



Universidad de Valladolid

Facultad de Derecho

Grado en Derecho

MENORES, REDES SOCIALES Y PROTECCIÓN DE DATOS

Presentado por:

Víctor Herreros Carrascal

Tutelado por:

Cristina Guilarte Martín-Calero

Valladolid, 11 de diciembre de 2024

RESUMEN

Las redes sociales son cada vez más utilizadas para la interacción y comunicación, permitiendo compartir información personal públicamente y en privado. Sin embargo, esto conlleva riesgos significativos para los derechos de los menores, preocupando a nivel nacional e internacional. La publicación de datos personales en Internet puede vulnerar derechos como el honor, la intimidad y la propia imagen, siendo más graves cuando afectan a menores. Dada su falta de madurez y su gran uso de estas plataformas, es crucial garantizar una protección especial para su desarrollo personal y derechos fundamentales. Se requiere una protección reforzada donde el interés superior del menor prevalezca sobre otros derechos legítimos. Existen normativas y recomendaciones nacionales e internacionales que buscan proporcionar esta protección. Este trabajo analiza la regulación legal existente, los riesgos a los que se pueden enfrentar y las medidas para poder hacer frente y prevenir esos riesgos.

PALABRAS CLAVE: Interés superior del menor, consentimiento, redes sociales, protección de datos, RGPD

ABSTRACT

Social networks are increasingly used for interaction and communication, allowing personal information to be shared publicly and privately. However, this carries significant risks for children's rights, which are of national and international concern. The publication of personal data on the Internet can violate rights such as honour, privacy and self-image, being more serious when it affects minors. Given their lack of maturity and their extensive use of these platforms, it is crucial to guarantee special protection for their personal development and fundamental rights. Reinforced protection is required where the best interests of the child prevail over other legitimate rights. There are national and international regulations and recommendations that seek to provide this protection. This paper analyses the existing legal regulation, the risks they may face and the measures to address and prevent those risks.

KEY WORDS: Best interests of the child, consent, social networks, data protection, RGPD

ÍNDICE

1. INTRODUCCIÓN	5
2. EVOLUCIÓN DE LA PROTECCIÓN DE DATOS	6
2.1 A nivel internacional	6
2.2 A nivel nacional.....	7
3. REGULACIÓN ESPECÍFICA DE LOS MENORES EN MATERIA DE PROTECCIÓN DE DATOS	9
3.1 Ley COPPA.....	9
3.2 Ámbito comunitario.....	11
3.2.1 Reglamento General de Protección de Datos	11
3.2.2 Grupos de trabajo	12
3.3 Ámbito nacional	14
3.3.1 Patria potestad: Concepto y límites.....	14
3.3.2 Interés superior del menor.....	15
3.3.3 Cuestión del consentimiento: Edad para consentir	17
4. MENORES Y EL USO DE LAS REDES SOCIALES	19
4.1 Origen y concepto de las redes sociales	19
4.2 Uso generalizado de las redes sociales	20
4.3 Derechos de los menores en las redes sociales.....	21
4.3.1 Derechos digitales	21
4.3.2 Derechos ARSULIPO.....	23
4.3.3 Derechos de la personalidad	27
4.3.3.1 Derecho al honor	28
4.3.3.2 Derecho a la intimidad.....	29
4.3.3.3 Derecho a la propia imagen	30
4.3.4 Intromisiones ilegítimas en los derechos del honor, intimidad y propia imagen	31
4.3.5 Medidas para hacer frente a las posibles intromisiones	33
4.4 Riesgos de los menores en las redes sociales	35
5. LOS PROVEEDORES DE SERVICIO EN LINEA	38
5.1. Actuación y responsabilidad	38
5.2. Supuestos que provocan responsabilidad.....	40
5.3 Breve referencia a la Ley de Servicios Digitales	41
6. PAPEL DE LAS AUTORIDADES	42
6.1 Posición del Ministerio Fiscal.....	44
6.2 Labor de los abogados	46

7. MEDIDAS DE PREVENCIÓN DE LOS MENORES DE LOS RIESGOS DE LAS REDES SOCIALES	48
7.1 Medidas educativas.....	48
7.2 Herramientas tecnológicas de control parental.....	49
7.3 Indicaciones para los operadores de servicio en línea	49
8. CONCLUSIONES	51
9. BIBLIOGRAFÍA.....	54

1. INTRODUCCIÓN

En la era digital, el uso de las redes sociales se han convertido en una parte esencial de la vida cotidiana, especialmente para los menores. Estas plataformas ofrecen oportunidades para la comunicación, el aprendizaje y la socialización. Sin embargo, también presentan riesgos significativos en términos de protección de datos y privacidad, como la exposición a contenidos inapropiados o el uso indebido de sus datos personales.

Ante esta realidad, la legislación nacional como internacional, busca equilibrar el derecho de los menores a participar en el entorno digital con la necesidad de garantizar su protección. Instrumentos normativos como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) establecen medidas estrictas sobre el consentimiento y el tratamiento de los datos de menores imponiendo límites claros para salvaguardar sus derechos fundamentales.

El rápido avance de la tecnología y el creciente uso de las redes sociales por menores exigen una constante revisión y adaptación de las normativas. En una sociedad cada vez más globalizada y dependiente de estas plataformas, los menores, desde edades tempranas, interactúan en entornos digitales sin plena conciencia de los riesgos asociados. Por ello, es crucial no solo reforzar el marco jurídico, sino también fomentar la educación digital desde edades tempranas, permitiendo que los menores aprovechen los beneficios de las tecnologías mientras se minimizan los riesgos.

Este trabajo explorará los conceptos básicos de la protección de datos y su aplicación en la interacción de los menores con las tecnologías. Se examinarán los retos actuales en la protección de su privacidad en redes sociales, así como las posibles mejoras necesarias en el marco legislativo y educativo para garantizar una protección efectiva. A través de este análisis, se busca destacar la importancia de combinar la regulación adecuada con la formación digital para preservar la dignidad y los derechos fundamentales de los menores en el entorno digital.

2. EVOLUCIÓN DE LA PROTECCIÓN DE DATOS

2.1 A nivel internacional

En el plano internacional, uno de los primeros indicios sobre este derecho se encuentra en el artículo 12 de la Declaración Universal de Derechos Humanos de 1948, que establece que:

“Nadie será objeto de injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, ni de ataques a su honra o reputación, y que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”¹

Este artículo destaca la importancia de proteger la privacidad y el honor de las personas frente a posibles abusos.

El desarrollo de la tecnología hizo evidente la necesidad de proteger los derechos individuales. Esto es así que, en el año 1968, la Recomendación 509 del Consejo de Europa sobre *"Derechos humanos y los nuevos logros científicos y técnicos"*² marcó un punto de inflexión en la protección de datos en Europa de tal manera que ya se empezó a tomar conciencia de la amenaza que suponía el uso indebido de la tecnología para la privacidad.

Así, en 1981, el Consejo de Europa aprobó el Convenio 108 en Estrasburgo³, que estableció normas básicas para la protección de datos personales, garantizando el respeto de los derechos y libertades de los ciudadanos, especialmente el derecho a la vida privada en relación con el tratamiento de datos personales.

El Convenio permitía que cada Estado firmante estableciera excepciones y restricciones en su legislación interna, siempre y cuando se respetaran los principios y derechos establecidos, principalmente en los casos de protección de la seguridad del Estado, de la persona afectada, y de los derechos y libertades de otras personas. Aunque el convenio no tenía aplicación directa, los Estados debían decidir qué instrumentos o mecanismos establecer para hacer

¹ Artículo 12 de la Declaración Universal de Derechos Humanos de 1948

² Recomendación 509 del Consejo de Europa sobre "Derechos humanos y los nuevos logros científicos y técnicos"

³ Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

efectivo su contenido. A su vez, el Consejo de Europa emitió varias recomendaciones significativas, como la Recomendación R (87) 15 sobre la utilización de datos personales en el sector de la policía⁴ y la Recomendación R (99) 5 sobre la protección de la intimidad en internet⁵.

Paralelamente, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) contribuyó al desarrollo normativo en esta materia, dando fuerza vinculante a sus textos elaborados por expertos gubernamentales. Asimismo, en 1990, la Asamblea General de las Naciones Unidas emitió la Resolución 45/95 sobre los principios rectores para la regulación de los ficheros computarizados de datos personales⁶, que estableció las bases mínimas que cada legislación estatal debería contener al legislar sobre la protección de datos.

La situación jurídica en Europa se armonizó con la Directiva 95/46/CE, que se convirtió en un punto de referencia para la protección de los datos de los ciudadanos. Esta directiva fue derogada por el Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de dichos datos, que entró en vigor en 2018. Este reglamento se complementa con la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como con el Reglamento (UE) 2018/1807 sobre la libre circulación de datos personales en la Unión Europea.

2.2 A nivel nacional

A pesar de que el punto de partida para la protección de datos se encuentra en el artículo 18.4 de la Constitución de 1978, este derecho no aparece específicamente recogido en la Constitución, sino que se trata de un derecho de creación jurisprudencial derivado del mencionado artículo, tal y como nos señala la Sentencia STC 254/1993, de 20 de julio, cuando en el Fundamento sexto habla de *«una nueva garantía constitucional como forma de respuesta a una nueva forma de amenaza a la dignidad y a los derechos de la persona»*⁷.

