continuaba mostrando anuncios personalizados a menores. Algo que, como bien sabemos, esté prohibido en el Reglamento; y 3. Diseño adictivo: se investigó si el diseño de Tik Tok (*scroll* infinito, recompensar visuales) perjudicaban la salud metal de los menores y adolescentes.

[22] El artículo 3 letra j): "motor de búsqueda en línea" es: "un servicio intermediario que permite a los usuarios introducir consultas para hacer búsquedas de, en principio, todos los sitios web, o de sitios web en un idioma concreto, mediante una consulta sobre un tema cualquiera en forma de palabra clave, consulta de voz, frase u otro tipo de entrada, y que en respuesta muestra resultados en cualquier formato en los que puede encontrarse información relacionada con el contenido que es objeto de la consulta".

[23] En cuanto las grandes plataformas, los sistemas de inteligencia artificial destinado a la influencia política, el DSA y el Reglamento Europeo sobre Transparencia y Segmentación de Publicidad Política (RTSPP), vid, CERNADA BADÍA, R. "Grandes plataformas y sistemas de inteligencia artificial destinados a la influencia política: la intersección entre la "Ley de Servicios Digitales" y el Reglamento de inteligencia artificial desde la perspectiva del riesgo". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, p. 393 señala al respecto que "el tratamiento que realiza el RIA respecto a VLOPs y sistemas destinado a la influencia política resulta adecuado en términos sistemáticos y responde de forma más precisa a la lógica de la normativa aplicable, centrada en el proveedor/responsable del despliegue en el caso del RIA y en el usuario final respecto a la DSA y el RTSPP— estas distintas perspectivas resultan complementarias en la valoración global de los riesgos subyacentes al uso de sistemas de IA en plataformas digitales".

[24] El artículo 3 letra u) define "condiciones generales" como: "todas las cláusulas, sea cual sea su nombre y forma, que rijan la relación contractual entre el prestador de servicios intermediarios y los destinatarios del servicio".

[25] MARTÍNEZ MARTÍNEZ, R. y FERNÁNDEZ HERNÁDNDEZ, C. (2024). "Publicidad digital y menores: una visión integrada de la Ley de Servicios Digitales y el Reglamento de Inteligencia Artificial (manipulaciones y conductas prohibidas, riesgos sistémicos en grandes modelos del lenguaje", *op. cit.*, pp. 4-5 siguiendo a Michael Lavi describen distintos procedimientos de manipulación publicitaria que sustenta la exigibilidad de responsabilidad civil a las plataformas que causan daños a los menores. Las sitúan en el contexto de llamado capitalismo de vigencia y el uso de algoritmos para dirigir contenido a usuarios, incluyendo niños: "1. Personalización a través de algoritmos; (…) 2. Explotación de vulnerabilidades emocionales; (…) 3. "Framig" (encuadre); (…) 4. Sistemas de recomendación; (…) 5. Manipulación del proceso de pensamiento intuitivo; (…) 6. Creación de contexto de vulnerabilidad; (…) 7.

Uso de datos biométricos; (…) 8. Explotación de sesgos cognitivos; (…) y, 9. Influencia en las decisiones".

[26] El artículo 96 relativo a los Códigos de conducta para tratamiento adecuado de menores en noticiarios y programas de contenido informativo de actualidad dispone que. "La autoridad audiovisual competente promoverá entre los prestadores del servicio de comunicación audiovisual televisivo, lineal y a petición, la adopción de códigos de conducta con el fin de dar un tratamiento adecuado a los menores en noticiarios y programas de contenido informativo de actualidad en los que: a) Se informe de que un menor de edad se ha visto involucrado, de cualquier modo, en una situación de riesgo o violencia, incluso si no llega a ser un hecho constitutivo de delito; b) Aparezcan menores en situaciones de vulnerabilidad".

[27] El artículo 98 bajo la rúbrica de calificación de los programas audiovisuales establece que: "1. Los prestadores del servicio de comunicación audiovisual televisivo, lineal o a petición, están obligados a que los programas emitidos dispongan de una calificación por edades, visible en pantalla mediante indicativo visual y fácilmente comprensible para todas las personas. 2. La Comisión Nacional de los Mercados y la Competencia firmará un acuerdo de corregulación, de acuerdo con lo previsto en el artículo 15.2, entre otros, con los prestadores del servicio de comunicación audiovisual televisivo, lineal y a petición y con los prestadores del servicio de intercambio de vídeos a través de plataforma, garantizando la participación de las asociaciones de consumidores y usuarios y de las organizaciones representativas de los usuarios de los medios, con el fin de coadyuvar al cumplimiento de las obligaciones establecidas en este artículo; 3. Cuando el acuerdo de corregulación previsto en el apartado anterior pueda afectar a la calificación de los programas y a la recomendación de visionado en función de la edad, la Comisión Nacional de los Mercados y la Competencia solicitará a la autoridad audiovisual competente, al Instituto de la Cinematografía y de las Artes Audiovisuales y a los órganos correspondientes de la Comunidades Autónomas con competencia en la materia, la emisión de un informe preceptivo sobre el mismo; 4. Los prestadores del servicio de comunicación audiovisual televisivo, lineal y a petición, cumplimentarán los campos de los descriptores de forma que las Guías Electrónicas de Programas, previstas en la normativa de telecomunicaciones, y/o los equipos receptores muestren la información relativa al contenido de los programas; 5. Los prestadores del servicio de agregación de servicios de comunicación audiovisual respetarán y mantendrán la información y los descriptores presentes en las Guías electrónicas de programas, previstas en la normativa de telecomunicaciones, de los servicios que comercializan; 6. Los apartados anteriores no serán de aplicación a los servicios de comunicación audiovisual ofertados de forma exclusiva en otro Estado miembro de la Unión Europea siempre que el prestador haya demostrado a la autoridad audiovisual competente que la protección de los menores frente a contenidos dañinos o perjudiciales se ajusta al nivel de protección establecido en el presente artículo; 7. Las autoridades audiovisuales competentes de ámbito autonómico podrán formalizar acuerdos de corregulación con los prestadores del servicio de comunicación audiovisual autonómico, con objeto de coadyuvar al cumplimiento de las obligaciones establecidas en este artículo".

[28] El artículo 99 añade que: "2. el servicio de comunicación audiovisual televisivo lineal en abierto tiene las siguientes obligaciones para la protección de los menores del contenido perjudicial: a) Se prohíbe la emisión de programas o contenidos audiovisuales que contengan escenas de violencia gratuita o pornografía. b) La emisión de otro tipo de programas o contenidos audiovisuales que puedan resultar perjudiciales para los menores exigirá que el prestador forme parte del código de corregulación que se prevé en el artículo 98.2 y disponga de mecanismos de control parental o sistemas de codificación digital. c) Los programas cuya calificación por edad "No recomendada para menores de dieciocho años" solo podrán emitirse entre las 22:00 y las 6:00 horas. 3. El servicio de comunicación audiovisual televisivo lineal de acceso condicional tiene las siguientes obligaciones para la protección de los menores del contenido perjudicial: a) Formar parte del código de corregulación previsto en el artículo 98.2. b) Proporcionar mecanismos de control parental o sistemas de codificación digital. 4. El servicio de comunicación audiovisual televisivo a petición tiene las siguientes obliga-

ciones para la protección de los menores del contenido perjudicial: a) Incluir programas y contenidos audiovisuales que puedan incluir escenas de pornografía o violencia gratuita en catálogos separados. b) Formar parte del código de corregulación previsto en el artículo 98.2. c) Proporcionar mecanismos de control parental o sistemas de codificación digital. 5. Los prestadores del servicio de comunicación audiovisual televisivo lineal en abierto y de acceso condicional solo podrán emitir programas relacionados con el esoterismo y las paraciencias, basados en la participación activa de los usuarios, entre la 1:00 y las 5:00 horas, y tendrán responsabilidad subsidiaria sobre los delitos que puedan cometerse y los daños que puedan causarse a través de dichos programas. 6. Los prestadores del servicio de comunicación audiovisual televisivo lineal en abierto y de acceso condicional solo podrán emitir programas de actividades de juegos de azar y apuestas entre la 1:00 y las 5:00 horas, salvo los sorteos de modalidades o productos de lotería cuya comercialización está reservada en exclusiva a los operadores designados al efecto por la Ley 13/2011, de 27 de mayo, de Regulación del Juego, o por la correspondiente legislación autonómica, que podrán ser emitidos sin sujeción a la mencionada limitación horaria.

Quedan igualmente excluidos de la limitación sobre franjas horarias establecida en el párrafo anterior los juegos de concursos emitidos por esos mismos prestadores, según la definición de esos juegos dada por la Ley 13/2011, de 27 de mayo, o por la legislación autonómica correspondiente, siempre que esos juegos estén conexos o subordinados a la actividad ordinaria de esos prestadores y, además, no se utilice su difusión para promocionar, de forma directa o indirecta, ninguna otra actividad de juegos de azar o de apuestas.

En fin, el artículo 100 referido al contenido audiovisual especialmente recomendado para menores dispone que: "La autoridad audiovisual competente pondrá en marcha actuaciones dirigidas a fomentar la producción y emisión de programas especialmente recomendados para menores de edad, adaptados a su edad, madurez y lenguaje que promuevan su desarrollo y bienestar integral".

[29] JIMENEZ LÓPEZ, J. (2024). "El Reglamento de Inteligencia Artificial y el Reglamento general de protección de datos". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, pp. 159-160.

[30] ARGELICH COMELLES, C. (2025). "La proyectada Ley Orgánica para la protección de las personas menores de edad en los entonos digitales: del control parental defectivo a las obligaciones del fabricante", *Actualidad Civil, nº 5, mayo*, p. 9.

[31] Vid., las sentencias del Tribunal Supremo, Sala de lo Contencioso-administrativo, de 20 de septiembre de 2018 (Roj. STS 3221/2018; ECLI:ES:TS:2018:3221); y, de 27 de noviembre de 2023 (Roj. STS 5133/2023; ECLI:ES:TS:2023:5133).

[32] Vid., el Auto del Tribunal Supremo, Sala de lo Contencioso-administrativo, de 7 de febrero de 2018 (Roj. ATS 732/2018; ECLI:ES:TS:2018:732A); y, las sentencias del Tribunal Supremo, Sala de lo Contencioso-administrativo, de 11 de enero de 2019 (Roj. STS 19/2019; ECLI:ES:TS:2019:19); de 22 de junio de 2020 (Roj. STS 2031/2020; ECLI:ES:TS:2020:2031); de 17 de septiembre de 2020 (Roj. STS 4159/2020; ECLI:S:TS:2020:4159); de 27 de noviembre de 2020 (Roj. STS 4016/2020; ECLI:ES:TS:2020:4016); de 21 de diciembre de 2023 (Roj. ST 5992/2023; ECLI:ES:ST:2023:5992); y, de 4 de marzo de 2024 (Roj. STS 1401/2024; ECLI:ES:TS:2024:1401).

[33] Vid., la sentencia del Tribunal Supremo, Sala de lo Contencioso-administrativo, de 19 de julio de 2022 (Roj. STS 3207/2022; ECLI:ES:TS:2022:3207).

[34] Vid., el Dictamen 15/2011 sobre la definición del consentimiento del Grupo de Trabajo del Artículo 29 adoptado el 13 de julio de 2011 (WP 187), p. 12.

Asimismo, vid., las sentencias del Tribunal Supremo, Sala de lo Contencioso-administrativo, secc. 5ª, de 2 de noviembre de 2016 (RJ 2016,5718); y, de 20 de diciembre de 2023 (Roj. STS 5778/2023; ECLI:ES:TS:2023:5778); y la sentencia de la Audiencia Nacional, Sala de lo Contencioso-administrativo, secc. 1ª, de 29 de noviembre de 2018 (JUR 2019,27374).

[35] En el Dictamen 15/2011 sobre la definición del consentimiento, pp. 9-10 y 27 señala al respecto que, el concepto de consentimiento está vinculado a la idea de que el interesado debe controlar el uso que se hace de sus datos. Asimismo, el consentimiento está relacionado con el concepto de autodeterminación y la transparencia es una condición para la posesión del control y de validez del consentimiento. Para ser válido el consentimiento debe estar informado y, la obtención del consentimiento antes del comienzo del tratamiento de los datos constituye una condición fundamental para legitimar el tratamiento de datos. Es fundamental utilizar el consentimiento "en el contexto adecuado". Para ser válido, el consentimiento debe ser específico. Y un consentimiento informado por parte del interesado supone un consentimiento basado en la apreciación y comprensión de los hechos y consecuencias de una acción.

En cuanto a los parámetros de privacidad por defecto de una red social a los que los usuarios no acceden necesariamente al utilizarla, permiten a la totalidad de la categoría "amigos de amigos" hacer que, toda la información personal de cada usuario puede ser vista por todos los "amigos de amigos" señala el Dictamen que, los usuarios que no desean que su información sea vista por los "amigos de amigos" tienen que pulsar un botón. El responsable del tratamiento considera que, si se abstiene de actuar o no pulsan el botón han consentido en que se puedan ver sus datos. Sin embargo, es muy cuestionable que no pulsar el botón signifique que por lo general las personas *consienten* en que su información pueda ser vista por todos los amigos de amigos. Debido a la incertidumbre en cuanto a si la inacción significa consentimiento, el hecho de no pulsar no puede considerarse consentimiento inequívoco. Este ejemplo como aclara el citado Dictamen ilustra el cado de la persona que permanece pasiva (por ejemplo, inacción o "silencio"). Por lo que, el consentimiento inequívoco no encaja bien con los procedimientos para obtener el consentimiento a partir de la inacción o el silencio de las personas: el silencio o la inacción de una parte es intrínsecamente equívoco (la intención del interesado podría ser de asentimiento o simplemente no realizar la acción).

[36] En esta línea, VALDECANTOS, M. (2018). "El consentimiento como base legitimadora del tratamiento en el Reglamento Europeo de Protección de Datos", *Actualidad Civil, número 5, mayo*, p. 8.