⁴ Recomendación R (87) 15 sobre la utilización de datos personales en el sector de la policía

⁵ Recomendación R (99) 5 sobre la protección de la intimidad en internet .

⁶ Resolución 45/95 sobre los principios rectores para la regulación de los ficheros computarizados de datos personales

⁷ Sentencia STC 254/1993, de 20 de julio, Fundamento sexto

Esta garantía constitucional, surge para combatir, precisamente, la informática a la que hace referencia el artículo 18.4 de la Constitución cuando establece que será *el legislador quien «limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*⁸ y que ya comenzaba a plantear entre la sociedad del momento la necesidad de protección legal frente a las agresiones que la tecnología podía llegar a cometer frente a la dignidad y la libertad de la persona.

Antes de la promulgación de la sentencia, en 1992, se publicó la Ley Orgánica 5/1992 (LORTAD)⁹, que regulaba el tratamiento automatizado de los datos personales, estableciendo por vez primera, limitaciones al uso de la informática para proteger la intimidad de las personas acorde con el artículo 18 CE. Esta ley marcó el inicio de la protección legal frente a los abusos tecnológicos dado que en ese mismo año se crea la AEPD (Agencia Española de Protección de Datos) aunque su funcionamiento tendrá que esperar hasta el año 1994.

La evolución normativa continuó con la Ley Orgánica 15/1999 (LOPD), que sustituyó a la LORTAD y se basaba en la Directiva 95/46. Reguló el tratamiento de los datos personales y estableció los derechos de las personas y las obligaciones de aquellos que trataban datos, con independencia del medio utilizado y, que, además, fue desarrollada por el Real Decreto 1720/2007¹⁰. Este marco normativo fue completado por diversas sentencias del Tribunal Constitucional, que definieron tanto su contenido como su alcance. Es por ello por lo que cabe destacar la Sentencia 94/1998¹¹ según la cual este derecho garantiza a las personas el control y el uso sobre sus datos personales para evitar un uso ilícito o perjudicial; y la Sentencia del Tribunal Constitucional 292/2000¹² que fue la que declaró que el derecho a la protección de datos es un derecho fundamental independiente, aunque interrelacionado con otros derechos fundamentales.

⁸ Tal y como indica el fundamento jurídico sexto, pone de manifiesto una emergente amenaza que tiene su origen en los posibles usos ilegítimos del tratamiento mecanizado de datos que en definitiva la Constitución engloba como «la informática».

⁹ Ley Orgánica 5/1992 (LORTAD) , que regulaba el tratamiento automatizado de los datos personales

¹⁰ Real Decreto 1720/2007 del 21 de diciembre, que aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999.

¹¹ Sentencia del Tribunal Constitucional 94/1998

¹² Sentencia del Tribunal Constitucional 292/2000

Tras años de cambios legislativos, en el año 2010, la Comisión Europea determinó que la Directiva 95/46 ya no era la adecuada para abordar la globalización y los avances tecnológicos que se estaban experimentando. Por ello la Unión Europea adoptó el Reglamento General de Protección de Datos (RGPD) en 2016, que entró en vigor en 2018, año en el que se derogó la Directiva 95/46/CE. Este reglamento tiene efecto directo y no requiere transposición a las legislaciones nacionales, asegurando una protección uniforme en toda la UE. En España, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales adaptó la normativa nacional al RGPD. Esta ley no solo incorpora las disposiciones del reglamento europeo, sino que también introduce un catálogo de derechos digitales para responder a las necesidades de la sociedad tecnológica actual y futura.

3. REGULACIÓN ESPECÍFICA DE LOS MENORES EN MATERIA DE PROTECCIÓN DE DATOS

3.1 Ley COPPA

Dentro de las normas dedicadas a la protección de datos de los menores de edad, no podemos no mencionar a la Ley COPPA (Children's online privacy) de Estados Unidos puesto que fue el primer país en adoptar una normativa en este ámbito y un modelo a seguir por parte de la legislación europea. Esta normativa fue llevada a cabo por FTC (Federal Trade Commission) y se centra en la protección de los menores de 13 años frente al tratamiento que llevan a cabo los operadores de sitios web dirigidos directamente a menores o a un público en concreto.

El objetivo principal de esta ley es permitir que los padres supervisen la información en línea obtenida por sus hijos. Esta normativa se aplicará a los sitios web y servicios en línea destinados a los menores de 13 años, incluyendo aplicaciones móviles y operadores de sitios web. También se va a aplicar a aquellos sitios web o servicios en línea que recopilan información personal de usuarios de otros sitios o servicios dirigidos a menores. Ejemplos de estos servicios en línea incluyen plataformas de videojuegos, redes sociales como Facebook, Instagram, Twitter y MySpace, tiendas en línea, servicios de publicidad, música y video como Spotify, YouTube o YouTube Kids, servicios de comunicación y mensajería como WhatsApp, y servicios de búsqueda geolocalizada, entre otros.

Asimismo, esta ley establece varias obligaciones para los operadores en relación a la protección de los datos de los niños en Internet. Estas obligaciones incluyen:

1. Publicar una política de privacidad clara y comprensible que describa cómo se utiliza la información obtenida de los niños en línea.
2. Obtener el consentimiento previo y verificable de los padres antes de recopilar información personal en línea de los niños, a menos que haya excepciones limitadas.
3. Permitir a los padres acceder a la información personal de sus hijos, rectificarla o eliminarla.
4. Prohibir condicionar la participación de un niño en una actividad en línea a que proporcionen más información de la necesaria para participar en esa actividad.
5. Mantener la confidencialidad, seguridad e integridad de la información obtenida de los niños, asegurándose de transferirla solo a terceros capaces de mantener la confidencialidad y seguridad.¹³

De esta manera al detallar cada una de estas obligaciones, apenas se deja mucho margen a una interpretación flexible de la normativa establecida.

Dejando a un lado la normativa, cabe destacar un caso significativo que ilustra el impacto de COPPA y ese es el caso de la plataforma YouTube. En 2019, la plataforma fue sancionada por la Federal Trade Commission (FTC) por no haber implementado medidas adecuadas para identificar y proteger el contenido dirigido a menores. Como consecuencia, YouTube tuvo que ajustar sus políticas a partir de enero de 2020, requiriendo a los creadores de contenido que indicaran si su contenido estaba dirigido a niños y limitando la publicación de anuncios personalizados en dichos contenidos. Esta medida tuvo repercusiones globales, incluyendo España, afectando a numerosos creadores de contenido que dependían de ingresos por publicidad ¹⁴

¹³ ANDREU MARTÍNEZ, M.^a B., 2013, *La protección de datos personales de los menores de edad*, Thomson Reuters, Aranzadi.S.A Navarra

¹⁴ Artículo de prensa Redacción Depor a 24 de noviembre de 2019. Obtenido de <https://depor.com/depor-play/tecnologia/la-ley-coppa-en-youtube-que-es-como-afectara-a-los-canales-y-todo-sobre-la-polemica-de-la-nueva-regulacion-estados-unidos-usa-nnda-nnlt-noticia/>

3.2 Ámbito comunitario

3.2.1 Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos (RGPD), adoptado por la Unión Europea, constituye el principal marco legal para la protección de datos personales. En vigor desde el 25 de mayo de 2018, este reglamento derogó la Directiva 95/46/CE de 1995, adaptándose a los avances tecnológicos y a la creciente importancia de la protección de datos en la era digital. Fue diseñado para unificar las leyes de protección de datos en todos los Estados miembros, garantizando un marco coherente y resolviendo la disparidad normativa que dificultaba el flujo de información y generaba inseguridad jurídica.

Es por ello, por lo que su ámbito de aplicación es bastante amplio, pues afecta no solo a las entidades dentro de la UE, sino también a aquellas fuera del territorio que procesan datos de ciudadanos europeos, lo que refuerza su impacto global.

Entre sus principales innovaciones destaca la incorporación del derecho al olvido, que, aunque ya había sido reconocido¹⁵ por la jurisprudencia previa, no tenía regulación alguna a nivel europeo ni nacional. Asimismo, el RGPD introduce el principio de responsabilidad proactiva¹⁶ que obliga a las organizaciones a implementar medidas preventivas destinadas a garantizar el cumplimiento de la normativa.

En relación a los menores, el RGPD es coherente con la Carta Europea de Derechos Fundamentales, puesto que vincula la protección de datos con la dignidad personal. Reconoce la especial vulnerabilidad de los menores y establece medidas específicas para garantizar su protección. Por ejemplo, los menores de 16 años requieren el consentimiento parental para el tratamiento de sus datos personales, aunque se otorga a los Estados miembros la facultad de reducir este límite a un mínimo de 13 años.

En el contexto de las redes sociales y los servicios digitales, el RGPD exige un consentimiento claro y verificable por parte de los padres o tutores y que la información sobre el tratamiento de datos dirigida a los menores sea concisa, transparente, inteligible y de fácil acceso. El

¹⁵ Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014.

¹⁶ Hace referencia a la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento es conforme con el Reglamento

artículo 8¹⁷ del RGPD es especialmente relevante, en este sentido puesto que establece que el consentimiento de un menor solo es válido si tiene al menos 16 años (aunque como hemos visto, los estados miembros pueden rebajar este límite a 13 años) y si es menor, debe ser otorgado o autorizado por quien ejerza la patria potestad o tutela.

Además, el responsable del tratamiento de datos tiene la obligación de verificar la validez del consentimiento otorgado lo cual implica hacer “esfuerzos razonables” utilizando la tecnología disponible. Sin embargo, el reglamento no proporciona mecanismos específicos para cumplir con esta obligación, lo que ha generado desafíos prácticos para las empresas. En comparación normas como la COPPA, ofrecen opciones más concretas para el control parental como enviar un correo electrónico a los padres solicitando el consentimiento o realizar una llamada telefónica para verificar la identidad lo que evidencia un área de mejora en el RGPD.

A pesar de los avances, algunos autores como Macenaite o Kosta¹⁸ han señalado deficiencias en el presente reglamento en relación con la protección de menores argumentando que no se aborda de manera suficiente los riesgos específicos a los que se enfrentan en el ámbito digital debido a la falta de disposiciones específicas. Esta carencia podría disminuir la efectividad de la normativa para proteger a los sujetos más vulnerables lo que ha generado debates sobre la necesidad de un enfoque más claro y específico en el entorno digital.¹⁹

La implementación del RGPD ha supuesto un reto significativo para las organizaciones, que han tenido que revisar políticas de privacidad, formar a su personal, actualizar sistemas de seguridad y aplicar los principios de protección de datos desde el diseño y por defecto. Estos esfuerzos son esenciales no solo para garantizar el cumplimiento normativo, sino también para ofrecer una protección efectiva de los datos personales, en línea con las demandas de la era digital.

3.2.2 Grupos de trabajo

Antes del Reglamento General de Protección de Datos (RGPD), las principales normas europeas sobre protección de datos no contenían disposiciones específicas para proteger a los menores. A pesar de ello, se llevaron a cabo diversos estudios por parte de los diferentes

¹⁷ Reglamento General de la Protección de Datos. Artículo 8

¹⁸ Macenaite, Milda; Kosta, Eleni (2017). “*Consent for processing children’s personal data in the EU: Following in US footsteps?*”. Information & communications technology law, v. 26, n. 2, pp. 146-197. <https://goo.gl/L3nQye> <https://doi.org/10.1080/13600834.2017.1321096>

Estados miembros y autoridades de control correspondientes, para resaltar la importancia de proteger a los menores frente a las nuevas tecnologías. La página web de la Agencia Española De Protección de Datos²⁰ nos habla de una serie de grupos de trabajo: el WP29, un grupo de trabajo comunitario; IWGPDT, un grupo especializado en telecomunicaciones, y el WPSIP, que se centra en la seguridad de la información y privacidad bajo la OCDE.

El Grupo de Trabajo del Artículo 29 formalmente conocido como el “Grupo de Trabajo sobre la Protección de Datos del Artículo 29” (WP29), fue un organismo consultivo creado por la Directiva 95/46/CE que estaba compuesto de las Autoridades de Protección de Datos de los Estados miembros, un Supervisor Europeo de Protección de Datos y la Comisión Europea. Entre sus principales funciones eran la de proporcionar asesoramiento experto sobre la interpretación y aplicación de las diversas normativas de protección de datos en la UE, así como promover la cooperación entre las autoridades nacionales.

Desempeñó un papel importante en el desarrollo y en la ejecución de políticas de protección de datos en Europa, con un énfasis significativo en la salvaguarda de los derechos de los menores en el entorno digital.

Sus recomendaciones y dictámenes se pueden encontrar en la página de la Comisión Europea²¹ pero dos de ellas son especialmente relevantes de cara a la protección de datos de los menores: el Dictamen 2/2009 sobre la protección de datos personales de los niños y el Dictamen 5/2009 sobre las redes sociales.

El primero de ellas, el Dictamen 2/2009²² establece que el principio rector es el interés superior del menor y lo que busca es consolidar la protección de datos de forma estructurada, centrándose en la protección de datos personales en el ámbito escolar aplicando los principios fundamentales.

Sostiene que la protección de los menores debe seguir las normas generales de protección de datos, considerando de igual manera las normas especiales sobre menores y priorizando el interés superior del menor. Tanto la familia como los centros educativos, la sociedad y el

²⁰ Página Agencia Española de Protección de Datos <https://www.aepd.es/>

²¹ Página de la Comisión Europea http://ec.europa.eu/justice/dataprotection/article29/documentation/opinion/recommendation/index_en.htm#maincontentSec15

²² Dictamen 2/2009 sobre la protección de los datos personales de los niños

Estado tienen responsabilidades para garantizar el cumplimiento de estos principios y derechos. en la protección de datos de los menores

Y por otro lado tenemos el Dictamen 5/2009²³ sobre las redes sociales se centra específicamente en cuestiones de privacidad y protección de datos relacionadas con las redes sociales y hace hincapié en la necesidad de obtener un consentimiento informado y específico por parte de los usuarios para el tratamiento de sus datos, así como en la importancia de brindar opciones claras y accesibles de configuración de privacidad.

3.3 Ámbito nacional

En el contexto nacional, la protección de los menores en el entorno digital requiere un equilibrio entre tres elementos fundamentales: la patria potestad, el interés superior del menor y su consentimiento.

Este apartado tiene como objetivo analizar cómo estos conceptos se interrelacionan para asegurar que los derechos de los menores sean respetados y protegidos adecuadamente, garantizando su bienestar y seguridad en el uso de las redes sociales.

3.3.1 Patria potestad: Concepto y límites

La patria potestad según CARLOS LASARTE²⁴ es el conjunto de deberes, facultades y derechos de los padres sobre sus hijos menores. Regulada en el Código Civil, en sus artículos 154 y 162.1, su objetivo es proteger los intereses de los menores. El artículo 154 establece que los padres tienen la responsabilidad de cuidar, educar y proteger a sus hijos menores y que deben tomar las decisiones importantes sobre su bienestar de manera conjunta, siempre buscando lo mejor para ellos. Por su parte, el artículo 162.1 es relevante porque señala que los padres tienen la representación legal de los menores, lo que les otorga la capacidad para tomar decisiones en su nombre. Esto garantiza la protección y cuidado, pero también delimita ciertos ámbitos en los que el menor puede actuar por sí mismo como es el caso de los derechos personalísimos o cuando el menor genera ingresos por su propio trabajo.

Ante el auge de las redes sociales y la tecnología, la patria potestad se ha visto desafiada, especialmente en cuanto a la protección de la privacidad y la seguridad digital de los menores.

²³ Dictamen 5/2009 sobre las redes sociales

²⁴ LASARTE ÁLVAREZ, C.: *Principios de Derecho civil. Derecho de Familia*, Tomo sexto, Decimosexta edición. Ed. Marcial Pons, Madrid 2015 pág. 393

La Ley 26/2015 y modificaciones del Código Civil han impulsado cambios en la manera en que los padres ejercen este derecho, buscando un equilibrio entre su responsabilidad parental y la autonomía progresiva del menor. Autores como AIME ROJAS destacan *“la llegada de las nuevas tecnologías, internet y las redes sociales, y su uso cada vez más extendido, ha llevado a una redefinición del ejercicio de la patria potestad de los padres hacia sus hijos”*²⁵

Hoy en día, los padres o tutores enfrentan importantes desafíos al tratar de proteger a los menores en internet, ya que deben equilibrar la vigilancia necesaria con el respeto a la privacidad de sus hijos. En este sentido, BATUECAS CALETRÍO²⁶ señala que el control parental debe ser ejercido sin anular la personalidad del menor ni convertir la patria potestad en una autoridad absoluta. Con los avances tecnológicos, los padres deben establecer límites adecuados en la supervisión del uso de redes sociales por parte de sus hijos, conforme a lo establecido en los artículos 154 y 162.1 del Código Civil y en la Ley Orgánica de Protección Jurídica del Menor.

Además, es fundamental que el ejercicio de la patria potestad se enfoque en el beneficio del menor sobre el de los padres, siguiendo el enfoque de DÍEZ-PICAZO, y evitando cualquier acción que solo beneficie a los progenitores²⁷. Por eso, los padres o tutores deben tener en cuenta la madurez y el criterio de los menores al tomar decisiones, y que escuchen activamente a sus hijos cuando estos alcancen un nivel de madurez adecuado. El deber parental no solo implica guiar y educar, sino también proteger a los hijos de terceros, lo que justifica las intervenciones en su privacidad cuando se busque su protección o la prevención de posibles peligros.

3.3.2 Interés superior del menor

El interés superior del menor es un principio esencial en la normativa sobre menores que debe guiar las decisiones de los progenitores. Este principio está respaldado por varios instrumentos legales, como la Convención de Naciones Unidas sobre los Derechos del Niño, la Carta de Derechos Fundamentales de la Unión Europea y la Constitución Española. Su

²⁵ AIME ROJAS, M.: *Análisis de un problema deóntico respecto del derecho a la intimidad de los menores de edad y el alcance del ejercicio de la patria potestad en la utilización de internet y las redes sociales*, Revista de derecho privado, núm. 2, 2014, pág. 100

²⁶ BATUECAS CALETRÍO, A.: *El control de los padres sobre el uso que sus hijos hacen de las redes sociales*, en AA.VV. APARICIO VAQUERO, J.P.: *En torno a la privacidad y protección de datos en la sociedad de la información*, Comares, 2015, pág. 137.

²⁷ DÍEZ-PICAZO, L Y PONCE DE LEÓN, L; GUILLÓN BALLESTEROS, A. *Sistema de Derecho Civil*. Volumen I. Edición Tecnos, 1997, pág. 276.

objetivo es fortalecer la protección de los menores, considerando su falta de madurez física y psicológica. No obstante, a pesar de esa falta de madurez, los menores gozan de todos los derechos inherentes a la persona, como establece el Código Civil en sus artículos 29 y 30, que confieren la personalidad desde el nacimiento.