[37] Se aplica a todos los menores que, se encuentren en la Unión Europea —el artículo 3 apartado 2 del Reglamento antes de la corrección de errores se refería a los interesados que residían en la Unión, ahora que tras la misma, la redacción definitiva basta que se encuentren en la Unión Europea—. Los menores son interesados (personas físicas) cuyo tratamiento de datos realizado por los responsables o encargados del tratamiento va a ser objeto de protección.

[38] El Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas) del Grupo de Trabajo del Artículo 29, emitido el 11 de febrero de 2009 (WP 160), pp. 2-6 y 11-12 debe considerarse en el contexto de la iniciativa general de la Comisión Europea que se describe en la Comunicación "Hacia una estrategia de la Unión Europea sobre los Derechos de la Infancia", pretende reforzar el derecho fundamental de los niños a la protección de datos personales. El objeto de este Dictamen es analizar los principios generales que se aplican a la protección de los datos de los niños, así como explicar su pertinencia en un sector crítico específico como el de los datos escolares. Se indica que, un niño es una persona mayor de 18 años, salvo si ha adquirido la mayoría de edad legal antes de esa edad. Desde un punto de vista estático, el niño es una persona que todavía no ha alcanzado la madurez física y psicológica. Desde el punto de vista dinámica, se encuentra en un proceso de desarrollo físico y mental que le convertirá en adulto. Los derechos del niño y su ejercicio —incluso el derecho de protección de datos— deben expresarse teniendo presente ambas perspectivas. Por otra parte, el principio de interés superior del menor presenta dos aspectos: en primer lugar, el principio que exige que la intimidad de los niños se proteja de la mejor manera posible mediante la aplicación, en la medida de lo posible, de los derechos de protección del niño y su derecho a la intimidad entren en conflicto. En estos casos, los derechos de protección de datos podrán dejar paso al principio del

interés superior. Al ser el niño una persona todavía en desarrollo, el ejercicio de sus derechos, incluidos los relativos a la protección de datos, debe adaptarse al nivel de su desarrollo físico y psicológico. Los niños no solo están en proceso de desarrollo, sino que tienen derecho a este desarrollo. La regulación jurídica de este proceso varía según los Estados, pero todas las sociedades deben tratar a los niños según el grado de madurez. Cuando el tratamiento de los datos de un niño haya requerido el consentimiento de su representante legal, al alcanzar la mayoría de edad el niño podrá retirar su consentimiento. Pero si desea que continúe el tratamiento de sus datos, parece que el interesado deberá dar si consentimiento expreso siempre que se le requiera. Finalmente, el derecho de acceso lo ejerce el representante legal del niño, pero siempre en el interés de éste. En función de grado de madurez del niño, este derecho se ejercerá en su nombre y conjuntamente con el niño. En ciertos casos, el niño puede ejercer sus derechos por sí mismo.

[39] El considerando número 58 del Reglamento establece al respecto que "dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender".

[40] El artículo 4 apartado 25 del Reglamento define el servicio de la sociedad de la información como "todo servicio conforme a la definición del artículo 1 apartado 1 letra b) de la Directiva (UE) 2015/1535 del Parlamento y del Consejo".

La sentencia del Tribunal de Justicia de la Unión Europea de 2 de diciembre, asunto C-108/09 (KER/Optoka), apartados 22 y 28 ha señalado que servicios de la sociedad de la información incluye los contratos y otros servicios que se celebran o transmiten en línea. Cuando un servicio tenga dos componentes independientes desde el punto de vista económico, siendo una el componente en línea, como la oferta y la aceptación de una oferta en el contexto de la celebración de un contrato o la información relacionada con productos o servicios, incluidas las actividades de mercadotecnia, este componente se definirá como servicio de la sociedad de la información. El otro componente, que sería la prestación física o la distribución de bienes, no estará incluido en la noción de servicios de la sociedad de la información. La prestación de un servicio en línea formaría parte del ámbito de aplicación del término servicio de la sociedad de la información que se contiene en el artículo 8 del Reglamento.

[41] El artículo 1 de la Convención sobre los Derechos del Niño de Naciones Unidas de 20 de noviembre de 1989 "(…) se entiende por niño todo ser humano menor de dieciocho años, salvo que, en virtud de la ley que le sea aplicable haya alcanzado antes la mayoría de edad".

[42] El auto del Juzgado de Primera Instancia e Instrucción, número 4, de Massamagrell de 27 de abril de 2020 (JUR 2023,263336) no ha lugar de atribuir la facultad de decidir a ninguno de los progenitores sobre la prestación de consentimiento del menor para la cesión de sus datos personales en redes sociales o la cesión de su propia imagen en la web ixbi.es, pudiendo consentirlo el menor por sí mismo al ser un menor mayor de 14 años.

[43] GARCÍA HERRERA, V. (2018). "El válido consentimiento para el tratamiento de los datos personales de los menores de edad en Internet. Especial referencia al supuesto en que los representantes legales estén divorciados o separados (1)", *LA LEY Derecho de Familia, n*úmero 20, octubre-diciembre, pp. 6-7; en esta línea, REYES MÉNDEZ D. (2019). "El acceso del menor a las redes sociales y el problema de su autentificación: la necesidad de una respuesta tecnológica", *Diario La Ley, número 9335, sección Tribunal, 11 enero,* p. 3.

En el Dictamen 2/2009 sobre la protección de los datos personales de los niños del Grupo de Trabajo del Artículo 29 (WP 160), p. 6 se indica al respecto que "gradualmente, los niños pueden llegar a ser capaces de participar en la toma de decisiones que les conciernen. A medida que crecen deben participar con más regularidad en el ejercicio de sus derechos, incluidos los relativos a la protección de datos.

[44] CASTÁN PÉREZ-GÓMEZ, J (2015). "La patria potestad". En: M. Garrido De Palma (coord.) *Instituciones de Derecho Privado,* T. IV Familia, vol. 2, 2ª ed., Cizur Menor (Navarra): Civitas Thomson Reuters, p. 143.

[45] Vid., la sentencia del Tribunal Supremo, Sala de lo Civil, de 25 de febrero de 2009 (RJ 2009,2788).

[46] Vid., la sentencia del Tribunal Supremo, Sala de lo Civil, de 15 de enero de 2018 (RJ 2018,28).

[47] MARTOS DÍAZ, N. (2019). "Principios (artículos 6-11 del RGPD. Artículos 4-10 de la LOPDGDD)". En: J. López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Barcelona: Bosch, p. 340 precisa al respecto que "a día de hoy, hay escasos mecanismos tecnológicos que pueden verificar la identidad jurídica de una persona y los que hay no están accesibles para cualquier ciudadano que utilice los servicios de la sociedad de la información".

[48] Por su parte, GARCÍA HERRERA, V. (2018). "El válido consentimiento para el tratamiento de los datos personales de los menores de edad en Internet. Especial referencia al supuesto en que los representantes legales estén divorciados o separados (1)", *op. cit.*, p. 11 plantea la posibilidad que el menor que no puede prestar el consentimiento por sí solo, engañe al responsable del tratamiento, falsificando su DNI o falsificando la firma de sus representantes legales y presentando su DNI sin su consentimiento e incluso, sin su conocimiento. Para evitar esto, propone que "a los mecanismos previos de verificación del consentimiento, se podrían añadir otros aptos para llevar a cabo dicha comprobación *a posteriori*", así señala que "una vez facilitado el consentimiento por parte de los representantes legales, el responsable del tratamiento podría enviar un correo electrónico o un fax a la Dirección de e-mail o número de teléfono-fax facilitado por aquéllos en el formulario de consentimiento, para que respondan ratificando su declaración de voluntad, e incluso podrían hacer una llamada al número de teléfono proporcionado, con el mismo propósito".

[49] Vid., las sentencias del Tribunal Supremo, Sala de lo Civil, de 23 de julio de 1987 (RJ 1987,5809); de 31 de diciembre de 1996 (RJ 1996,9223); y, de 9 de julio de 2002 (RJ 2002,5905); y, las sentencias de la Audiencia Provincial de Murcia, secc. 1ª, de 27 de febrero de 1996 (AC 1996,358); de la Audiencia Provincial de Valencia, secc. 6ª, de 22 de julio de 1996 (AC 1996,1313); de la Audiencia Provincial de Sevilla, secc. 5ª, de 2 de octubre de 1998 (AC 1998,2037) ejercicio conjunto y función establecida en beneficio de los hijos; de la Audiencia Provincial de Vizcaya, secc. 1ª, de 8 de febrero de 1999 (AC 1999,3913) función al servicio del hijo; de la Audiencia Provincial de Ávila, de 18 de junio de 1999 (AC 1999,2279); de la Audiencia Provincial de Las Palmas, secc. 1ª, de 22 de junio de 1999 (AC 1999,8394); de la Audiencia Provincial de Murcia, secc. 1ª, de 18 de enero de 2000 (AC 2000,157); de la Audiencia Provincial de Málaga, secc. 6ª, de 26 de enero de 2012 (JUR 2012,329118); y, los autos de la Audiencia Provincial de Pontevedra de 25 de octubre de 2017 (JUR 2017,308428) donde se sobreseen las actuaciones por no revestir caracteres de infracción penal la revisión de las conversaciones de WhatsApp de su hija en presencia de la propia menor. Tal revisión se ejercita confirme el artículo 154 del CC que contiene, en relación con la patria potestad, la obligación de velar por ellos, educarles y procurarles una formación integral. El desarrollo de las redes sociales —como lo es WhatsApp— requiere atención y vigilancia de los progenitores para preservar la intimidad de los menores. Por lo que, hay ausencia de los requisitos típicos del artículo 194 del CP (descubrimiento de secreto), ni puede hablarse de falta de consentimiento, ni calificarse los mensajes como datos "reservados" atinentes a la intimidad desconocida u oculta de la menor que ésta no quiera que el padre conociera. Tampoco se da el elemento subjetivo de voluntad del denunciado en descubrir secreto o vulnerar la intimidad de la menor; y de la Audiencia Provincial de Asturias, secc. 4ª, de 13 de marzo de 2019 (JUR 2019,150994) oposición de la madre apelante a la publicación de fotos de la niña por parte del padre en redes sociales. El consentimiento de los menores deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten de acuerdo con la legislación civil, siendo en otro caso su representante legal quien habría de otorgarlo comunicando previamente al Ministerio Fiscal. La difusión y publicación de fotografías de la menor requiere en este caso el consentimiento de ambos progenitores. Es a sus progenitores a quienes, en el ejercicio de las funciones inherentes a la patria potestad, incumbe llevar a cabo un control parental en el uso de las nuevas tecnologías por parte de sus hijos menores de edad.

[50] Precisamente, en este deber de velar por los hijos y sobre la base de un control parental, la sentencia del Tribunal Supremo, Sala de lo Penal, de 10 de diciembre de 2015 (RJ 2015,6401) se ha considerado lícito el acceso a la cuenta abierta por su hija menor en una red social por parte de su madre sin contar con su anuencia ante la sospecha que pudiera ser víctima de un delito de ciberacoso o *Child Grooming* argumentando la Sala que "estamos hablando de un madre que, es titular de la patria potestad concebida no como poder sino como función tuitiva respecto de la menor. Es ella quien accede a esa cuenta ante signos claros que se estaba desarrollando una actividad presuntamente criminal en la que no cabría excluir la victimización de su hija. No puede el ordenamiento hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de controlar en caso como el presente en que las evidencias apuntaban inequívocamente en esa dirección. La inhibición de la padre ante hechos de esta naturaleza, contrariarían los deberes que le asigna por la legislación civil". Además señala la citada resolución que "se trata de una actividad delictiva no agotada sino viva: es objetivo prioritario hacerla cesar" y "la menor titular de la cuenta no solo no ha protestado por esta intromisión en su intimidad (lo que permite presumir un consentimiento o anuencia *ex post*), sino que además ha refrendado con sus declaraciones el contenido de esas comunicaciones ya producidas en los que constitutiva una prueba independiente de la anterior y no enlazada por vínculos de antijuridicidad".

[51] Vid., las sentencias del Tribunal Supremo, Sala de lo Civil, de 7 de noviembre de 2002 (RJ 2002,9484); de 5 de noviembre de 2003 (RJ 2003,8026); de 9 de julio de 2004 (RJ 2004,5246); y, de 5 de junio de 2012 (RJ 2012,6700).

[52] Vid., las Directrices sobre consentimiento, p. 29.

[53] Vid., las Directrices sobre consentimiento, p. 30.

[54] BRITO IZQUIERDO, N. (2017). "Tratamiento de los datos personales de menores de edad en la nueva normativa europea protectora de datos personales", *Actualidad Civil, número 5, mayo, 2018*, pp. 9-11; de la misma autora (2017). "Tratamiento de los datos personales de menores de edad: supuestos, límites, retos y desafíos", *LA LEY Derecho de Familia, Menores y Redes Sociales, número 14, abril-junio*, pp. 7-8. También hace referencia a la normativa COPPA, REYES MÉNDEZ, D. (2019). "El acceso del menor a las redes sociales y el problema de su autentificación: la necesidad de una respuesta tecnológica", *op. cit.,* p. 8.

[55] Como señala CASTÁN PÉREZ-GÓMEZ, J. (2015). "La patria potestad", *op. cit.,* pp. 75-76 deducida de la conducta del otro progenitor. Vid., asimismo, las sentencias de la Audiencia Provincial de Alicante, secc. 6ª, de 14 de mayo de 2014 (JUR 2014,219141); y, de la Audiencia Provincial de Madrid, secc. 24ª, de 4 de junio de 2014 (JUR 2014,240175) cotitularidad conjunta. Debe considerarse como la medida más normal de ejercicio de la patria potestad.