El artículo 2.1 de la Ley Orgánica de Protección Jurídica del Menor (LOPJM) establece que *"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."*²⁸ Sin embargo, pese a estar reconocido, este principio no tiene una definición precisa.

VIRGINIA MÚRTULA LAFUENTE²⁹ ha definido este principio en base a tres aspectos que pasaremos a analizar a continuación.

El primer aspecto es el interés superior del menor como un derecho sustantivo. Los artículos 2.1 y 2.4 de la LOPJM indican que el interés del menor debe prevalecer sobre cualquier otro interés legítimo, tanto en el ámbito público como en el privado. Cuando hay incompatibilidad de intereses, se debe realizar una valoración para encontrar la solución más justa para todos los involucrados. Sin embargo, en caso de incompatibilidad, el interés del menor debe prevalecer absolutamente. Las acciones o decisiones que afecten a los menores deben priorizar su interés, y jueces, tribunales y la Administración tienen la responsabilidad de garantizarlo. Así, el interés superior del menor pasa de ser un principio aplicable a una ley específica (LOPJM) a ser considerado un derecho subjetivo invocable ante los tribunales, al igual que un principio general que guía la interpretación y aplicación de cualquier norma que afecte al menor, sin desvincular al juez del sistema de fuentes establecido.

El segundo aspecto reconoce el interés superior del menor como un principio jurídico fundamental de interpretación. Atendiendo a los apartados b) y c) del artículo 2.2 de la LOPJM, se requiere la interpretación judicial para que este interés sea efectivo. Además, el artículo 2.3 de la LOPJM establece que el interés del menor debe interpretarse junto con los principios de necesidad y proporcionalidad, garantizando de esta manera, que el interés del menor no sea exclusivamente restrictivo, sino que también proteja otros derechos garantizados.

²⁸ Ley Orgánica de Protección Jurídica del Menor (LOPJM) Artículo 2

²⁹ MÚRTULA LAFUENTE, V. (2016). Valoración del interés superior del menor a la hora de adoptar medidas civiles en situaciones de conflicto parental. Madrid: Dykinson.

El tercer aspecto considera el interés superior del menor como una norma de procedimiento, conforme al artículo 2.5 de la LOPJM. Para asegurar su efectividad, se deben respetar ciertas garantías procesales: el derecho del menor a ser informado, escuchado y participar en el proceso según la normativa vigente; la participación de profesionales cualificados o expertos; la participación de progenitores, tutores, representantes legales o un defensor judicial en caso de conflicto, así como del Ministerio Fiscal para defender los intereses del menor; la adopción de decisiones con una motivación clara, especificando los criterios y elementos considerados; y la existencia de recursos que permitan revisar la decisión si no se consideró el interés superior del menor como primordial o si hay cambios significativos en las circunstancias que motivaron la decisión.

3.3.3 Cuestión del consentimiento: Edad para consentir

En cuanto al último de los aspectos relevantes, el consentimiento, debemos saber que el RGPD establece en su considerando 32 “*debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal*”³⁰

De esta manera, el consentimiento para el tratamiento de los datos personales debe cumplir con cuatro requisitos fundamentales: ser libre, específico, informado e inequívoco³¹.

- **Libre:** el consentimiento debe ser otorgado sin ningún vicio o coacción alguna. Esto implica que la persona que da su consentimiento debe hacerlo de manera voluntaria, sin presiones ni amenazas. Si el individuo no o puede ejercer su decisión libremente, ya sea por miedo a consecuencias negativas o por cualquier otro tipo de presión, el consentimiento no es válido.³²
- **Específico:** Cuando los datos se destinan para múltiples fines, el consentimiento debe ser otorgado de manera diferenciada para cada uno de esos fines. No se puede considerar válido un consentimiento genérico para todos los usos de los datos personales.

³⁰ Reglamento General de Protección de Datos, Considerando 32

³¹ AYLLON GARCIA, J.D., en *Consentimiento de los menores de edad en las redes sociales: especial referencia a TikTok*. Pp 587-589

³² Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, del Grupo de Protección de Datos del artículo 29, adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, p. 6

- **Informado:** se exige que el interesado debe ser informado previamente sobre el tratamiento de sus datos de manera clara y comprensible. Las políticas de privacidad deben ser accesibles y redactadas en un lenguaje sencillo para que cualquier persona pueda entenderlas sin dificultad.
- **Inequívoco:** el consentimiento debe ser expresado de manera clara y sin ambigüedades. Debe consistir en una acción afirmativa que refleje la voluntad del interesado como marcar una casilla o hacer clic en un botón lo cual deja claro que la persona ha dado su consentimiento para el tratamiento de sus datos personales.

En materia de menores, la LOPDGDD, en su artículo 7³³, establece que la edad mínima para otorgar consentimiento en el tratamiento de datos personales es de 14 años. Esta normativa se ajusta al marco europeo del RGPD, que permite a los Estados miembros fijar una edad mínima dentro del rango de 13 a 16 años. De acuerdo con el artículo 7.1 de la LOPDGDD, *“el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años”*. Esto implica que, a partir de los 14 años, los menores tienen la capacidad de otorgar un consentimiento informado, siempre que comprendan las implicaciones del tratamiento de sus datos personales, lo cual está basado en la idea de que a esa edad han alcanzado un desarrollo cognitivo y emocional adecuado para tomar decisiones en este ámbito.

Por otro lado, para los menores de 14 años, el artículo 7.2 de la LOPDGDD establece que será necesario el consentimiento de los padres o tutores de modo que cualquier tratamiento de datos personales de menores en plataformas digitales debe contar con autorización expresa de los responsables de la patria potestad, con el fin de proteger la privacidad y seguridad de los menores en el entorno digital.

Esta regulación se fundamenta en la necesidad de proteger a los menores frente a los riesgos asociados al uso de las redes sociales que se detallarán más adelante. Asimismo, la normativa también refuerza la responsabilidad de las plataformas digitales de implementar mecanismos efectivos para verificar la edad de los usuarios y obtener el consentimiento parental en los casos que sea necesario.

³³ Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) Artículo 7

En este sentido, la Agencia de Protección de Datos ha emitido varios informes como el informe 466/2004³⁴, en el que se establece límites a la edad de consentimiento especialmente cuando el tratamiento de datos pueda tener implicaciones patrimoniales para el menor. Además la jurisprudencia ha abordado situaciones relacionadas con la falta de consentimiento como se evidencia en el caso de la Resolución 1663/2010³⁵, que versa sobre un procedimiento contra una Página Web dirigida a jóvenes y adolescentes que no verificaba adecuadamente la edad de los usuarios permitiendo que personas menores de edad accedieran sin el consentimiento de los padres o tutores.

4. MENORES Y EL USO DE LAS REDES SOCIALES

4.1 Origen y concepto de las redes sociales

Las Redes Sociales aparecen entorno a los años 90 cuando comenzaron a surgir las primeras plataformas en Internet que objetivo principal era facilitar el contacto entre personas que se conocieron en la universidad o colegio. En esta década, surgieron algunas como Geocities, Classmates O SixDegrees³⁶ siendo esta última diseñada para conectar en contacto a amigos, mediante un sistema que agrupaba a los usuarios en función del grado de relación que tuvieran, para que interactuaran a través de mensajes Sin embargo, no tuvieron mucha popularidad y fue a partir de comienzos 2000 donde se produce un significativo auge, alcanzando el “boom” en el año 2008. Desde entonces, se ha observado un aumento considerable en su uso.

Aunque el objetivo fundamental de las redes sociales sigue siendo la interacción y el contacto entre usuarios, su uso ha evolucionado y se ha consolidado como un canal primordial para la publicidad de marcas y empresas, entre otros usos. En términos generales, podemos definir red social como una plataforma en la que los usuarios crean perfiles donde comparten sus gustos, preferencias e ideologías, y pueden conectarse con otros usuarios que comparten intereses similares y agregarlos como "amigos".

³⁴ Informe 466/2004 sobre la comunicación a los padres de las calificaciones de sus hijos menores de edad.

³⁵ Resolución 1663/2010

³⁶ La primera Red Social que se creó fue “SixDregrees” su creador fue Andrew Weinreich

Para profundizar en la definición de red social, el profesor FÉLIX REQUENA entiende que son “un conjunto de puntos (actores sociales) vinculados por una serie de relaciones que cumplen determinadas propiedades. Las redes sociales gozan de una estructura y una morfología propias, cuyas cualidades, como la posibilidad de cuantificar las relaciones y su consiguiente tratamiento matemático, evidencian importantes aplicaciones para el análisis e interpretación de las conductas sociales”³⁷

Además, resulta relevante mencionar una definición más actual y es la que proporcionada por el Grupo de Trabajo del Artículo 29. Este grupo de trabajo en su dictamen 5/2009³⁸, en su apartado segundo la define como una plataforma online que permite a las personas unirse a redes predefinidas o crear nuevas redes con usuarios que comparten intereses similares.

4.2 Uso generalizado de las redes sociales

El uso de dispositivos electrónicos como ordenadores, tablets, móviles en estos últimos años ha experimentado un gran aumento lo que ha llevado un incremento en las formas de interactuar y conectarse con otras personas, principalmente a través de las redes sociales. Asimismo, en estas plataformas confluyen un gran número de personas – denominadas usuarios- concretamente, se estiman que alrededor del 5.610 millones de personas en todo el mundo son usuarios activos de las redes sociales a principios del año 2024 lo que representa aproximadamente el 69,4% para de la población mundial.³⁹ Así que para tener en cuenta la dimensión de la que estamos tratando vamos a ver el número de usuarios de algunas de las redes sociales más destacadas como es el caso de Instagram en la que los usuarios se han incrementado a lo largo de los años hasta el año 2022 donde la cifra de usuarios activos eran de 2000 millones en los que los menores representaban el 8,5%⁴⁰. O en el caso de TikTok que el porcentaje de usuarios a nivel global de menores de 18 años es del 28% por lo que estaríamos hablando de unos 22,15 millones de usuarios⁴¹. Estos datos nos ponen de relieve

³⁷ REQUENA, FÉLIX. (1989). «*El concepto de red social*» Reis, vol. 48, pp. 137-152

³⁸ Opinion 5/2009 on online social networking, de 12 de junio de 2009, del Grupo de Trabajo del Artículo 29: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion/recommendation/files/2009/wp163_en.pdf

³⁹ El informe sobre las tendencias digitales, redes sociales y mobile [Digital Report 2024: El informe sobre las tendencias digitales, redes sociales y mobile. - We Are Social Spain](https://wearesocial.com/es/blog/2024/01/digital-2024/) <https://wearesocial.com/es/blog/2024/01/digital-2024/>

⁴⁰ [vTutor Blog | Demografía de Instagram en 2022: las estadísticas más importantes - vTutor Blog](#)

⁴¹ Informe sobre el uso de las redes sociales en España [IX-INFORME-RRSS-THESMF.pdf \(thesocialmediafamily.com\)](#)

de que en los últimos años los menores tienen acceso a las redes sociales cada vez a una edad más temprana, frecuentemente antes de los 14 años

En España, los menores de 16 años, especialmente aquellos de 10 a 15 años, se han convertido en grandes usuarios de dispositivos con acceso a Internet debido al uso de móviles, ordenadores y tablets, lo que ha llevado a desarrollar gran parte de sus vidas en el entorno digital. El uso de redes sociales, aplicaciones y plataformas es común entre ellos, y esta tendencia se ha visto reforzada durante la pandemia ya que el 95% de los menores utiliza ordenadores y el 98% accede a Internet y es que el uso al mismo es prácticamente universal entre los menores siendo más frecuente en los mayores⁴²

Estas plataformas digitales permiten a los usuarios conectarse, comunicarse y compartir información con otros usuarios de todo el mundo. Con la llegada de las redes sociales, la forma en que nos comunicamos ha cambiado drásticamente. Ahora, podemos mantenernos en contacto con amigos y familiares, incluso si están en diferentes partes del mundo. Al mismo tiempo, las redes sociales han abierto nuevas oportunidades para establecer conexiones con personas que comparten nuestros intereses y pasiones incluso se han convertido en una poderosa herramienta para difundir información y concienciar sobre diversos temas por lo que, de esta manera, los usuarios pueden compartir noticias, artículos o videos.

4.3 Derechos de los menores en las redes sociales

4.3.1 Derechos digitales

Como se ha expuesto, el nuevo marco normativo a nivel nacional en materia de protección de datos es la LOPDGDD. Esta ley, a diferencia de su predecesora, introduce un matiz importante: la garantía de los derechos digitales. Esta mención no es solo un cambio de nombre, sino que, en el TÍTULO X de la ley, se regulan específicamente los derechos digitales.

Aunque no existe una definición única y oficial de los derechos digitales, podemos entenderlos como aquellos derechos reconocidos por diversos instrumentos jurídicos

⁴² El uso de la tecnología por los menores

<https://www.ontsi.es/sites/ontsi/files/202202/usotecnologiamenoresespa%C3%B1a2022.pdf>

nacionales e internacionales que se aplican en el entorno digital. Estos derechos abarcan, entre otros, el acceso, uso, creación y publicación de contenidos digitales, así como el acceso a dispositivos electrónicos.

El TÍTULO X de la LOPDGDD⁴³ está compuesto por una serie de preceptos normativos, desde el artículo 79 hasta el artículo 97, que desarrollan y concretan estos derechos. En este contexto, nos centraremos principalmente en los artículos que hacen referencia a los menores⁴⁴.

El derecho a la educación digital, regulado en el artículo 83 de la LOPDGDD, amplía el derecho a la educación reconocido en la Constitución española, orientándose a la integración plena del alumnado en la sociedad digital. Su objetivo es garantizar un uso seguro, responsable y respetuoso de Internet, promoviendo que los estudiantes desarrollen competencias digitales esenciales para desenvolverse de forma autónoma y consciente en el entorno digital. Para ello, se exige la inclusión de asignaturas sobre competencias digitales en todas las etapas educativas, acompañada de una formación adecuada del profesorado.

El artículo 84 regula la protección de los menores en el ámbito digital, regulada en el artículo 84 de la LOPDGDD, asigna a los padres, tutores y representantes legales la responsabilidad de promover un uso equilibrado y responsable de los dispositivos digitales, garantizando el adecuado desarrollo de la personalidad del menor, así como la preservación de su dignidad y derechos fundamentales. Además si la difusión de imágenes en redes sociales u otras plataformas vulneran los derechos fundamentales del menor, el Ministerio Fiscal interviene adoptando medidas de protección conforme a la Ley Orgánica de Protección Jurídica del Menor.

El artículo 92 regula la protección de los datos personales de los menores en Internet, estableciendo que tanto los centros como otras entidades educativas deben garantizar el interés superior del menor en cualquier publicación de datos personales. Esta obligación no se limita a los menores de 14 años, sino que se extiende hasta que alcanzan la mayoría de edad. Asimismo, cuando los datos se publiquen en redes sociales o servicios similares, será

⁴³ Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) Título X.

⁴⁴ BARRIO ANDRÉS M, “*Los derechos digitales y su regulación en España, la Unión Europea e Iberoamérica*” (Cuaderno 1) (Colex, 2023), p. 48-49

obligatorio contar con el consentimiento del menor o de sus representantes legales, conforme al artículo 7 de la misma ley.

Y para finalizar, el artículo 97 establece una serie de medidas orientadas a garantizar e impulsar los derechos digitales, con un enfoque particular hacia los menores y colectivos vulnerables. Para ello, dispone que el Gobierno, en colaboración con las comunidades autónomas, debe elaborar un Plan de Acceso a Internet con el objetivo de reducir las brechas digitales y garantizar el acceso equitativo a Internet. Además, se menciona que se fomentarán programas educativos para impulsar el desarrollo de competencias digitales básicas en colectivos en riesgo de exclusión digital, con el fin de promover un uso autónomo, seguro y responsable de las tecnologías. Para asegurar la eficacia de estas medidas, el Gobierno se compromete a presentar un informe anual ante el Congreso de los Diputados, en el que se detallarán los avances en la implementación de estos derechos digitales y de las medidas adoptadas para su promoción y protección.

4.3.2 Derechos ARSULIPO

Para situar el contexto de este punto, es fundamental entender que los derechos ARSULIPO, surgieron inicialmente bajo la denominación de derechos ARCO en la Ley Orgánica 15/1999⁴⁵, de Protección de Datos de Carácter Personal (LOPD). Estos derechos fueron desarrollados y ampliados en la Ley 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)⁴⁶ así como en el Reglamento General de Protección de Datos (RGPD)⁴⁷.

La normativa vigente permite a los interesados ejercer ante el responsable del tratamiento de datos⁴⁸ los siguientes derechos: acceso, rectificación, oposición, supresión (conocido como "derecho al olvido"), limitación del tratamiento, portabilidad de los datos y el derecho a no ser objeto de decisiones individualizadas automatizadas. Conocidos bajo el acrónimo

⁴⁵ Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), publicada en el BOE núm.298, de 14/12/1999.

⁴⁶ Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) publicada en el BOE núm.294 de 6 de diciembre de 2018, Referencia: BOE-A-2018-16673.

⁴⁷ Reglamento General de Protección de Datos (RGPD), de 25 de mayo de 2018

⁴⁸ Es la persona física o jurídica, autoridad o servicio que se encarga de prestar un servicio al responsable que en este caso es el tratamiento de datos personales.

ARSULIPO,⁴⁹ aparecen recogidos en el título III de la LOPDGDD que refleja la evolución y expansión de las protecciones ofrecidas a los individuos en materia de protección de datos, reforzando las disposiciones del RGPD y adaptándolas al ordenamiento jurídico nacional.

- **Derecho de Acceso:**

El derecho de acceso, regulado en el artículo 13⁵⁰ de la LO 3/2018 y en el artículo 15 del Reglamento (UE) 2016/679 permite a las personas saber si sus datos están siendo tratados y con qué finalidad. Asimismo, incluye información sobre las categorías de datos personales involucrados, los destinatarios o categorías de destinatarios que tienen acceso a ellos, si se transfieren a terceros países o a organizaciones internacionales, el plazo previsto de conservación, el origen de los datos, y la existencia de decisiones automatizadas, incluidas las basadas en perfiles, junto con sus implicaciones.