[56] DÍEZ GARCÍA, H. (2013). "Comentario al artículo 154 del Código Civil". En: R. Bervovitz-Rodríguez-Cano (coord.), *Comentarios al Código Civil,* T. I, Cizur Menor (Navarra): Thomson Reuters Aranzadi, p. 1593 quien añade que "esto no debe impedir que el padre actuante, en un ejercicio correcto y leal comunique inmediatamente su decisión al otro".

[57] DÍEZ GARCÍA, H. (2013). "Comentario al artículo 154 del Código Civil", *op. cit.,* p. 1599 que, además entiende que "habrá también que valorarse también la naturaleza del acto que se trata, pues no sería lo mismo la que resulta exigida para un acto ordinario o cotidiano que para un acto extraordinario (realizar un acto de disposición)"; PÉREZ ÁLVAREZ, M.Á. (2024). "La protección de los menores y las medidas de apoyo a las personas con discapacidad. La patria potestad". En: C. Martínez de Aguirre Aldaz (coord.), *Curso de Derecho Civil (IV) Derecho de Familia*, 7ª ed., Madrid: Edisofer, p. 403; CASTÁN PÉREZ-GÓMEZ, J. (2015). "La patria potestad", *op. cit.,* p. 94 señalan que, con esta norma se facilita el tráfico jurídico y se evita que se impugnen los actos llevados a cabo por uno de los progenitores.

[58] Vid., la sentencia de la Audiencia Provincial de Valencia, de 11 de junio de 1993 (AC 1993,1898).

[59] En la sentencia de la Audiencia Provincial de Cantabria, secc. 2ª, de 13 de enero de 2020 (JUR 2020,51511) se prohíbe la difusión de imágenes de la hija de la pareja en redes

sociales sin el previo consentimiento de ambos progenitores o con la autorización de juez en caso de desacuerdo; y asimismo, en la sentencia del Juzgado de Primera Instancia e Instrucción, número 2, de Aoiz/Agoitz de 8 de febrero de 2021 (JUR 2021,142537) se prohíbe a la pareja actual del padre subir imágenes de los hijos de la demandante en redes sociales. Prohibición que se hace extensiva a las futuras parejas que puedan tener cualquiera de los dos progenitores.

[60] Vid., las sentencias de la Audiencia Provincial de Barcelona, secc. 18ª, de 18 de septiembre de 2000 (AC 2001,37); y, de la Audiencia Provincial de Burgos, secc. 2ª, de 5 de noviembre de 2015 (JUR 2015,297307).

[61] Roj. STS 467/2023; ECLI:ES:TS:2023:467.

[62] TINTORÉ GARRIGA Mª.P. (2017). "Sharenting y la responsabilidad parental", *LA LEY Derecho de Familia. Monográfico Menores y Redes Sociales, número 14, abril-junio*, p. 2 se refiere, precisamente, a los "Padres Shareng" y señala que "actualmente, varios estudios concluyen que un porcentaje muy elevado de padres sube imágenes de sus hijos a redes sociales diariamente, siendo muy reducido el de aquellos que nunca han colgado ninguna fotografía de sus hijos". Los estudios, añade la autora también advierten que "el 80% de los bebés tiene presencia en internet al cumplir los seis meses de edad y el 25% incluso antes de haber nacido. Las motivaciones de los padres son muy diversas: tener informados a amigos y familiares sobre las actividades de sus hijos un 56%; mostrar el afecto hacia sus hijos un 49%; algunos consideran que es un buen lugar para guardar los recuerdos con un 34%; y otros grupos simplemente por rivalidad con las actividades de los hijos de otros padres, el 25%". Y, respecto a las plataformas más utilizadas y en las cuales se pueden encontrar más fotografías de menores señala la autora son: "Facebook con un 77% de información subida a la red; le sigue Instagram con un 48%; y el resto de plataformas y servicios de mensajería instantánea como Flickr, Twitter, WhatsApp cubren el otro porcentaje". ANDREU MARTÍNEZ, Mª.B. y GRIMALT SERVERA, P. (2024). "Responsabilidad civil, consentimiento y difusión de datos de menores en entornos digitales", *LA LEY Derecho de familia, nº 44, octubre*, p. 16 no descartan que un futuro los menores demanden a sus progenitores por esta sobreexposición.

[63] Entre los delitos que se cometen a través de medios tecnológicos podemos citar, el llamado delito de groomimg o Child grooming regulado en el artículo 183 ter del Código Penal en el que un adulto —habitualmente un depredador sexual— contacta con un menor a través de internet, telefonía móvil o cualquier otra tecnología de la información y la comunicación con el objeto de crear un vínculo afectivo, intentando ganarse su confianza y concertar un encuentro o una cita con claros fines sexuales. Incluye actuaciones que van desde un acercamiento con empatía y/o engaño, hasta el chantaje para obtener imágenes comprometidas del menor con el objeto de cometer abusos o agresiones sexuales contra el mismo, o de utilizar a los menores con fines exhibicionistas o pornográficos (artículos 183 y 189 del CP); el delito de ciberstalking o acoso reiterado y continuado a través de internet, impidiendo a la víctima desarrollar una vida normal. El delito de stalking o acoso reiterado o insistente no autorizado ni consentido por la víctima que, le impide desarrollar una vida normal, alternando el desarrollo de la misma está previsto en el artículo 172 ter del Código Penal; la usurpación de cuentas en redes sociales y la suplantación de identidad normalmente a través de la creación de perfiles falsos utilizando el nombre e imagen de otra persona que, puede ser un menor para cometer actos delictivos en la red: fraudes, ciberacoso, extorsión; la práctica conocida como "morphing" que es distorsionar, manipular y modificar la imagen de una persona difundida en la red, que puede ser la de un menor, con intenciones sexuales o vejatorias. En fin, las imágenes de los menores se pueden utilizar con fines de pornografía infantil. Vid., sobre tales formas delictivas, TINTORÉ GARRIGA, Mª.P. (2017). "Sharenting y la responsabilidad parental", *op. cit.*, p. 3; GUARDIOLA, M. (2017). "Menores y nuevas tecnologías: los nuevos retos en el sector legal en España", *LA LEY Derecho de Familia. Monográfico Menores y Redes Sociales, número 14, abril-junio*, pp. 1-3; POLVOROSA ROMERO, S. (2017). "El acoso escolar llevado a internet: los smartphone y los smarwatch", *LA LEY Derecho de Familia. Monográfico Menores y Redes Sociales, número 14, abril-junio*, pp. 6 y 8-9; GÓRRIZ ROYO, E.M. (2016).

"*On-line child grooming*" desde las perspectivas comparada y criminológica, como premisas de estudio del artículo 183 ter) 1º CP". En: Mª. L. Cuerda Arnau (dir.), *Menores y Redes sociales,* Valencia: tirant lo blanch, p. 265; VIDAL HERRERO-VIOR, Mª. S. (2024). "Casuística y regulación legal de la responsabilidad penal de menores infractores en delitos relacionados con la tecnología". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson, pp. 165-173.

[64] Vid., la sentencia de la Audiencia Provincial de Pontevedra, secc. 1ª, de 4 de junio de 2015 (JUR 2015,163149) dispone al respecto que "aun encontrándonos ante un caso de padres separados en que la guarda y custodia del hijo menor ha sido atribuida a la madre, en la sentencia de divorcio se ha acordado que, ambos progenitores conserven la patria potestad. Con lo cual, de pretender el Sr. Adrián la publicación de fotos de su hijo menor en las redes sociales habrá de recabar previamente el consentimiento de la progenitora recurrente y de oponerse ésta, podrá acudir a la vía judicial en orden a su autorización"; la sentencia de la Audiencia Provincial de Lugo, secc. 1ª, de 12 de mayo de 2016 (JUR 2016,145707) prohíbe el uso de la imagen del menor en redes sociales en contra del criterio de uno de los progenitores; la sentencia de la Audiencia Provincial de Cantabria, secc. 2ª, de 17 de mayo de 2021 (JUR 2021,183652) condena al padre a pagar 3.000 euros por vulnerar la intimidad y el derecho de imagen de su hija mediante la publicación de fotografías de la menor en internet. La utilización de la menor para exponer su imagen, se considera completamente innecesaria y en apoyo de unas expresiones reivindicativas en el conflicto que mantenía con la madre respecto a la custodia y comunicación con la menor. Por su parte, la sentencia de la Audiencia Provincial de Barcelona, secc. 18ª, de 22 de abril de 2015 (JUR 2015,164632) matiza que, cuando la publicación de las fotos de los menores en redes sociales se destinan únicamente a parientes y amigos más cercanos, no se atenta con ello al derecho de imagen del menor. Si bien, recuerda de nuevo que, ambas partes son cotitulares de la potestad parental sobre su hijo y ambos deben velar por la protección integral de su hijo, restringiendo la privacidad de las imágenes únicamente a sus familiares y amistades más cercanas. También en esta línea, la sentencia de la Audiencia Provincial de Lugo, secc. 1ª, de 15 de febrero de 2017 (JUR 2017,82242) pues, ante la falta de prueba que, el acceso a la cuenta fuese pública y el no constar más que la posibilidad de acceso a fotografías realizadas por la abuela a su círculo más íntimo de familiares y amigos entre los que se encontraba la madre y los padres de los niños, no se puede entender que se haya podido vulnerar la intimidad y la propia imagen de los menores por adecuarse el comportamiento de la abuela a los usos sociales más extendidos de publicación de noticias y fotografías de ámbito familiar ente los más allegados; y, la sentencia de la Audiencia Provincial de Madrid, secc. 12ª, de 6 de julio de 2017 (AC 2017,1201) acción de protección del derecho a la propia imagen de su hija menor frente a la conducta del padre y de la abuela paterna consistente en la obtención de determinadas fotografías del menor y su inclusión en los respectivos perfiles de Facebook de los demandados. En dichas fotografías se hace únicamente alarde de cariño y orgullo, en el caso de la abuela por su nieto. Todo ello sin perjuicio que cuando conoció la oposición de la madre, se retiraron las fotografías, por lo que se entiende que no hay intromisión en la intimidad del menor

En un caso de custodia compartida se prohíbe al padre la publicación en las redes sociales de fotografías, hechos o manifestaciones relativos a la intimidad de su hija o de la progenitora, vid., la sentencia de la Audiencia Provincial de Santa Cruz de Tenerife, secc. 1ª, de 6 de julio de 2018 (JUR 2018,273525). Igualmente, se prohíbe para el futuro la publicación de fotografías de la menor en las redes sociales por su padre y la pareja de éste, vid., la sentencia de la Audiencia Provincial de Navarra, secc. 3ª, de 26 de febrero de 2020 (JUR 2020,299802).

[65] Los menores sin tener en cuenta los riesgos que de ello se derivan, han generalizado una práctica de enviarse videos o imágenes con cierto contenido erótico, sexual, lo que puede dar lugar a la sextorsión, esto es, extorsionar a la víctima con la amenaza de difundir o divulgar las imágenes de forma generalizada sin no se cede a determinadas pretensiones económicas. El sexting está regulado en el artículo 197.7 del Código Penal consiste en el envío de contenidos de tipo sexual (fotografías y/o videos) producidos generalmente por el

propio remitente a otras personas por medio de teléfonos móviles; o, en fin, el ciberbullying o el ciberacoso entre escolares. La sentencia de la Audiencia Provincial de Granada, secc. 1ª, de 5 de junio de 2014 (JUR 2014,258699) señala que, el sexting "supone el envío de imágenes estáticas (folografías) o dinámicas (vídeos) de contenido sexual de mayor o menor carga erótica entre personas que voluntariamente consiente en ello y que forma parte de su actividad sexual que se desarrolla de manera libre (*Fundamento de Derecho Primero*). Vid., asimismo, las sentencias del Tribunal Supremo, Sala de lo Penal, de 24 de febrero de 2015 (Roj. STS 823/2015; ECLI:ES:TS:2015:823) en un caso de ciberacoso sexual (grooming); de 27 de marzo de 2017 (Roj. STS 1071/2017; ECLI:ES:TS:2027:1071) y de 15 de enero de 2020 (Roj. STS 69/2020; ECLI:ES:TS:2020:69) en un supuesto de delito sexual a menor de 13 años y child grooming; y, de 31 de octubre de 2024 (Roj. STS 5580/2024; ECLI:ES:TS:2024:5580) en un caso sexting y ciberacoso.

Por su parte, GUARDIOLA, M. (2017). "Menores y nuevas tecnologías: los nuevos retos en el sector legal en España", *op. cit.,* p. 3 se refiere a un nuevo caso de ciberacoso el llamado "happy slapping" en el que "dos o más acosadores atacan a un menor y en el que además de la agresión física, hay una agresión moral devastadora puesto que esa agresión es grabada y difundida en las redes y a través de Internet". Por su parte, POLVOROSA ROMERO, S. (2017). "El acoso escolar llevado a internet: los smartphone y los smarwatch", *op. cit.,* p. 6 señala que, los últimos estudios sitúan la edad en la que empieza a darse el sexting en niñas de 7 y 8 años; y, como características del ciberbullying señala las siguientes: "1. La víctima sufre un deterioro de la autoestima y dignidad personal dañando su estatus social, provocándole victimización psicológica, estrés emocional y rechazo social; 2. La situación de acoso se dilata en el tiempo: excluyendo las acciones puntuales; 3. El comportamiento por parte del acosador es intencional, no accidental; 4. El medio utilizado para llevar a cabo el acoso es tecnológico: internet y cualquier medio asociados a esta forma de comunicación: telefonía móvil, redes sociales; 5. Puede evidenciarse cierta jerarquía de poder; 6. Es frecuente los episodios de ciberacoso puedan estar ligados a situaciones de acoso en la vida real y de acoso escolar; 7. El alcance 24x7 que hace referencia a que la potencial agresión se puede producir 24 horas al día, los 7 días de la semana; y 8. El anonimato o engaño acerca de la autoría desde el que se puede producir la agresión" (p. 7).

[66] GUARDIOLA, M. "Menores y nuevas tecnologías: los nuevos retos en el sector legal en España", *op. cit.,* p. 4 se refiere a diversas herramientas de control parental como: Quostodio, Talk Kids, kiddle, Yahoo Kids, Kids place, y Teen Safe entre otras.

[67] Vid., la sentencia de la Audiencia Provincial de Pontevedra, secc. 1ª, de 28 de mayo de 2020 (JUR 2020,196683) se sustituye el actual régimen de custodia compartida por guarda y custodia materna del menor, ante la actitud permisiva del padre con las nuevas tecnologías.

[68] Vid., la sentencia del Tribunal Europeo de Derechos Humanos, secc. 3ª, de 20 de junio de 2017 (TEDH 2017,66); las sentencias del Tribunal Supremo, Sala de lo Civil, de 30 de junio de 2015 (RJ 2015,2661); y, de 25 de noviembre de 2015 (RJ 2015,5324) menores de edad fotografiados en el momento de su recogida por sus padres a la salida del colegio con un ligero difuminado de sus ojos que permiten perfectamente reconocer su rostro; y, las sentencias de la Audiencia Provincial de Madrid, secc. 19ª, de 21 de febrero de 2013 (AC 2013,924) fotografía de una menor en una vida al aire libre, siendo una publicación no autorizada por el padre, de la Audiencia Provincial de Huelva, secc. 3ª, 8 junio 2014 fotografías de una menor junto a sus padres en revista del corazón sin difuminar ni ocultar su rostro; de la Audiencia Provincial de Madrid, secc. 9ª, de 3 de mayo de 2017 (AC 2017,966) pixelado insuficiente en periódico digital que, no impide el reconocimiento del menor y ausencia de consentimiento; de la Audiencia Provincial de Valladolid, sección 3ª, de 31 de mayo de 2018 (AC 2018,1806); y, de la Audiencia Provincial de Toledo, sección 1ª, de 5 de julio de 2018 (JUR 2018,265069).

[69] TINTORÉ GARRIGA, Mª.P. (2017). "Sharenting y la responsabilidad parental", *op. cit.*, p. 4 expone dos casos, así señala que "en Austria una joven de 18 años denunció a sus padres por no retirar el álbum de fotos familiares que había colgado en las redes". Y, asimismo, indica que, en Francia el año pasado "las autoridades advirtieron a los padres que la ley prevé

multas de hasta 60.000 euros y hasta un año de cárcel si se difunden fotos de una persona sin su consentimiento". En fin, recuerda la autora que "los menores con la mayoría de edad, también pueden presentar demandas contra sus progenitores por haber subido fotos o videos que consideren denigrantes o dañen su propia imagen".

[70] El Grupo de Trabajo del Artículo 29 en su Dictamen 5/2006 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido, adoptado el 25 de noviembre de 2005 (WP 115), pp. 9-10 señala con respecto a la localización de menores que: "el Grupo ha observado el desarrollo de servicios de localización pata los padres que permiten, por ejemplo, conectarse a un sitio web para conocer el paradero de un hijo al que le han dado un teléfono móvil. Este tipo de servicios plantea una serie de problemas relacionados especialmente con la necesidad de mantener un equilibrio entre los distintos intereses y derechos en juego". Ciertamente, "es muy probable que un servicio por el que se pueda conocer el paradero de sus hijos mediante un teléfono móvil satisfaga los deseos de algunos padres". Por lo que, el Grupo hace un llamamiento para que al menos se vigile la utilización de este tipo de servicios y señala que "se deberían prestar de acuerdo con las normas sobre el tratamiento de datos de localización y de conformidad con la legislación nacional específica relativa a la edad de los menores en cuestión". En consecuencia, señala que "los proveedores de servicios han de introducir los procedimientos apropiados para identificar a las personas que se registren como padres y circunscribir el acceso al servicio a dichas personas".

[71] Vid., la sentencia del Tribunal Supremo, Sala de lo Civil, de 17 de septiembre de 1996 (RJ 1996,6722) principio del interés del menor inspirador de todo el régimen; el Auto del Tribunal Superior de Justicia de Cataluña, Sala de lo Civil y Penal, secc. 1ª, de 14 de junio de 2012 (RJ 2012,8798) interés del menor representa un concepto jurídico indeterminados que se debe precisar en cada caso concreto; y, las sentencias de la Audiencia Provincial de Asturias, secc. 5ª, de 16 de marzo de 2004 (JUR 2004,106754); y de la Audiencia Provincial de Cádiz, secc. 5ª, de 2 de febrero de 2010 (JUR 2010,186025) principio inspirador de todo el régimen de la patria potestad, y, el Auto de la Audiencia Provincial de La Rioja, secc. 1ª, de 5 de diciembre de 2018 (JUR 2019,37872) cualquier medida que se adopte en relación con el menor tiene presente el interés más digno de protección el del menor.

[72] FERNÁNDEZ ACEVEDO, J. (2019). "Redes sociales y aplicaciones móviles", *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, coordinador J. López Calvo, Bosch, Barcelona, 2019, pp. 910-911. Para GRIMALT SERVERA P. (2017). *La responsabilidad civil por los daños causados a la dignidad humana por los menores en el uso de las redes sociales*, Granada: Comares, Granada, pp. 47-48 "no se puede generalizar la consideración de medio de comunicación a los efectos del artículo 4.3 de la LOPJM a toda red social", pero si entiende que aquellas que "tienen vocación de ser públicas y sin fronteras" como por ejemplo Facebook o Twitter pueden ser equiparados, pues, pueden tener el mismo eco que pueda tener un medio de comunicación tradicional, mientras que los que tienen vocación de redes restringidas como whatsapp no responden a criterios de medio de comunicación del artículo 4.3 de la LOPJM, por lo que no les resultará de aplicación".

Por su parte, la sentencia del Tribunal Supremo, Pleno de la Sala Segunda, de 2 de junio de 2022 (RJ 2022,3414) considera lugar de la comisión de un delito a los efectos del artículo 48 del CP no sólo a los lugares o espacios físicos, sino también los espacios virtuales de encuentro y comunicación que se crean en internet.

[73] Vid., el Dictamen 5/2009 sobre las redes sociales en línea, p. 5.

En todo caso, como servicios de la sociedad de la información les resulta aplicable el artículo 16.1 de la Ley 34/2002 de 11 de junio de Servicios de la Sociedad de la Información y del Comercio Electrónico que, entiende que son responsables de la información almacenada siempre que, tengan conocimiento efectivo que, la información almacena es ilícita. De ahí que, se considere que el prestador de servicios tiene el conocimiento efectivo "cuando el órgano competente haya declarado la ilicitud de los datos, ordenando su retirada o que se imposibilite el acceso a los mismos o se hubiera declarado la existencia de la lesión y el prestador conociera la correspondiente resolución sin perjuicio de los procedimientos de

detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse". Si bien, al respecto, la sentencia del Tribunal Supremo, Sala de lo Civil, de 9 de diciembre de 2009 (Roj. STS 7684/2009; ECLI:ES:TS:2009:7684) pone de manifiesto que, conocimiento efectivo no solo tiene lugar cuando el órgano competente haya declarado previamente la ilicitud de los datos almacenados o la lesión de los derechos de los actores y ordenado la retirada de los contenidos, no cabe prescindir que conocimiento efectivo también tiene lugar cuando el mismo se obtiene por el prestador del servicio a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas el alcance de cualquiera, una afectiva aprehensión de la realidad que se trate. Por lo que, estima que, el propio nombre de la página en la que se incluían los contenidos ya suponía un elemento fáctico de su posible ilicitud y la necesaria actuación del prestador del servicio. Por su parte, la sentencia de la Audiencia Provincial de Lugo, sección 1ª, de 9 de julio de 2009 (JUR 2009,328919) no hay acreditación de connivencia entre los internautas y los administradores de la página. Asimismo, hay una falta de acreditación que los creadores del foro tuvieran un conocimiento efectivo que, la información fuese ilícita. Retirada inmediata de los comentarios tras la comunicación efectuada por la Guardia Civil.

De todas formas, para MESSÍA DE LA CERDA BALLESTEROS, J.A. (2017). "La protección del honor de los menores en las redes sociales", *LA LEY Derecho de Familia. Monográfico Menores y Redes Sociales, número 14, abril-junio*, p. 4 "es obvio que, en estos casos resulta necesario encontrar una posición de equilibrio en la posición del titular de la red social que, se debate entre sus posibilidades de control y la elevada exigencia que ello puede suponer".

[74] El Grupo de Trabajo del Artículo 29 recomienda con respecto a la información que deben proporcional los servicios de redes sociales que: "1. Los proveedores de SRS adviertan adecuadamente a los usuarios sobre los riesgos de ataque a su intimidad y a la de otros cuando ponen información en línea en los SRS; 2. Los SRS recuerden a sus usuarios que poner en línea información relativa a otras personas puede perjudicar su derecho a la intimidad y a la protección de datos; y, 3. Los SRS aconsejen a sus usuarios que no pongan en línea fotografías o información relativa a otras personas son el consentimiento de éstas". Vid., el Dictamen 5/2009 sobre las redes sociales en línea, p. 8.

[75] GUTIÉRREZ MAYO, E. (2024), "La figura del Ministerio Fiscal en la defensa de los derechos digitales". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson, p. 83 señala que "según un Estudio Anual de Redes Sociales de la AIB Spain, publicado en mayo de 2023 en España, un 85% de los internautas mayores de edad (entre los 12 y 74 años) utilizan las redes sociales, lo que representa 30,2 millones de usuarios, en el caso de los jóvenes (entre 18-24 años) este porcentaje aumenta hasta el 94%". Y añade la autora que "las redes sociales más visitadas/utilizadas en España son: whatsApp (87%), Facebook (65%), Instagram (65%), Youtube (63%) y Twitter (38%), Telegram (33%), TikTok (32%). Telegram, Linkedln y TikTok son las redes que más crecen en usuarios respecto a 2022".

[76] En esta línea, vid., CABALLERO, A. (2024). "Mercantilización de los datos de los menores por las plataformas de redes sociales", *op. cit.*, pp. 5-7.

[77] Vid., El Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, p. 5.

[78] Vid., El Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, pp. 31-36.

[79] El Comité Europeo de Protección de Datos (CEPD) ha adoptado en su reunión plenaria de abril unas directrices sobre el tratamiento de datos personales mediante tecnología blockchain (*Guidelines 02/2025 on processing of personal dato though blokchain technologies*). Estas directrices están sometidas a consulta pública hasta el 9 de junio de 2025, dando a las partes interesadas la posibilidad de presentar sus observaciones. Blokchain es un registro digital distribuido que permite validar transacciones y garantizar la integridad de los datos sin una autoridad central. También permite esta tecnología manjar y transferir datos de forma segura garantizando su integridad y trazabilidad. Precisamente, en sus directrices, el Comité

explica cómo funcionan las cadenas de bloques, evaluando las diferentes arquitecturas posibles y sus implicaciones para el tratamiento de datos personales. Estas directrices destacan la importancia de aplicar medidas técnicas y organizativas en las primeras fases del diseño del tratamiento. Además, destacan que las organizaciones deben llevar a cabo una evaluación de impacto sobre la protección de datos (EIPD) antes de tratar datos personales mediante tecnologías de blokchain cuando sea probable que el tratamiento suponga un alto riesgo para los derechos y libertades de personas. En fin, las directrices ofrecen ejemplos de diferentes técnicas de minimización de datos, así como de tratamiento y almacenamiento de datos personales. asimismo, el Comité destaca la importancia de los derechos de las personas, especialmente en materia de transparencia, rectificación y supresión de datos personales.

[80] Aclara el considerando número 12 del RIA que: "El término "basado en una máquina" se refiere al hecho de que los sistemas de IA se ejecutan en máquinas. La referencia a objetivos explícitos o implícitos subraya que los sistemas de IA pueden funcionar con arreglo a objetivos definidos explícitos o a objetivos implícitos. Los objetivos del sistema de IA pueden ser diferentes de la finalidad prevista del sistema de IA en un contexto específico". A esto añade que "otra característica principal de los sistemas de IA es su capacidad de inferencia. Esta capacidad de inferencia se refiere al proceso de obtención de resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos y virtuales, y a la capacidad de los sistemas de IA para deducir modelos o algoritmos, o ambos, a partir de información de entrada o datos. Las técnicas que permiten la inferencia al construir un sistema de IA incluyen estrategias de aprendizaje automático que aprenden de los datos cómo alcanzar determinados objetivos y estrategias basadas en la lógica y el conocimiento que infieren a partir de conocimientos codificados o de una representación simbólica de la tarea que debe resolverse. La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos, al permitir el aprendizaje, el razonamiento o la modelización". En fin, asimismo, se indica que "los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. La capacidad de adaptación que un sistema de IA podría mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso. Los sistemas de IA pueden utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente del producto (integrado) o contribuye a la funcionalidad del producto sin formar parte de él (no integrado)".

Por su parte, COTINO HUESO, L. (2024). "¿Qué es "inteligencia artificial" para el Reglamento?. Análisis, delimitación y aplicaciones prácticas". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, p. 120 aclara a lo expuesto que "hay que partir que no todo sistema informático que permite procesos o decisiones automatizados es *automáticamente* IA. No se consideran "inteligencia artificial" aunque pueden razonar o modelar automáticamente. Ello es importante si el sistema de decisiones automatizado no es un Sistema de IA, aunque se utilices para un caso de uso y finalidades de alto riesgo (anexo III), quedará también fuera de la aplicación del RIA".