El artículo 15 del RGPD⁵¹ establecen que el derecho de acceso garantiza que los interesados puedan obtener esta información de manera clara y comprensible y se entenderá otorgado si el responsable facilita un sistema de acceso remoto, directo y seguro a los datos personales, garantizando su disponibilidad de manera permanente. Sin embargo, su ejercicio puede ser limitado en circunstancias específicas como la seguridad pública o el desarrollo de procedimientos judiciales

- **Derecho de Rectificación:**

Este derecho permite a los usuarios solicitar la modificación de datos personales inexactos o desactualizados que les conciernen para que se utilicen correctamente⁵². Resulta especialmente relevante cuando la información errónea puede perjudicar la reputación, intereses legítimos o derechos fundamentales del individuo.

⁴⁹ COBOS, P. S. (2007). Cap. III “*Los derechos del interesado*”. Buenas prácticas en protección de datos. Fundación Dintel.

⁵⁰ Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) publicada en el BOE núm.294 de 6 de diciembre de 2018, Referencia: BOE-A-2018-16673.

⁵¹ Reglamento General de Protección de Datos (RGPD), de 25 de mayo de 2018

⁵² RODRÍGUEZ AYUSO, J.F, “*Garantía Administrativa de los derechos del interesado en materia de protección de datos personales*”, , Bosch Editor, capítulo primero, pág.58.

La rectificación debe llevarse a cabo en un plazo de un mes y puede ser solicitada por el interesado, sus representantes legales o herederos.

- **Derecho de Cancelación:**

Conocido como derecho de supresión con la normativa actual, este derecho permite al interesado solicitar la eliminación permanente de sus datos personales cuando sean inadecuados o excesivos, o ya no sean necesarios para los fines para los que fueron previstos. Este derecho complementa al de rectificación y es esencial para garantizar que los datos personales no se conserven de manera innecesaria protegiendo así la privacidad y los derechos fundamentales del individuo.

- **Derecho de Oposición:**

Reflejado en el artículo 18 de la LOPDGDD y en los artículos 21 y 22 del RGPD, este derecho permite al interesado oponerse en cualquier momento al tratamiento de sus datos personales por motivos de intereses legítimos del responsable o de un tercero en el ejercicio de los poderes públicos⁵³ El RGPD amplía este derecho para incluir la posibilidad de que el usuario exija que sus datos no sean tratados de manera individualizada o automatizada.

Estos cuatro derechos son lo que anteriormente se conocía como los derechos ARCO originales. Sin embargo, en la actualidad, el número de derechos incluidos en la protección de datos ha aumentado significativamente debido a las novedades introducidas por el RGPD, tanto en términos de derechos como en su ejercicio

- **Derecho de Supresión, (“Derecho al olvido”):**

El derecho al olvido es un mecanismo que permite a las personas proteger su privacidad y controlar el uso de sus datos personales en el entorno digital. Está reconocido en el artículo 17 del Reglamento General de Protección de Datos (RGPD) y en el artículo 15 de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) que adapta el RGPD al marco jurídico español.

⁵³ Sobre el interés legítimo como base jurídica para el tratamiento de datos, puede verse el Considerando 47, que pone como ejemplo la existencia de una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable.

Aunque está relacionado con los derechos de cancelación y oposición, el derecho al olvido tiene un carácter más amplio y autónomo. A diferencia de los anteriores, no depende exclusivamente del consentimiento del titular y puede ejercerse sobre información publicada por terceros, siempre y cuando se respeten los límites⁵⁴. Además, su ejercicio no implica necesariamente la eliminación completa de los datos, sino que puede limitarse a la suspensión de su tratamiento o la restricción de su visibilidad pública. De este modo se refuerza, control de los interesados sobre su información, permitiéndoles revocar el consentimiento previamente otorgado y, si lo desean, solicitar la eliminación permanente de sus datos⁵⁵.

En España, este derecho puede ejercerse ante el responsable o el Encargado del tratamiento de datos, o ante la Agencia Española de Protección de Datos (AEPD) si la respuesta no es satisfactoria. Las solicitudes deben ser atendidas en un plazo de un mes, ampliable a dos meses.

Sin embargo, este derecho va a tener limitaciones⁵⁶. No se va a aplicar cuando los datos sean necesarios para garantizar el interés público, la investigación científica o histórica, o la libertad de expresión e información.

- **Derecho de Portabilidad:**

El derecho de portabilidad, regulado en el artículo 20 del RGPD, permite a los interesados recibir los datos personales que han proporcionado a un responsable del tratamiento⁵⁷ y transmitirlos a otro responsable sin que haya impedimento alguno, facilitando esos datos en un formato estructurado, de uso común y lectura mecánica⁵⁸. Este derecho se puede ejercer siempre que el interesado haya prestado su consentimiento y el tratamiento sea necesario para la ejecución de un contrato, además de haberse realizado un tratamiento automatizado de los datos.

⁵⁴ PLATERO ALCÓN, A., “El derecho al olvido en Internet. El fenómeno de los motores de búsqueda” Opinión Jurídica, núm. 29, enero-junio 2016, pág. 249. Disponible en <http://www.redalyc.org:9081/home.oa?cid=2118986>.

⁵⁵ MATE SATUÉ L.C. (2016) *¿Qué es el derecho al olvido?*, Revista de Derecho civil (ISSN 2341-2216, vol3, n°2), págs. 187-222.

⁵⁶ AEPD, (12/07/2023) “Derecho de supresión (“al olvido””, <https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido>

⁵⁷ Es la persona de decidir sobre el tratamiento de datos personales de los individuos.

⁵⁸ RODRÍGUEZ AYUSO, J.F., “*Garantía Administrativa de los derechos del interesado en materia de protección de datos personales*”, Bosch Editor, capítulo primero, pág. 148.

Existen limitaciones para el ejercicio de este derecho, especialmente en relación con los datos personales especialmente protegidos, como los relativos a la salud o el origen étnico que cuentan con tratamiento especial reflejado en el RGPD⁵⁹.

Asimismo, hay excepciones al ejercicio del derecho, como por ejemplo cuando los datos no son proporcionados por el interesado o se refieren a terceros. Para garantizar el cumplimiento, la AEPD tiene la potestad de imponer sanciones en caso de incumplimiento

- **Derecho a la Limitación del tratamiento**

Este derecho, también es una de las últimas incorporaciones y está incluido en el artículo 16 de la LOPDGDD y en el artículo 18 del RGPD, y permite a los interesados limitar el procesamiento de sus datos en aquellos casos en los que los interesados se cuestionan la validez de la información o la legalidad del procesamiento, o, incluso, desean que los datos sean eliminados pero la organización tiene la obligación legal de conservarlos⁶⁰.

No se trata de un derecho absoluto, y los interesados van a poder solicitar la limitación de sus datos en dos casos, como cuando impugnan la exactitud de los datos hasta que se resuelva o cuando se oponen al borrado de datos que han sido procesados ilegalmente.

Las solicitudes de limitación deben ser atendidas en un plazo máximo de un mes, ampliable a dos meses en casos complejos o si una persona presenta varias solicitudes.

4.3.3 Derechos de la personalidad

Los derechos de la personalidad son fundamentales dentro del derecho, ya que protegen aspectos esenciales de la identidad y dignidad humana. Se trata, por tanto, de derechos inherentes a todo ser humano desde su nacimiento, directamente vinculados a su existencia y a su integridad.

Según las directrices de BONILLA SÁNCHEZ⁶¹, estos derechos se caracterizan por ser irrenunciables e intransferibles, pues están estrechamente ligados a la persona lo que significa que no pueden ser cedidos ni renunciados. En línea con el artículo 1.3 de la Ley Orgánica

⁵⁹ Reglamento General de Protección de Datos (RGPD), de 25 de mayo de 2018, Art 23.

⁶⁰ RODRÍGUEZ AYUSO, J.F, “*Garantía Administrativa de los derechos del interesado en materia de protección de datos personales*”, Bosch Editor, capítulo primero, pág. 145.

⁶¹ BONILLA SÁNCHEZ, J.J.: “*Personas y derechos de la personalidad*”, Ed. Reus, Madrid, 2010, pp 32-35

1/1982, estos derechos son personalísimos, es decir, le pertenecen únicamente al individuo y desaparecen con su muerte. A su vez, se caracterizan por ser derecho absolutos y erga omnes, lo que implica que son oponibles frente a cualquier tercero, ya sea una persona privada o una entidad pública. Esto otorga al titular la facultad de ejercerlos frente a cualquier intrusión ilegítima en su esfera personal.

A continuación, abordaremos el estudio del derecho al honor, a la intimidad personal y a la propia imagen, derechos reconocidos en el artículo 18.1 de la CE que establece que “*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*” y cuya regulación se desarrolla de manera detallada en la Ley Orgánica 1/1982.

4.3.3.1 Derecho al honor

A lo largo de la historia, el honor ha sido objeto de protección, siendo reconocido legalmente en numerosas normativas, pero con diferentes interpretaciones. Ejemplo de ello nos lo encontramos con el derecho romano que entre sus preceptos ya se recogía la protección del honor o en normativas españolas anteriores a la Constitución de 1978 en las que ya se protegía la dignidad de la persona a través de los tribunales del honor.

A nivel internacional podemos mencionar tanto la Declaración Universal de los Derechos Humanos de 1948⁶² que recogía el derecho al honor como fama o renombre como la Convención Internacional sobre los Derechos del Niño de 1989 vinculaba el honor con la dignidad humana.