[81] Para BARRIO ANDRÉS, M. (2024). "Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia artificial". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch, pp. 35-36 "la definición no pretende abarcar los sistemas de software o enfoques de programación tradicionales más sencillo y el RIA habilita a la Comisión para que elabore directiva sobre su aplicación que resultarán en este punto fundamentales". A lo que añade que "la definición positivizada en el RIA pretende reflejar el consenso científico que los objetivos de un sistema de IA pueden ser *explícitos* (por ejemplo, cuando están directamente programados en el sistema por un desarrollador humano) o *implícitos*, o cuando el sistema es capaz de aprender nuevos objetivos)". Por su parte, MARTÍN CASALS, M. (2023). "Las propuestas de la Unión Europea para regular la responsa-

bilidad civil por los daños causados por sistemas de inteligencia artificial", *Indret, núm. 3*, p. 61 señala que esta definición "(…) se quiere basar en características clave de la inteligencia artificial, como sus capacidades de aprendizaje, razonamiento o modelado, para distinguirla de sistemas de software o enfoques de programación más simples. Dado que los sistemas de IA están diseñados para operar con diferentes niveles de autonomía, la definición requiere que el sistema tenga al menos cierto grado de independencia de las acciones de los controles humanos y de las capacidad para operar sin intervención humana".

[82] Un análisis de la clasificación y gestión de riesgos previsto en el RIA, vid., CAMPOS ACUÑA, C. (2024). "Las 15 claves del Reglamento Europeo de Inteligencia Artificial (AI Act) (1)", *El Consultor de los Ayuntamientos, de 15 de julio*, pp. 3-5.

[83] Un grupo de investigadores del Instituto Tecnológico de Massachusetts (MIT) presenta una base de datos denominada "Repositorio de Riesgos de la IA" con 777 riesgos asociados a la IA extraídos de 43 taxonomías. Se describe la iniciativa "adoptar la IA puede estar plagado de peligros. Los sistemas pueden ser tendenciosos, repetir falsedades, o incluso volverse adictivos".

[84] Para un tratamiento más amplio de la materia, vid., FERNÁDEZ HERNÁNDEZ, C. (2024). "Comentario al artículo 6 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia, tirant lo blanch, pp. 184 a 205. En relación con los sistemas de categorización biométrica señala que "es uno de los aspectos en los que el RIA colisiona con el RGPD, en concreto con el artículo 9" (p. 201). Por su parte, ESCAJEDO SAN-EPIFANIO, L. (2024). "El reconocimiento biométrico en el Reglamento de inteligencia artificial: exenciones, prohibiciones y especialidades de alto riesgo". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, p. 234 después de analizarlos sistemas de reconocimiento biométrico, lleva a cabo una crítica "por cuanto se refiere al reconocimiento biométrico automatizado, el RIA no pasará a la historia por su grandes aportaciones. Cuanto texto, para decir tan poco y tan mal. Tan pronto parece que entra a regular algún supuestos, inmediatamente se enreda en tanto matices y salvedades que resulta muy penoso llegar a determinar el alcance real de sus preceptos". En esta línea, SIMÓN CASTELLANO, P. (2024). "El resto de los sistemas de inteligencia artificial prohibidos o inaceptables en el Reglamento de Inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, pp. 286-287 tas indicar que el Comité Europeo de Protección de Datos ha realizado un cambio interpretativo con sus directrices de 2022 y la AEPD ha exteriorizado ese cambio de criterio en la Guía de Tratamientos de control de presencia mediante sistemas biométricos de 23 de noviembre de 2023; a juicio del autor "esta guía de la AEPD supone un freno u óbice insalvable para que las empresas puedan apoyarse en determinados sistemas para cumplir con la obligación legal de mantener un control de jornada horaria, que cabe recordar es un derecho de los trabajadores y una obligación empresarial".

[85] Un análisis más profundo de la materia, vid., GONZÁLEZ MENESES GARCÍA-VALDECASAS, M. (2024). "Comentario al artículo 6 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch, pp. 207-227. Por su parte, COTINO HUESO, L. (2024). "Alcance y delimitación de los sistemas de alto riesgo en el Reglamento de inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, p. 313 precisa que "se ha expuesto que ya no hay automatismo por el que si el sistema tiene una de las 25 finalidades del Anexo III pasa a ser automáticamente un SAR. En la evolución del RIA se ha incorporado el requisito que el sistema de IA debe tener una influencia sustancial en la toma de decisiones. Así, se considera que un sistema de IA influye sustancialmente en la toma de decisiones si sus resultados afectan directamente decisiones importantes para las finalidades dl Anexo III". A lo que añade "afortunadamente, este criterio se ha regulado de modo mucho más perfilado que las daciones únicamente automatizada del

artículo 22 del RGPD. Este criterio es esencial para determinar la clasificación de alto riesgo y, por tanto, si aplican las obligaciones correspondientes".

[86] Como precisa en esta línea, CASTILLO PARRILLA, J.A. (2024). "Inteligencia artificial de uso general, modelos fundacionales (y "Chat GPT") en el Reglamento de Inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi., pp. 775-776 "los modelos IA de uso general son modelos IA entrenados con gran cantidad de datos utilizando supervisión a gran escala que presenta un grado considerable de generalidad y son capaces de realizar de manera competente una gran variedad de tareas distintas así como integrarse en diversos sistemas o aplicaciones posteriores. (…) Un modelo IA uso general presenta riesgo sistémico si tiene capacidades de gran impacto (de acuerdo con el Anexo XIII RIA, que podrán actualizarse según la evolución técnica) o si presenta unas repercusiones potenciales considerables en el mercado interior debido a su alcance". En fin, indica que "los modelos de IA generativa, por su parte, presenta ciertos retos relacionados con la responsabilidad civil derivada del uso de la IA, la desinformación, la protección de datos personales y la propiedad intelectual". Respecto al tratamiento de datos personales manifiesta que: "los problemas se refieren a si y cómo deben tratarse los datos personales tanto en el entrenamiento de las herramientas de la IA como posteriormente en su uso".

[87] Los considerandos 99 y 100 del RIA establecen respectivamente: "Los grandes modelos de IA generativa son un ejemplo típico de un modelo de IA de uso general, ya que permiten la generación flexible de contenidos, por ejemplo, en formato de texto, audio, imágenes o vídeo, que pueden adaptarse fácilmente a una amplia gama de tareas diferenciadas" y "Cuando un modelo de IA de uso general esté integrado en un sistema de IA o forme parte de él, este sistema debe considerarse un sistema de IA de uso general cuando, debido a esta integración, el sistema tenga la capacidad de servir a diversos fines. Un sistema de IA de uso general puede utilizarse directamente e integrarse en otros sistemas de IA".

[88] Para un tratamiento más amplio de la materia, vid., RECIO GAYO, M. (2024). "Comentario al artículo 16 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch, pp. 311 a 322; y, asimismo PALMA ORTIGOSA, A. (2024). "Régimen general de obligaciones de proveedores y responsables del despliegue en el Reglamento de inteligencia artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, pp. 447-471; CHAVELI DONET, E. (2024). "La evaluación de impacto de derechos fundamentales por quienes despliegan sistemas de inteligencia artificial en el Reglamento". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, pp. 495-533; SIMÓN CASTELLANOS, P. (2024). "Los sistemas de gestión de riesgos como obligación específica para los sistemas de inteligencia artificial de alto riesgo en el artículo 9 del Reglamento". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, pp. 535-564; RAMÓN FERNÁDEZ, FCA. (2024). "Sistemas de gestión de calidad, documentación técnica y conservación en el Reglamento". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, pp. 595-611; y, ARRELLANO TOLEDO, W. y MERCHÁN MURILLO, A. (2024). "La obligación de conservar registros de los sistemas de alto riesgo en el Reglamento de Inteligencia Artificial". En: L. Cotino Hueso y P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia artificial de la Unión Europea*, Cizur Menor (Navarra): Aranzadi, pp. 613-626.

[89] El considerando número 93 del RIA señala que: "(…) Los responsables del despliegue se encuentran en una posición óptima para comprender el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, detectar potenciales riesgos significativos que no se previeron en la fase de desarrollo, al tener un conocimiento más preciso del contexto de uso y de las personas o los colectivos de personas que probablemente se vean afectados, entre los que se incluyen colectivos vulnerables. Los responsables del despliegue de los

sistemas de IA de alto riesgo que se enumeran en un anexo del presente Reglamento también desempeñan un papel fundamental a la hora de informar a las personas físicas y, cuando tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, deben, en su caso, informar a las personas físicas de que son objeto de la utilización de un sistema de IA de alto riesgo. Esta información debe incluir la finalidad prevista y el tipo de decisiones que se toman. El responsable del despliegue también debe informar a las personas físicas de su derecho a una explicación con arreglo al presente Reglamento. Por lo que respecta a los sistemas de IA de alto riesgo que se utilizan a efectos de la garantía del cumplimiento del Derecho, esa obligación debe ejecutarse de conformidad con el artículo 13 de la Directiva (UE) 2016/680".

[90] El considerando número 56 señala, en esta línea, que: "El despliegue de sistemas de IA en el ámbito educativo es importante para fomentar una educación y formación digitales de alta calidad y para que todos los estudiantes y profesores puedan adquirir y compartir las capacidades y competencias digitales necesarias, incluidos la alfabetización mediática, y el pensamiento crítico, para participar activamente en la economía, la sociedad y los procesos democráticos. No obstante, deben clasificarse como de alto riesgo los sistemas de IA que se utilizan en la educación o la formación profesional, y en particular aquellos que determinan el acceso o la admisión, distribuyen a las personas entre distintas instituciones educativas y de formación profesional o programas de todos los niveles, evalúan los resultados del aprendizaje de las personas, evalúan el nivel apropiado de educación de una persona e influyen sustancialmente en el nivel de educación y formación que las personas recibirán o al que podrán acceder, o supervisan y detectan comportamientos prohibidos de los estudiantes durante las pruebas, ya que pueden decidir la trayectoria formativa y profesional de una persona y, en consecuencia, puede afectar a su capacidad para asegurar su subsistencia. Cuando no se diseñan y utilizan correctamente, estos sistemas pueden invadir especialmente y violar el derecho a la educación y la formación, y el derecho a no sufrir discriminación, además de perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, las personas con discapacidad o las personas de cierto origen racial o étnico o con una determinada orientación sexual".

[91] ChaptGPT es un modelo de IA desarrollado por Open AI, basado en la arquitectura de modelos del lenguaje (LLM). Su propósito es generar texto de manera coherente y responder preguntas en un lenguaje natural. Desde su lanzamiento en 2022 ha evolucionado con versiones más avanzadas como GPT-4 yGPT-4 o. Con posterioridad se ha desarrollado otras herramientas de IA (copilot —microsft— y gemini —google—).

Todos estos modelos generales se han integrado en diversas aplicaciones y servicios, permitiendo a los usuarios acceder a respuestas rápidas, generar contenido y mejorar la productividad.

Para un tratamiento más profundo de los modelos de uso general, vid., MUÑOZ GARCÍA, Mª.C. (2024). "Comentarios a los artículos 52 a 55 del Reglamento". En: M. Barrio Andrés (dir.), *El Reglamento Europeo de Inteligencia artificial*, Valencia: tirant lo blanch, pp. 537 a 582; de la misma autora (2024). "Taxonomía de los modelos de IA de uso general. Probabilidad de generar riesgos de alto impacto y las necesidades de identificarlos". En: J.A. Moreno Martínez y P.J. Femenía López (coords.), *Inteligencia artificial y derecho de daños: cuestiones actuales*, Madrid. Dykinson, pp. 787-816.

[92] El considerando número 93 del RIA señala, al respecto, que: "Aunque los riesgos relacionados con los sistemas de IA pueden derivarse de su diseño, también pueden derivarse riesgos del uso que se hace de ellos. Por ello, los responsables del despliegue de un sistema de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales, como complemento de las obligaciones del proveedor al desarrollar el sistema de IA. Los responsables del despliegue se encuentran en una posición óptima para comprender el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, detectar potenciales riesgos significativos que no se previeron en la fase de desarrollo, al tener un conocimiento más preciso del contexto de uso y de las personas o los

colectivos de personas que probablemente se vean afectados, entre los que se incluyen colectivos vulnerables. Los responsables del despliegue de los sistemas de IA de alto riesgo que se enumeran en un anexo del presente Reglamento también desempeñan un papel fundamental a la hora de informar a las personas físicas y, cuando tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, deben, en su caso, informar a las personas físicas de que son objeto de la utilización de un sistema de IA de alto riesgo. Esta información debe incluir la finalidad prevista y el tipo de decisiones que se toman. El responsable del despliegue también debe informar a las personas físicas de su derecho a una explicación con arreglo al presente Reglamento. Por lo que respecta a los sistemas de IA de alto riesgo que se utilizan a efectos de la garantía del cumplimiento del Derecho, esa obligación debe ejecutarse de conformidad con el artículo 13 de la Directiva (UE) 2016/680".

[93] PARDO DE VERA, M.M. (2024). "La incidencia de la inteligencia artificial en los derechos de los menores. Regulación legal y problemática actual". En: D. Rodríguez (coord.), *La protección de la infancia en entornos digitales*, Madrid: Dykinson, p. 125 manifiesta que "la UE considera que Meta es responsable de estimular la adicción en los niños mediante el uso de las llamadas "madrigueras de conejo" (*rabbit hole*), un concepto inspirado en Alicia en el País de las Maravillas". Para la citada autora "las "madrigueras de conejo" describen la situación en la que los usuarios, impulsados por el diseño de algoritmos sofisticados y adictivos, se sumergen en una serie interminable de contenidos relacionados, manteniéndose enganchados durante horas generando una clara adicción".