Sin embargo, en contraposición con las anteriores, el Convenio Europeo de Derechos Humanos (CEDH) no menciona explícitamente el derecho al honor, sino que simplemente protege la reputación de las personas en su artículo 10.2⁶³, limitando la libertad de expresión para salvaguardar la reputación ajena.

A día de hoy, la Real Academia Española define el honor como “*la gloria o reputación que sigue a la virtud, al mérito o a las acciones heroicas, la cual trasciende a las familias, personas y acciones mismas de quien se la granjea*”⁶⁴

A pesar de ello, ningún texto legal da una definición precisa acerca de este derecho personal, ni si quiera la propia LO 1/1982, dado que se trata de un derecho tan impreciso y a la vez

⁶² Declaración Universal de los Derechos Humanos de 1948

⁶³ Convenio Europeo de Derechos Humanos (CEDH) Artículo 10.2

⁶⁴ Definición de la Real Academia Española (RAE)

tan amplio que no se puede definir con exactitud todos los puntos que alcanza. Esto ha provocado que la definición jurídica del honor haya sido desarrollada por la jurisprudencia.

Fue la STC 49/2001 de 26 de febrero, (Rec. 881/1997)⁶⁵ la que definió el derecho al honor como *aquel que protege la buena reputación de una persona frente a intromisiones ilegítimas que puedan menoscabar su consideración social*. Del mismo modo, la STC 9/2007, de 15 de enero (Rec. 5586/2004)⁶⁶, en su Fundamento Jurídico Tercero, señaló que *“este derecho al honor se declara como honra, siendo parte de la moral de la persona y actuando directamente en la reputación del mismo, vista esta como la opinión o estima que tiene la sociedad frente a él como individuo.”*

Conforme ha transcurrido el tiempo, este derecho ha evolucionado y se ha adaptado a los cambios sociales y tecnológicos. Inicialmente, se centraba en proteger la dignidad y reputación en contextos más tradicionales, pero con la aparición de las TICS ha experimentado un aumento significativo en las formas en las que puede ser vulnerado por lo que se ha extendido el concepto de este derecho para poder incluir la protección contra difamaciones y ataques en plataformas digitales. Un ejemplo de ello, lo encontramos en la sentencia anteriormente mencionada, la STC 9/2007 que amplió el concepto de honor para incluir el "prestigio profesional" y la reputación en el entorno escolar y social, subrayando la importancia de proteger la percepción social de los menores

4.3.3.2 Derecho a la intimidad

El derecho a la intimidad surge de la necesidad de proteger el ámbito personal de cada individuo manteniéndolo ajeno a los demás sujetos. Esto es así, que caben destacar dos momentos, que según LUIS GARCÍA SAN MIGUEL⁶⁷, marcaron un antes y un después en la consideración de este derecho. El primero de ellos fue un artículo publicado en 1890 por juristas estadounidenses Warren y Brandeis, que se titulaba *"The right to privacy"*, en el que se discutía acerca de la intimidad y se examinaban las formas más comunes de intrusión en la privacidad sentando las bases para comprender qué es la intimidad marcándolo como algo constitucionalmente protegible lo que permitiría frenar todo tipo de irrupciones que se diesen tanto en la vida privada como familiar por parte de terceros.

⁶⁵ STC 49/2001 de 26 de febrero, (Rec. 881/1997)

⁶⁶ STC 9/2007, de 15 de enero (Rec. 5586/2004) , Fundamento Jurídico Tercero,

⁶⁷ GARCÍA SAN MIGUEL, L., *“Estudio sobre el derecho a la intimidad”*, Techos, Madrid, 1992, p.15

El segundo momento importante fue la sentencia del Tribunal Supremo de Estados Unidos en el caso de Nueva York versus Sullivan en 1964, que sentó las bases para la regulación de la difamación y que tuvo una influencia en la jurisprudencia de otros países occidentales

El concepto de intimidad sufre la misma circunstancia que el derecho al honor, al no contar con una definición específica dentro de la Ley. Esto obliga a derivar su interpretación a las valoraciones hechas por la jurisprudencia, la cual ha ido marcando este concepto con el paso de las décadas.

Así que, ante la ausencia de definición, el Tribunal Supremo ha declarado que “*la delimitación de la esfera de la intimidad es eminentemente relativa y ha de ser el juzgador quien, en referencia a cada persona y atento a las circunstancias del caso, prudencialmente delimite el ámbito de la protección*”⁶⁸. Asimismo, la STC 196/2004, de 15 de noviembre (Rec. 1322/2000)⁶⁹, fue la que marcó que este derecho otorgaba a su titular la posibilidad de evitar que terceros o poderes públicos vulneraran este mismo derecho fundamental, dando así una facultad negativa

Con el surgimiento de las nuevas tecnologías, este derecho no solo incluye la capacidad de decidir, sino que también regula la no divulgación aquellos aspectos más íntimos de la persona y el derecho al anonimato en Internet. Esto implica que no se deben revelar datos personales ni imágenes sin el consentimiento del afectado, ni para otras actividades que no hayan sido autorizadas.⁷⁰

4.3.3.3 Derecho a la propia imagen

La protección de la imagen personal ha sido un tema de relevancia en la legislación debido a su estrecha relación con la identidad y la dignidad del individuo. Autores como GITRAMA define este derecho como “un derecho innato de la persona, que se concreta en la reproducción o representación de la figura de ésta, en forma visible y reconocible. Es un derecho subjetivo de carácter privado y absoluto, un derecho personalísimo, pero dotado de un contenido potencialmente patrimonial. Es un derecho inalienable e irrenunciable y en general inexpropiable, en fin, es un derecho imprescriptible”.⁷¹

⁶⁸ STS de 4 de noviembre de 1986. Fundamento Jurídico 7º

⁶⁹ STC 196/2004, de 15 de noviembre (Rec. 1322/2000)

⁷⁰ DE URANO CASTRILLÓN, EDUARDO, “*Derechos de la personalidad en Internet*”, Revista Aranzadi Doctrinal, núm. 9/2010, Aranzadi, Pamplona, 2010.

⁷¹ GITRAMA GONZALEZ, M., “*Voz “imagen, (derecho a la propia)”*”, Nueva enciclopedia jurídica. Tomo XI”, Barcelona, 1967, p.326

Pero al igual que en los casos anteriores, la jurisprudencia ha contribuido de manera significativa a la definición y protección de este derecho. La Sentencia del Tribunal Supremo de 24 de julio de 2012 establece en su fundamento jurídico sexto que este derecho es *“un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos y personales que pueden tener difusión pública y a impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad -informativa, comercial, científica, cultural, etc., perseguida por quien la capta o la difunde”*⁷²

Este derecho ha experimentado un notable desarrollo dada la presencia de los medios de comunicación que permiten la captura de fotografías y videos de individuos. Con el auge de las redes sociales, la imagen adquiere una dimensión dual: por un lado, personal y espiritual, y por otro, patrimonial y económica. En este contexto surgen dos problemáticas relevantes. La primera radica en la divulgación de imágenes de terceros sin su autorización, mientras que la segunda involucra el uso de estas imágenes fuera del ámbito de la red social, sin consentimiento y sin conocimiento por parte de la persona afectada.

El propósito de este derecho es establecer los límites legítimos para la obtención y explotación de la imagen de las personas, protegiendo las reproducciones que permitan su reconocimiento a través de sus características identificativas únicas.

4.3.4 Intromisiones ilegítimas en los derechos del honor, intimidad y propia imagen

La Ley Orgánica 1/1982, regula en los artículos 7 y 8 qué actos constituyen intromisiones ilegítimas así como en los casos en los que dichas intromisiones pueden considerarse justificadas respecto en los derechos al honor, a la intimidad personal y a la propia imagen respectivamente.

Dentro del artículo 7⁷³ nos encontramos con una serie de conductas que dan lugar a una intromisión ilegítima no consentida por el titular del derecho.

La primera de ellas consiste en establecimiento en cualquier lugar de dispositivos de escucha, filmación, aparatos ópticos u otros medios que sean capaces de grabar o reproducir la vida privada de las personas.

⁷² Sentencia del Tribunal Supremo de 24 de julio de 2012

⁷³ 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. Artículo 7

La segunda hace referencia al uso de dispositivos de escucha, ópticos u otros medios que permitan acceder a la vida íntima de las personas, así como la grabación, registro o reproducción de manifestaciones privadas o cartas que no estén destinadas a quien los utiliza.

En tercer lugar, nos encontramos con la divulgación de hechos relacionados con la vida privada de una persona o su familia que puedan afectar a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos de carácter íntimo.

La cuarta consiste en la revelación de información privada de una persona o su familia obtenida a través de su actividad profesional u oficial por parte del que la revela.

La quinta de ellas hace referencia a la captura, reproducción o difusión por medio de fotografía, vídeo u otro procedimiento de la imagen de una persona en lugares o momentos de su vida privada, excepto en los casos permitidos según el artículo octavo, apartado segundo.

En sexto lugar, el uso del nombre, voz o imagen de una persona con fines publicitarios, comerciales o similares.

Y en último lugar la difusión de expresiones o hechos que puedan difamar a una persona o menoscabar su reputación ante terceros.

Una vez expuestos los actos, vamos a exponer qué conductas se consideran intromisiones ilegítimas dentro de cada derecho personal.

Dentro del ámbito del derecho al honor, se consideran intromisiones ilegítimas:

- Divulgar hechos sobre la vida privada de un menor o su familia que dañen su imagen y estatus.
- Realizar acciones o expresiones que menoscaben la dignidad de una persona.