[94] Informe sobre el desarrollo de un entorno digital seguro para la juventud y la infancia en sus páginas 112-113 señala que, los proveedores que ofrecen plataformas, aplicaciones y servicios, tratan datos personales de sus usuarios. En muchos casos, el modelo de negocio de estas entidades las lleva a intentar alargar las sesiones de los usuarios cuando utilizan sus productos, o a incrementar su nivel de compromiso y la cantidad de datos personales que se recogen sobre ellos. Todos estos factores tendrían un impacto positivo en el retorno de la inversión realizada en el desarrollo y mantenimiento de aplicaciones y servicios que teóricamente se ofrecen de forma gratuita o a un coste muy reducido. Por este motivo algunos proveedores añaden operaciones adicionales al tratamiento de datos personales de sus usuarios para implementar patrones de diseños engañosos y adictivos cuyo objetivo es manipular las acciones y decisiones de los usuarios. El Comité Europeo de Protección de Datos (CEPD) ya abordó los patrones engañosos en el documento "Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them". La AEPD ha llevado a cabo una revisión sistemática de la evidencia científica existente acerca de los patrones adictivos en diferentes plataformas, aplicaciones y servicios (redes sociales, pero también plataformas de vídeo o música, de contenido para adultos, juegos, entornos de aprendizaje, aplicaciones de salud y bienestar, etc.) lo que supone abordar, desde una perspectiva complementaria, nuevos casos de uso, en el "Informe sobre la influencia de los patrones adictivos en Internet", y en especial sobre los menores y adolescentes en julio de 2024 completando las directrices del CEPD mediante un enfoque unificado de los patrones engañosos y adictivos. Los patrones adictivos se han definido como características, atributos o prácticas de diseño que determinan una manera concreta de utilizar plataformas, aplicaciones o servicios digitales y persiguen que los usuarios dediquen mucho más tiempo a utilizarlos o con un mayor grado de compromiso del esperado, pudiendo no ser conveniente o saludable para ellos. El análisis en el documento referenciado muestra cómo el tratamiento de datos personales de los usuarios en numerosas plataformas, aplicaciones y servicios incluyen operaciones específicas —todas ellas engañosas— para aumentar su tiempo de conexión o su nivel de compromiso, de manera que se influya en sus decisiones. Esto les permite utilizar sus datos personales con este fin o para generar nuevos datos y realizar focalización (que permite personalizar con un grado muy fino las estrategias adictivas). Todos estos patrones podrían necesitar datos personales como entrada, recoger o generar nuevos datos personales, o influir en el comportamiento y la toma de decisiones del usuario en el marco del tratamiento de los mismos. La incorporación de operaciones que implementan patrones adictivos a

los tratamientos de datos personales tiene importantes implicaciones para diferentes aspectos relativos a la protección de datos, como la responsabilidad proactiva (accountability), la aplicación efectiva de las obligaciones de protección de datos desde el diseño y por defecto, la transparencia, la licitud, la lealtad, la limitación de la finalidad, la minimización de datos, las decisiones automatizadas que afectan significativamente a los usuarios o el tratamiento de categorías especiales de datos. También implica un riesgo para los derechos y libertades de todos los usuarios. En particular, para el derecho a su integridad física y psíquica, pero también pudiendo provocar discriminación, exclusión, manipulación, socavar la autonomía individual, influir en su proceso de pensamiento, sus emociones, su comportamiento, limitar su libertad de información y expresión, generar autocensura y afectar a la autonomía y desarrollo. Estas consecuencias pueden ser especialmente graves para la infancia y los usuarios y las usuarias más jóvenes.

[95] El considerando número 110 del RIA manifiesta, en este contexto, que: "Los códigos de buenas prácticas deben constituir una herramienta fundamental para el cumplimiento adecuado de las obligaciones previstas en el presente Reglamento para los proveedores de modelos de IA de uso general. Los proveedores deben poder basarse en códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones. Mediante actos de ejecución, la Comisión podrá decidir aprobar un código de buenas prácticas y conferirle una validez general dentro de la Unión o, alternativamente, establecer normas comunes para la puesta en práctica de las obligaciones pertinentes si, para el momento en que el presente Reglamento sea aplicable, no ha podido finalizarse un código de buenas prácticas o la Oficina de IA no lo considera adecuado. Una vez que se haya publicado una norma armonizada y que la Oficina de IA la considere adecuada para cubrir las obligaciones pertinentes, el cumplimiento de una norma armonizada europea debe dar a los proveedores la presunción de conformidad. Además, los proveedores de modelos de IA de uso general deben poder demostrar el cumplimiento utilizando medios alternativos adecuados si no se dispone de códigos de buenas prácticas o de normas armonizadas, o si deciden no basarse en ellos".

[96] Los SVE son soluciones que tienen como fin comprobar que quien está accediendo a cierto contenido online es una persona mayor de edad, pudiendo catalogarse en función del modo utilizado: verificación por declaración de edad, basada Por su parte, los sistemas de verificación de edad (SVE) son soluciones que tienen como fin comprobar que quien está accediendo a cierto contenido online es una persona mayor de edad, pudiendo catalogarse en función del modo utilizado: verificación por declaración de edad, basada en la comprobación de documento oficial-como DNI o tarjeta bancaria—, estimación de edad, o a través de certificados digitales o carteras de identidades.

Para un análisis específico de estos SVE, vid., ALAMILLO-DOMINGO, I. (2024). "La verificación de edad para el acceso a servicios digitales a la luz del nuevo marco de identidad del reglamento EIDAS 2", *LA LEY Derecho de familia, nº 44, octubre*, pp. 1-22.

[97] PARDO DE VERA, M.M. (2024). "La incidencia de la inteligencia artificial en los derechos de los menores. Regulación legal y problemática actual", *op. cit*, 2024, p. 124 destaca que "en el ámbito educativo, por ejemplo, los programas que utilizan IA están revolucionando la manera en que los niños aprenden, adaptando materiales a las necesidades de cada alumno o monitorizando su progreso de forma que antes ni siquiera podríamos imaginar". Esto, continúa la autora "permite una educación mucho más personalizada y efectiva, ajustándose a los ritmos y estilos de aprendizaje de cada alumno. Además, las herramientas de IA tienen el potencial de facilitar el acceso a una educación de calidad".

[98] Señala IKER NAVARRO en Diario LA LEY 30 de mayo de 2025 que "se está hablando mucho de la utilidad que tienen los sistemas de inteligencia artificial generativa para abordar tareas rutinarias o que exigen el procesamiento de un enorme volumen de datos con el fin de extraer conclusiones. Pero para obtener el máximo rendimiento de la IA es necesario darle las indicaciones necesarias y adecuadas, de forma precisa y con detalles para que pueda ofrecer las respuestas y los resultados más adecuados al escenario que tiene que resolver. De ahí que la mayor parte de las organizaciones que están adoptando esta tecnología empiecen por

formar a sus empleados sobre cómo plantear estas peticiones o instrucciones, más conocidas como prompts". Y se pregunta ¿qué es un prompt?. A lo que contesta "es una instrucción clara, precisa y detallada con la que pedimos al sistema que realice una tarea. La idea es que la IA procese correctamente el mensaje y genere el resultado que se espera de ella". Y concluye se puede decir que hay que especificar la siguiente información: 1. Plantear un objetivo claro y preciso; 2. Ofrecer contexto, es decir, detalles adicionales sobre lo que se necesita para que la respuesta se adapte bien a cada escenario concreto; 3. Incluir parámetros específicos, como estilo, formato o tono, si se trata de un texto; 4. Testeo y ajustes, es decir, repetir las peticiones con nuevas indicaciones para lograr dar con el resultado más preciso".

[99] Vid., las sentencias del Tribunal Supremo, Sala de lo Penal, de 15 de septiembre de 2020 (RJ 2020,3511) ciberacoso sexual: contactos con una menor de 16 años a través de internet, del teléfono o de cualquier otra tecnología de la información y la realización de actos dirigidos a embaucarle con la finalidad que facilite al autor material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor. No requiere violencia o intimidación; si ben, la conducta del autor admite, por lo general, una mezcla de promesas y amenazas o conductas similares a través de las cuales se pretende conseguir la finalidad típica doblegando la voluntad del menor; de 21 de enero de 2021 (RJ 2021,305); y, de 10 de julio de 2023 (RJ 2023,4519) contracto a través de redes sociales con menor de 16 años para mantener relaciones sexuales; y, el Auto del Tribunal Supremo, Sala de lo Penal, de 30 de enero de 2025 (JUR 2025,23477).

GUADIX GARCÍA, N. (2024). "Los derechos de la infancia en la era digital", *LA LEY Derecho de Familia, número 44, octubre*, p. 3 señala que "las tasas de sexting (intercambio de contenidos digitales eróticos autoproducidos) en estudiantes españoles de ESO van desde el 13,8% (sexting activo, productores), al 42% (sexting pasivo, receptores), situándose en el 11,4% el porcentaje de adolescentes que afirma haber sufrido presiones o intentos de chantaje o sextorsión. Aunque el sexting es practicado por ambos géneros, las presiones las sufren generalmente las chicas. En 3º y 4º de ESO las tasas de sexting se duplican. El 57,2% de los estudiantes de ESO reconoce haber aceptado a desconocidos en una red social, y el 21,5% haber llegado a quedar en persona con gente que conoció exclusivamente a través de la Red. 1 de cada 10 adolescentes ha recibido una proporción sexual por parte de un adulto a través de Internet; y alrededor del 90% de los adolescentes dentro 13 y 18 años han consumido pornografía alguna vez en su vida, cifra que supone un incremento del 20% respecto a 2018".

[100] Vid., la sentencia del Tribunal Supremo, Sala de lo Penal, de 5 de febrero de 2025 (JUR 2025,18379).

[101] Según Save The Children: quien graba no suele participar directamente en la agresión física, pero es doblemente culpable: por no intervenir para impedir que suceda y por grabar, subir y compartir las imágenes en otro momento. Los jóvenes no siempre creen que se esté haciendo daño a la víctima: en muchos casos la violencia es únicamente un medio para generar contenido "gracioso" o "entretenido", que sucesivamente se utiliza para ganar popularidad en el entorno *online*.

Está claro que en el *happy slapping* suelen participar múltiples actores que causan daño a la persona grabada, una red extensa de actores que comparten un acto violento para después intentar hacerlo viral y ser más "populares"", Y ofrece como datos que, en España se estima que 76.643 jóvenes sufrieron *happy slapping* durante su infancia. La edad media en la que lo sufrieron por primera vez fue a los 14 años y, tal y como sucede en el ciberacoso, la persona que suele causar la violencia es un compañero o amigo del colegio. Sin embargo, también destacan otras personas responsables, como por ejemplo exparejas o familiares.

[102] Vid, las sentencias del Tribunal Supremo, Sala de lo Penal, de 18 de mayo de 2023 (RJ 2023,3688); y, de 3 de abril de 2024 (JUR 2024,342014).

[103] Vid., las sentencias del Tribunal Supremo, Sala de lo Penal, de 21 de maro de 2017 (RJ 2017,1263); y, de 24 de noviembre de 2021 (JUR 2021,5680).

Según INCIBE "una vez iniciada esa relación de amistad, ganarán confianza. El objetivo es hacer que el menor se sienta cómodo y comprendido, incluso puede que le engatuse con al-

gún regalo, físico o virtual (un móvil nuevo, dinero, saldo para hablar por teléfono o créditos para su videojuego favorito), o con la promesa de una relación perfecta. De este modo, poco a poco podrán intimar, subir el tono de las conversaciones y conseguir que el menor baje la guardia, para que le confíe una imagen o vídeo comprometido, o algún secreto privado. Esto se utilizará como arma de chantaje: una vez que tiene en su poder material para manipular al menor, le exigirá más imágenes y vídeos, o incluso llegar a un encuentro en persona. Si no cumple con sus deseos, le amenazará con hacer públicos todos esos contenidos comprometidos". Y añade que "las consecuencias para el menor o adolescente pueden ser de diferente gravedad dependiendo del alcance del delito, aunque en cualquier caso, el riesgo de daños para el menor es alto: 1. Abuso y agresión sexual. La petición de imágenes o vídeos de carácter sexual es en sí mismo un abuso. Aunque a veces es el menor el que envía este contenido de forma "voluntaria", manipulando en cualquier caso por parte del agresor, en otras ocasiones la víctima es chantajeada para que facilite los materiales comprometidos. En último término, el agresor podría llevar a cabo agresiones sexuales físicas comprometiendo la seguridad física y emocional del menor; 2. Ansiedad y depresión. Entre las consecuencias psicológicas más habituales aparecen la ansiedad y la depresión, presentándose secuelas muy diversas en función del abuso, su duración, el apoyo recibido y otras variables; 3. Problemas derivados en el rendimiento académico, sociabilidad y afectividad. Enfrentarse a una situación de *grooming* afecta seriamente a todos los ámbitos de la vida del menor, desde daños a su autoestima y la confianza en sí mismo, hasta la disminución de la concentración y la atención en clase, o la pérdida de amistades. También puede aparecer desinterés por sus actividades de ocio favoritas o dificultades a la hora de relacionarse con otras personas, entre otros".

En fin, concluye que "en una situación de *grooming*, las víctimas tienden a ocultar las consecuencias por sentimientos de vergüenza o culpabilidad. Pueden incluso pensar que la relación que mantienen con el agresor es real, y no ser conscientes de que están siendo o han sido víctimas de un abuso".

[104] Vid., la sentencia del Tribunal Supremo, Sala de lo Penal, de 26 de mayo de 2021 (RJ 2022,2734).

[105] BOCG, serie A, número 51-1, de 11 de abril de 2025, pp. 1-37.

[106] Para ALMENAR PINEDA, FCO. (2024). "Nuevos escenarios para el Derecho y el Derecho Penal en la protección de los menores: el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales", *LA LEY Derecho de familia, nº 44, octubre*, pp. 9-10 señala que "desde la perspectiva punitiva, la pena de alejamiento de los entornos virtuales, cuando el delito se comete en estos espacios, da definitivamente entrada al domicilio informático en nuestro ordenamiento penal, cumple con la prevención general y especial, responde a las exigencia doctrinales y jurisprudenciales y lo hace con unos límites precisos de duración". Y respecto, a la inclusión de las ultra falsificaciones considera el citado autor que "constituye una previsión que da cobertura a nuevas modalidades delictivas pluriofensivas, y también se anticipa a las venideras especialmente en el desarrollo de la inteligencia artificial que pueden encontrarse sin respuesta efectiva al no estar actualmente contempladas en el Código Penal, por los límites que el principio de legalidad implica". Asimismo, indica que "la ubicación entre los delitos contra la integridad moral es coherente con los bienes que trata de proteger".

[107] MARTÍNEZ MARTÍNEZ, R. (2024). "El consentimiento en el tratamiento de los datos de carácter personal: un riesgo sistémico para los menores", LA LEY Derecho de Familia, número 44, octubre, p. 13 entiende el autor que "la elevación de edad de consentimiento a los 16 años por el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, o va a suponer ningún cambio sustancial para la gestión del riesgo que afecta a los menores en nuestros días. En este sentido, ofrece un mayor grado de confianza el marco regido por el Reglamento de Servicios Digitales cuando obliga a los grandes operadores a implementar metodologías de análisis de riesgos, permite interpretar la existencia de un mayor nivel de exigencia en la aplicación de las estrategias de protección

de datos desde el diseño y por defecto, limita extraordinariamente la publicidad con destino a los menores y ofrece un blindaje frente a la utilización de algoritmos de perfilado".

[108] El artículo 33.2 l): "l) La prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual, por tiempo superior a cinco años".

[109] El artículo 33.3 letra m): "m) La prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual, por tiempo de seis meses a cinco años".

[110] El artículo 33.4 letra j): "j) La prohibición de acceso o de comunicación a través de redes sociales, foros, plataformas de comunicación o cualquier otro lugar en el espacio virtual, por tiempo de un mes a menos de seis meses".

[111] Se modifica el primer párrafo del artículo 57.1 que queda redactado: *"1. Las autoridades judiciales, en los delitos de homicidio, aborto, lesiones, contra la libertad, de torturas y contra la integridad moral, trata de seres humanos, contra la libertad e indemnidad sexuales, la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el honor, el patrimonio, el orden socioeconómico y las relaciones familiares y los delitos cometidos con ocasión del ejercicio de los derechos fundamentales y libertades públicas; atendiendo a la gravedad de los hechos o al peligro que el delincuente represente, podrán acordar en sus sentencias la imposición de una o varias de las prohibiciones contempladas en el artículo 48, por un tiempo que no excederá de diez años si el delito fuera grave, o de cinco si fuera menos grave"*.

[112] ALMENAR PINEDA, FCO. (2024). "Nuevos escenarios para el Derecho y el Derecho Penal en la protección de los menores: el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales", *LA LEY Derecho de Familia, número 44, octubre*, p. 7 justifica la necesaria reforma de este artículo 186 "ante el desarrollo vertiginoso de las nuevas tecnologías y la sobreexposición en muchos casos a visionados potencialmente peligrosos para ese colectivo, se hace necesario que la normativa penal también trate de progresar en la tutela de su libertad sexual". A esto añade que "la conducta tipificada no quedaría circunscrita solo al empleo de un medio inmediato, sino de cualquiera herramienta, dando así cobertura a instrumentos o artificios indirectos por los cuales se hiciera llegar material pornográficos a las citadas personas". Por último, "el elemento "a sabiendas" añade un plus al método empleado, que se identifica con "la clara conciencia que entre el público receptor hay menores de edad o personas necesitadas de especial protección y, de que el consumo por parte de estos sujetos de esta clase de material supone una afectación a un proceso de maduración sexual".

[113] CABALLERO, A. (2024). "Mercantilización de los datos de los menores por las plataformas de redes sociales", *op. cit.*, pp. 5-6 alude a pagar con datos, es pagar "el valor de esos datos y el alcance que tiene el entorno digital para recogerlos es opaco para la mayoría de los usuarios, especialmente para los niños, niñas y adolescentes. Lo que se presenta como servicios gratuitos ofrecidos por estas grandes plataformas, realmente no lo son". También hace referencia al estudio del think tank Epicenter donde señala que "el valor anual por usuario derivado de la explotación de sus datos personales es aproximadamente 81,61 euros, o que equivale a unos 6,80 euros al mes. Esta cifra se basa en el valor añadido del mercado publicitario y la proporción atribuible al uso de datos personales para generar anuncio personalizados", y añade la autora que "existen otros estudios que establece un valor superior. Cabe cita l artículo publicado por Jaron Lanier y E. Glen Weyl en Havard Business Rewiew en el que se estima un valor de 20.000 dólares americanos para una familia americana de 4 miembros".

[114] Vid., la Memora de la AEPD 2024, pp. 1-201.

[115] Vid., las sentencias del Tribunal Supremo, Sala de lo Civil, de 22 de enero de 1991 (RJ 1991,304) omisión del deber de vigilancia; de 7 de enero de 1992 (RJ 1992/149); y de 12 de mayo de 1999 (RJ 1999,4576) culpa *in vigilando*; y, las sentencias de la Audiencia Provincial de Girona, secc. 2ª, de 11 de julio de 1994 (JUR 1994,12678); de la Audiencia Provincial de Vizcaya, secc. 3ª, de 18 de enero de 2000 (AC 2000,284); de la Audiencia Provincial de Burgos, secc. 2ª, de 4 de abril de 2002 (JUR 2002,163928) culpa *in vigilando*; de la Audiencia Provin-

cial de Alicante, secc. 8ª, de 10 de diciembre de 2009 (JUR 2010,117452) culpa *in educando*; y, de la Audiencia Provincial de león, secc. 2ª, de 11 de julio de 2016 (JUR 2016,210476) omisión del deber de vigilancia.

[116] PARRA LUCÁN, MªÁ. (2016). "Responsabilidad por hecho ajeno". En: C. Martínez de Aguirre Aldaz (coord.), *Curso de Derecho Civil, T. II, vol. II Contratos y responsabilidad civil,* Madrid: Edisofer, p. 440; ABRIL CAMPOY, J.M. (2003). "La responsabilidad de los padres por los daños causados por sus hijos", *Revista Crítica de Derecho Inmobiliario, número 675, enero-febrero*, p. 28; DÍAZ ALABART, S. (1987). "La responsabilidad por los actos ilícitos dañosos de los sometidos a patria potestad y tutela", *Anuario de Derecho Civil*, p. 803; PEÑA LÓPEZ, F. (2013). "Comentario al artículo 1903 del Código Civil". En: R. Bercovitz Rodríguez-Cano (dir.), *Comentarios al Código Civil, T. IX*, Valencia: tirant lo blanch, p. 13004. Asimismo, vid., las sentencias del Tribunal Supremo, Sala de lo Civil, de 10 de julio de 1985 (RJ 1985,3968); de 22 de enero de 1991 (RJ 1991,304); de 8 de marzo de 2002 (RJ 2002,1912); y, de 10 de noviembre de 2006 (RJ 2006,7170); la sentencia del Tribunal Superior de Justicia de Navarra, Sala de lo Civil y Penal, de 4 de diciembre de 1995 (RJ 1995,9667); y, las sentencias de la Audiencia Provincial de Teruel, secc. única, de 29 de noviembre de 2000 (AC 2000,2417) omisión del deber de vigilancia; de la Audiencia Provincial de Córdoba, secc. 2ª, de 5 de diciembre de 2001 (JUR 2002,44482) omisión del deber de vigilancia. Culpa propia del guardador; de la Audiencia Provincial de Burgos, secc. 2ª, de 4 de abril de 2002 (JUR 2002,163928); de la Audiencia Provincial de Las Palmas, secc. 5ª, de 28 de abril de 2003 (AC 2003,1779); de la Audiencia Provincial de Sevilla, secc. 5ª, de 30 de noviembre de 2007 (JUR 2008,133131) culpa *in educando*; de la Audiencia Provincial de Madrid, secc. 18ª, de 11 de octubre de 2007 (AC 2007,2382); de la Audiencia Provincial de Granada, secc. 4ª, de 15 de febrero de 2013 (JUR 2013,177887) responsabilidad por culpa propia; de la Audiencia Provincial de Tarragona, secc. 1ª, de 15 de diciembre de 2015 (JUR 2016,12545) culpa propia de los padres; y, de la Audiencia Provincial de Cáceres, secc. 1ª, de 3 de mayo de 2016 (AC 2016,2057) responsabilidad por hecho de otro.

[117] Vid, la sentencia de la Audiencia Provincial de Murcia, secc. 5ª, de 6 de abril de 2009 (JUR 2009,314010) lesiones causadas por el menor. Moderación judicial de la responsabilidad ante la no concurrencia en el padre de dolo o imprudencia grave que favoreciera la conducta del menor.

[118] YZQUIERDO TOLSADA, M. (2015). *Responsabilidad civil extracontractual. Parte General. Delimitación y especies. Elementos. Efectos o consecuencias*, 3ª ed., Madrid: Dykinson, pp. 307-309; GÓMEZ CALLE, E. (2016). "Comentario al artículo 1903 del Código Civil". En: A. Cañizares Laso, P. de Pablo Contreras, J. Orduña Moreno y R. Valpuesta Fernández (dirs.), *Código Civil comentado, vol. IV*, 2ª ed., Navarra: Civitas Thomson Reuters, p. 1376. Vid., asimismo, la sentencia del Tribunal Supremo, Sala de lo Civil, de 30 de junio de 1995 (RJ 1995,5272) además de por culpa propia y omisión del deber de vigilancia; de 11 de marzo de 2000 (RJ 2000,1520) responsabilidad por semiriesgo o cuasiobjetiva; de 8 de marzo y de 10 de noviembre de 2006 (RJ 2006,1076; RJ 2006,7170) responsabilidad cuasiobjetiva o por riesgo. Presunción de culpa de los progenitores; y, las sentencias de la Audiencia Provincial de Vizcaya, secc. 4ª, de 8 de octubre de 1997 (AC 1997,2208); de la Audiencia Provincial de Murcia, secc. 1ª, de 14 de noviembre de 1996 (AC 1996,2386); de la Audiencia Provincial de Valencia, secc. 7ª, de 19 de noviembre de 2001 (JUR 2004,33028); de la Audiencia Provincial de Barcelona, secc. 17ª, 29 octubre 2004 (AC 2004/1944); de la Audiencia Provincial de Madrid, secc. 18ª, de 11 de octubre de 2007 (AC 2007,2382); de la misma Audiencia Provincial, secc. 10ª, de 28 de septiembre de 2010 (JUR 2011/24867); de la Audiencia Provincial de Valencia, secc. 7ª, de 23 de enero de 2012 (JUR 2012,171580) responsabilidad por riesgo o cuasiobjetiva. Omisión de los deberes de vigilancia y control de los hijos menores de edad; y de la Audiencia Provincial de Córdoba, secc. 1ª, 23 abril 2018 (AC 2018/1435).

[119] Vid., las sentencias de la Audiencia Provincial de Cantabria, secc. 3ª, de 24 de junio de 1998 (AC 1998,1185); y de la Audiencia Provincial de Ourense, secc. 2ª, de 28 de febrero de 2005 (JUR 2005,96794).

[120] GÓMEZ CALLE, E. (1992). *La responsabilidad civil de los padres*, Madrid: Montecorvo, p. 309; DE ÁNGEL YAGÜEZ, R. (1993). *Tratado de responsabilidad civil*, Madrid: Civitas, p. 349.

[121] Vid., la sentencia de la Audiencia Provincial de Castellón, secc. 1ª, de 22 de julio de 1999 (JUR 1999,309294) indica que en los casos de separación, nulidad o divorcio la responsabilidad será del progenitor con el que se encuentre el menor en el momento de producirse el hecho dañoso.

[122] Vid., las sentencias de la Audiencia Provincial de Zaragoza, de 31 de marzo de 2003 (AC 2003,1801); y, de la Audiencia Provincial de Cáceres, de 14 de abril de 2004 (AC 2004,146900).

[123] Vid., la Audiencia Provincial de León, secc. 2ª, de 9 de enero de 1998 (AC 1998,2816).

[124] YZQUIERDO TOLSADA, M. (2015). *Responsabilidad civil extracontractual. Parte General. Delimitación y especies. Elementos. Efectos o consecuencias, op. cit.,* pp. 311-314. En esta línea, GÓMEZ CALLE, E. (2016). "Responsabilidad de los padres y centros docentes". En: L. Fernando Reglero Campos y José Manuel Bustos Lago (coords.), *Tratado de Responsabilidad Civil, T. II*, 5ª ed., Navarra: Thomson Reuters Aranzadi, pp. 1204 a 1225.

[125] Vid., la sentencia del Tribunal Supremo, Sala de lo Civil, de 8 de julio de 1997 (RJ 1997,5576) indica que se trata de una deuda ganancial en cuanto corresponde a ambos padres la responsabilidad.

[126] YZQUIERDO TOLSADA, M. (2015). *Responsabilidad civil extracontractual. Parte General. Delimitación y especies. Elementos. Efectos o consecuencias, op. cit.,* p. 316. Vid., asimismo, en relación con el régimen de sociedad de gananciales, la sentencia del Tribunal Supremo, Sala de lo Civil, de 12 de mayo de 1981 (RJ 1981/2047).

[127] Vid., las sentencias de la Audiencia Provincial de Córdoba, secc. 2ª, de 5 de diciembre de 2005 (JUR 2006,129569) responsabilidad de los padres por el acoso realizado por su hijo en internet a otro menor; y, de la Audiencia Provincial de Asturias, secc. 5ª, de 22 de julio de 2013 (AC 2013,1599) responsabilidad de los padres por los daños y perjuicios materiales o morales ocasionados a los actores por las amenazas verbales vertidas en internet por el hijo de los demandados al hijo de los demandantes.

[128] Vid., la sentencia de la Audiencia Provincial de Guipúzcoa, secc. 1ª, de 10 de septiembre de 2002 (AC 2002,1681) agresión sexual y física de gran violencia cometida por menores. Responsabilidad directa y solidara de sus representantes legales. Daños morales; la Audiencia Provincial de Castellón, secc. 1ª, de 19 de abril de 2006 (JUR 2006,241011); de la Audiencia Provincial de Valencia, secc. 8ª, de 30 de diciembre de 2008 (AC 2009,270) maltrato de un menor a otro; de la Audiencia Provincial de Murcia, secc. 5ª, 6 abril 2009 (JUR 2009,314010); y, de la Audiencia Provincial de Guipúzcoa, secc. 2ª, de 10 de noviembre de 2015 (JUR 2016,60252).

[129] YZQUIERDO TOLSADA, M. (2015). *Responsabilidad civil extracontractual. Parte General. delimitación y especies. Elementos. Efectos o consecuencias*, *op. cit.,* pp. 327-328. Vid., también la sentencia de la Audiencia Provincial de La Rioja, 26 marzo 2010 (JUR 2010/219912).

[130] PARRA LUCÁN, MªÁ. (2016). "Responsabilidad por hecho ajeno", *op. cit.,* p. 445; ATIENZA NAVARRO, Mª.L. (2000). *La responsabilidad civil por los hechos dañosos de los alumnos menores de edad*, Granada: Comares, p. 493; YZQUIERDO TOLSADA, M. (2015). *Responsabilidad civil extracontractual. Parte General. delimitación y especies. Elementos. Efectos o consecuencias*, *op. cit.,* p. 329; GRIMALT SERVERA, P. (2017). *La responsabilidad civil por los daños causados a la dignidad humana por los menores en el uso de las redes sociales, op. cit.,* pp. 91 y 93 que señala que "el artículo 61.3 de la LORPM establece un listado de posibles "gestores efectivos del proceso educativo", atribuyendo la responsabilidad al sujeto sobre el que recae la obligación de velar y educar al menor en el momento en el que está cometiendo el delito". Asimismo, vid., la sentencia del Tribunal Supremo, Sala de lo Civil, de 1 de marzo de 1984 (RJ 1984,1193); y, las sentencias de la Audiencia Provincial de Guipúzcoa, secc. 1ª, de 10 de septiembre de 2002 (AC 2002,1681); de la Audiencia Provincial de Zaragoza, de 23 de

junio de 2005 (JUR 2005,168430); de la Audiencia Provincial de Barcelona de 13 de julio de 2006 (JUR 2007,56390); de la Audiencia Provincial de Valencia, secc. 6ª, de 30 de diciembre de 2009 (JUR 2010,150358) condena por delitos de abuso sexual y violación. Responsabilidad solidaria de los padres de los menores por transgresión de su deber de vigilancia o *"in educando"*, no pudiendo ampararse en la edad y falta de madurez del menor; de la Audiencia Provincial de Asturias, secc. 5ª, de 23 de julio de 2013 (AC 2013,1559) acoso por internet. Daños y perjuicios materiales y morales ocasionados a los actores por las amenazas vertidas por la hija menor de los demandados, a través de internet a la hija de los demandantes; de la Audiencia Provincial de Almería, secc. 3ª, de 14 de mayo de 2015 (AC 2015,1005) daño psicológico a cada del abuso sexual; de la Audiencia Provincial de Palencia, de 18 de marzo de 2016 (AC 2016,425) acoso escolar causado a la hija menor de los demandantes por parte de la hija de los codemandados. Continuidad en la acción acosadora e intimidatoria de una menor hacia la otra que responde a una dinámica de actos y menos precios que no pueden ni separarse, ni desvincularse; de la Audiencia Provincial de Guipúzcoa, secc. 2ª, de 27 de mayo de 2016 (AC 2016,1329) daños psicológicos ocasionados a la profesora por alumna menor de edad.; de la Audiencia Provincial de Les Illes Balears, secc. 5ª, de 6 de octubre de 2016 (AC 2018,2056) agresiones sexuales ocasionadas por menor de 13 años, a otro menor de 7 de años. Reconocimiento de la autoría y de los hechos; de la Audiencia Provincial de Asturias, secc. 7ª, de 21 de abril de 2020 (JUR 2020,180323) lesiones causadas por menor. Responsabilidad de los padres. La menor propinó una bofetada o manotazo en la cara al demandante, que puede calificarse de fuerte, lo que le provocó la lesión; de la Audiencia Provincial de Murcia, secc. 1ª, de 27 de abril de 2020 (AC 2020,1214) acoso a menor: acreditada la presión o coacción ejercida por el hijo del demandado a la menor para que esta se hiciese fotos desnuda y las publicase en Tuenti. Daños morales en la cantidad de 8.000 euros; y, de la Audiencia Provincial de Vizcaya, secc. 3ª, de 20 de septiembre de 2024 (LA LEY 328230,2024) condena de un menor por difundir en Instagram fotos íntimas de otro menor. La demandante ejercita una acción de indemnización de daños y perjuicios derivados de la difusión en Instagram de fotos íntimas de su hijo por otro menor, el demandado. La demanda fue desestimadas en primera instancia por estimar el titular del Juzgado que la acción ejercitada es la civil derivada del delito y que no concurre el requisito de la existencia de una condena penal, pues las diligencias preliminares que se siguieron por los mismos hechos fueron archivadas por prescripción. Sin embargo, la Audiencia Provincial de Vizcaya revoca la resolución de instancia por considerar que la ejercitada s la acción de responsabilidad civil por culpa extracontractual, tal y como quedó explicado en el acto de juicio por la defensa de la actora, sin que las aclaraciones realizadas en la vista supusiesen una modificación indebida de la causa de pedir. En cuanto al fondo del asunto, la Sala estima acreditado que fue el menor demandado quien, desde la dirección IP correspondiente al router del domicilio en el que residía con sus abuelos, creó los perfiles de Instagram desde lo que se enviaron las fotografías y los mensajes en los que amenazó a la víctima con difundir fotografías intimas si no le enviaba más imágenes de él y de terceros. Dicho hechos se realizaron de manera continuada y a lo largo del tiempo. De las declaraciones de los agentes se instruyeron las diligencias penales resultando que único morador de la vivienda que hacía un uso continuado de la wifi y que tenía los conocimientos suficientes para crear los perfiles era el demandado. Todo ello unid a las diligencias penales, a las averiguaciones realizadas por la Ertzaintza y al hecho que el menor demandado no pusiera su móvil a disposición de los agentes cuando se lo requirieron, son indicios suficientes según el Tribunal para determinar su responsabilidad civil. Por tanto, aunque no exista certeza absoluta, las pruebas constituyen indicios sólidos y suficientes a efectos civiles para considerar responsable y condenarle, junto a su madre, a indemnizar solidariamente a los demandantes pro los daños morales causados, los cuales han quedado plenamente probados, debiéndose añadir a la indemnización el importe de las facturas que fueron abonadas por los tratamientos psicológicos.

[131] DÍAZ ALABART, S. (1987). "La responsabilidad por los actos ilícitos dañosos de los sometidos a patria potestad y tutela", *op. cit.*, p. 828.

[132] Vid., las sentencias de la Audiencia Provincial de Asturias, secc. 5ª, de 22 de julio de 2013 (AC 2013,1559) acoso en internet; y, de la Audiencia Provincial de Palencia, secc. 1ª, de 18 de marzo de 2016 (AC 2016,425) acoso escolar.

[133] AC 2020,100.

[134] PARRA LUCÁN, MªÁ. (2016). "Responsabilidad por hecho ajeno", *op. cit.,* p. 456. Asimismo, vid., las sentencias del Tribunal Supremo, Sala de lo Civil, de 15 de febrero de 1994 (RJ 1004,1308); 29 diciembre 1998 (RJ 1998/9980); de 4 de junio de 1999 (RJ 1999,4286); de la Audiencia Provincial de Valencia, secc. 8ª, de 20 de noviembre de 1995 (AC 1995,2056); de la Audiencia Provincial de Cantabria, secc. 2ª, de 23 de abril de 1999 (JUR 1999,447399); de la Audiencia Provincial de Las Palmas, secc. 5ª, de 28 de abril de 2003 (AC 2003,1779) culpa *in vigilando* o *in eligiendo*; de la Audiencia Provincial de Málaga, secc. 7ª, de 26 de diciembre de 2003 (JUR 2004,60420) daños físicos y morales sufridos por in traumatismo. Negligencia de la profesora encargada de la custodia del menor en el tiempo de descanso; de la Audiencia Provincial de Álava, secc. 1ª, de 27 de mayo de 2005 (AC 2005,1062) acoso escolar o "bullying": Sufrimiento por la hija de los actores de una persecución física y moral por parte de una serie de alumnos de la ikastola demandada. No adopción por la misma de las medidas de prevención pertinentes en evitación de tales comportamientos. Daños psíquicos constitutivos de daño moral de la menor; de la Audiencia Provincial de Madrid, secc. 18ª, de 11 de octubre de 2007 (AC 2007,7382) culpa *in vigilando* y responsabilidad cuasiobjetiva; de la Audiencia Provincial de Murcia, secc. 5ª, de 14 de octubre de 2008 (JUR 2009,122614) daños derivados de los tocamientos realizados a una menor en los aseos del colegio durante el tiempo de recreo por otros dos menores; de la Audiencia Provincial de Madrid, secc. 10ª, de 18 de diciembre de 2008 (AC 2009.124) responsabilidad prácticamente objetiva. Acoso escolar o "bullying", malestar y sufrimiento experimentado por l hijo de los actores de once años de edad, quien fue objeto de burlas y males tratos en horario escolar; de la Audiencia Provincial de Madrid, secc. 12ª, de 22 de junio de 2009 (AC 2010,1095) defecto de organización o vigilancia del personal del centro; de la Audiencia Provincial de Barcelona, secc. 1ª, de 27 de enero de 2010 (JUR 2010,82805) coso escolar a menor. No consta la adopción de ninguna medida de prevención, ni que se ideara un plan de actuación y seguimiento que permitirá conocer y valorar la situación de hostigamiento que estaba sufriendo el hijo de los actos y de la que tenía constancia tras una agresión sufrida por el mismo en el pato por lo que fueron sancionados los responsables; de la Audiencia Provincial de Madrid, secc. 25ª, de 11 de mayo de 2012 (AC 2012,384) acoso escolar o "bullying": situación de acoso u hostigamiento al menor, continuada y reiterada en el tiempo. Actitud omisiva del centro demandado. Falta de adopción de medida alguna con relación a los hechos dura de posponer separa del grupo al menor hostigado, en lugar de separar a sus hostigadores, e incluso deshacer el grupo; de la Audiencia Provincial de Barcelona, secc. 11ª, de marzo de 2017 (AC 2017,607) acoso escolar. Responsabilidad por no adoptar el Centro todas las medidas a su alcance para poner fin a la situación. No constando vigilancia, atención o cautela, no solo con el menor, sino que incluyera a los compañeros que protagonizaban los conflictos con aquel, a fin de frenar la existencia de los mismos; de la Audiencia Provincial de Madrid, secc. 8ª, de 24 de abril de 2017 (JUR 2017,149463) falta de vigilancia directa y presencial; y, de la Audiencia Provincial de Madrid, secc. 9ª, de 10 de enero de 2023 (JUR 2023,79379) responsabilidad del centro educativo por acoso escolar sufrido por una menor. Las medidas adoptadas ni fueron adecuadas al adoptarse solo medidas de carácter preventivo insuficientes ante las señales de alarma que enviaba la menor. Indemnización de 10.000 euros. Derecho del centro docente a repetir a los profesores las cantidades satisfechas por dolo o culpa grave en el ejercicio de sus funciones que fueron las causantes del daño. Por su parte, la sentencia de la Audiencia Provincial de Navarra, secc. 1ª, de 12 de noviembre de 2004 (AC 2004,2085) señala que, la delegación de la educación al centro escolar no elimina la labor de educación de los padres.

[135] Vid., la sentencia de la Audiencia Provincial de Asturias, secc. 5ª, de 24 de febrero de 2015 (JUR 2015,947722).

[136] Vid., las sentencias del Tribunal Supremo, Sala de lo Civil, de 10 de diciembre de 1996 (RJ 1996,8975); y, de 4 de junio de 1999 (RJ 199974286).

[137] YZQUIERDO TOLSADA, M. (2015). *Responsabilidad civil extracontractual. Parte General. delimitación y especies. Elementos. Efectos o consecuencias*, *op. cit.,* p. 373. Vid., también, las sentencias de la Audiencia Provincial de Sevilla, secc. 3ª, de 15 de mayo de 2000 (AC 2000,1178) daños sufridos por un menor de cuatro años a causa de las agresiones producidas por otro menor de once años de edad en los servicios del colegio donde ambos estudiaban; de la Audiencia Provincial de Cantabria, de 23 de diciembre de 2003 (JUR 2003,30733); y, de la Audiencia Provincial de Málaga, de 14 de julio de 2010 (JUR 2011,173357).

[138] LA LEY 22174,2019. Asimismo, vid., la sentencia de la Audiencia Provincial de Madrid, secc. 8ª, de 16 de septiembre de 2014 (AC 2015,1056); de la Audiencia Provincial de Barcelona, secc. 11ª, de 1 de marzo de 2017 (AC 2017,607) acoso escolar o ciberbullying; y, de la Audiencia Provincial de Vizcaya, secc. 7ª, de 27 de septiembre de 2019 (AC 2019,1619) fotografía de una menor mientras se hallaba en vestuarios, duchándose tras un parido de futbol. Fotografía tomada por otra menor y difundida por WhatsApp. Responsabilidad del club deportivo que no extremó las medidas para que el móvil no se utilizara en los vestuarios. Por su parte, la sentencia de la Audiencia Provincial de Guipúzcoa, secc. 2ª, de 27 de mayo de 2016 (AC 2016,1329) se condenó conjuntamente a los padres de la menor y al Centro docente al que pertenece la menor ante la inserción en una red social de comentarios vejatorios terriblemente graves. Se acredita una falta de vigilancia de la menor en el uso de las nuevas tecnologías por parte de sus padres, y asimismo, una falta de adopción por el Centro docente de medidas de corrección, prevención y educación exigibles en estos casos.