El Tribunal Supremo sostiene que una intromisión en el derecho al honor se configura cuando una expresión difamatoria se difunde y afecta negativamente a la percepción pública de la persona afectada.⁷⁴

En cuanto a la intimidad personal y familiar, se consideran intromisiones ilegítimas:

⁷⁴ NAVIDAD CONTRERAS, SALVADOR (2012). La Protección del Honor, la Intimidad y la Propia Imagen en Internet, Pamplona Thomson Reuters, Aranzadi, p.95.

- Utilizar dispositivos para grabar o captar momentos de la vida privada de los usuarios sin su consentimiento.
- Revelar datos privados conocidos por la actividad profesional u oficial de quien los divulga.

Respecto al derecho a la propia imagen, son intromisiones ilegítimas:

- Captar, reproducir o publicar la imagen de una persona en lugares o momentos privados sin su autorización.
- Utilizar el nombre, voz o imagen de una persona con fines publicitarios, comerciales o similares.

Siguiendo en este contexto, la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial⁷⁵ cobra especial relevancia, ya que aborda las nuevas formas de intromisión derivadas de los avances tecnológicos. Herramientas de inteligencia artificial como los “*deepfakes*” permiten generar simulaciones hiperrealistas de imágenes y voces, que pueden emplearse para crear contenidos manipulados, con apariencia real, sin el consentimiento de las personas afectadas.

Al mismo tiempo, la proposición amplía los mecanismos de protección previstos en la Ley Orgánica 1/1982, reforzando la necesidad de un consentimiento explícito para el uso de la imagen o la voz generada mediante inteligencia artificial. Diferencia también entre los usos ilícitos y aquellos amparados por un interés histórico, científico o cultural relevante, en línea con el artículo 8 de la Ley Orgánica 1/1982 que establece qué determinadas conductas no serán consideradas ilegítimas.

4.3.5 Medidas para hacer frente a las posibles intromisiones

La protección de los derechos de la personalidad es esencial en un contexto donde las intromisiones ilegítimas son cada vez más comunes, especialmente a través de internet y las redes sociales. Así, para garantizar esta protección, el marco normativo español ofrece herramientas específicas, orientadas a la salvaguarda de los menores, un colectivo particularmente vulnerable en el entorno digital.

⁷⁵ Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial

La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE) incluye diversos mecanismos para asegurar la defensa de estos derechos. Según el artículo 30 de la LSSICE, se pueden iniciar una acción de cesación contra conductas que lesionen intereses colectivos o difusos, permitiendo la intervención de:

1. Los representantes legales del menor.
2. Instituciones públicas o privadas dedicadas a la protección del menor.
3. Asociaciones relacionadas con la protección de menores.

Además, el artículo 41 de la misma ley contempla el establecimiento de medidas provisionales, como la suspensión temporal de la actividad del prestador de servicios, el cierre provisional de establecimientos, y la incautación de registros y equipos informáticos. Asimismo, el artículo 9 de la Ley 1/1982 prevé la posibilidad de reclamar daños y perjuicios siguiendo la vía ordinaria o por el procedimiento judicial basado en los principios de preferencia y sumariedad previstos en el artículo 53.2 de la Constitución. En los casos de especial gravedad, se puede recurrir al Tribunal Constitucional mediante un recurso de amparo para garantizar el respeto de los derechos fundamentales.

Del mismo modo el artículo 9.2 establece que se deben adoptar las medidas para rectificar la situación generada por la intromisión, asegurando su cese, la restauración de los derechos del afectado, la prevención de futuras intromisiones y la indemnización por los daños ocasionados. No obstante, según la doctrina, no se trata una lista cerrada por lo que se deja la elección de la medida al arbitrio de la práctica jurídica.

Siguiendo en la misma línea con lo anterior, nos encontramos con la Ley Orgánica reguladora del Derecho de Rectificación⁷⁶ que se trata de una herramienta clave, especialmente en el contexto de internet. Esta ley permite a las personas afectadas por informaciones incorrectas o perjudiciales solicitar su rectificación en los medios de comunicación o plataformas digitales. Este mecanismo resulta crucial en una era donde las redes sociales amplifican rápidamente la difusión de información y las posibles afectaciones a la reputación o dignidad de las personas.

⁷⁶ Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Por otro lado, el Anteproyecto de Ley Orgánica de Protección de los Menores en los Entornos Digitales⁷⁷ introduce disposiciones específicas para garantizar la seguridad y privacidad de los menores en el ámbito digital. Entre las medidas propuestas destacan:

- La implementación de sistemas efectivos de verificación de edad para restringir el acceso a ciertos contenidos.
- La promoción de controles parentales avanzados para supervisar y limitar la actividad de los menores en internet.
- La obligación de los prestadores de servicios digitales de eliminar de forma inmediata contenidos que puedan resultar perjudiciales para los menores.

Además, este anteproyecto prevé sanciones más severas para las plataformas que incumplan estas medidas y refuerza la educación digital mediante campañas de concienciación dirigidas a menores y sus familias.

4.4 Riesgos de los menores en las redes sociales

Hoy en día, las redes sociales no solo para facilitan la comunicación y el intercambio de información entre los usuarios, sino también para recopilar datos personales. Estas plataformas permiten a los jóvenes interactuar y participar activamente, pero al mismo tiempo, representan un riesgo significativo para la exposición de sus datos personales. Desde datos básicos como nombres y edades hasta información más sensible como opiniones y ubicaciones, los menores comparten un gran volumen de datos en estas plataformas. Esta recopilación de datos suele realizarse sin que los usuarios, o sus representantes legales, sean plenamente conscientes u otorguen un consentimiento informado, lo que puede derivar en una serie de riesgos.

A continuación, se analizarán algunos riesgos asociados al uso de las redes sociales por parte de los menores, siguiendo la clasificación propuesta por DAVARA⁷⁸ y complementada con

⁷⁷ Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales

⁷⁸ DAVARA FERNANDEZ DE MARCOS, L, “*Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos*”, la Agencia Estatal Boletín Oficial del Estado Madrid, 2017, p.50, p.53

las aportaciones de SÁNCHEZ PARDO y CRESPO HERRADOR en su estudio sobre adolescentes y tecnologías de la información y comunicación⁷⁹:

- **Bullying y ciberbullying:** Ambos constituyen formas de acoso caracterizadas por comportamientos agresivos e intencionales dirigidos hacia una persona en los que se emplea fuerza o poder. El bullying puede manifestarse en formas físicas, verbales, sociales o psicológicas, manteniendo siempre una relación de desigualdad de poder entre el agresor y la víctima. El ciberbullying, por su parte, se trata de un acoso y persecución que ocurre través de redes sociales, mensajes de texto o correos electrónicos. Al igual que el bullying, el ciberbullying se caracteriza por ser continuado, intencional y por la desigualdad de poder. No obstante, en este caso, el agresor puede valerse del anonimato proporcionado por perfiles falsos, lo que dificulta su identificación y aumenta la sensación de vulnerabilidad de la víctima. El ejemplo más representativo de ciberbullying en las redes sociales incluyen burlas, insultos, persecución y actos de suplantación de identidad, con el propósito de perturbar de manera constante y persistente la vida de la víctima
- **Grooming:** se puede definir como el acoso ejercido por parte de un adulto hacia un menor, que se caracteriza por la creación de confianza entre el agresor y el menor para conseguir que éste acceda a sus peticiones. Generalmente, estas solicitudes están orientadas a obtener imágenes o videos de contenido sexual, en las que el menor, a menudo, no es consciente de que está siendo víctima de un delito, ya que el agresor se presenta como una persona de confianza. Un ejemplo donde se puede apreciar esta conducta delictiva es en la Sentencia 407/2019 de la Audiencia Provincial de Madrid⁸⁰
- **Sexting:** consiste en el envío de contenido sexual o erótico, como fotos o videos, a través de dispositivos móviles o mediante redes sociales ya sean propios o de terceras personas⁸¹. Aunque en la mayoría de los casos se realiza de manera voluntaria y en un contexto de confianza, la divulgación no autorizada de este material puede generar graves riesgos, especialmente cuando involucra a menores, dado que compromete su

⁷⁹ SÁNCHEZ PARDO, L., CRESPO HERRADOR, G., *“Los adolescentes y las Tecnologías de la Información y Comunicación”*. Disponible en línea en <https://digital.csic.es/bitstream/10261/132633/1/TICPadres.pdf>

⁸⁰ Sentencia 407/2019 de la Audiencia Provincial de Madrid

⁸¹ OJEDA PEREZ, M., en Tesis doctoral sobre “Sexting en la adolescencia: Prevalencia, factores asociados y líneas de actuación psicoeducativa”. Sevilla, 2021.

privacidad y seguridad. Además en algunos casos, el sexting puede derivar en situaciones de chantaje, conocidas como sextorsión, donde el material es utilizado para ejercer presión o extorsionar a la víctima.

- **Phishing o la suplantación de identidad:** Este término hace referencia a una práctica fraudulenta en la que una persona se hace pasar por otra o por una entidad confiable con el objetivo de obtener información confidencial de las víctimas. Generalmente, los agresores utilizan métodos engañosos, como correos electrónicos falsos o mensajes que simulan provenir de instituciones legítimas, con el fin de persuadir a los usuarios de compartir datos sensibles. Estos datos pueden incluir información bancaria, contraseñas u otros datos personales, que posteriormente son utilizados para cometer fraudes o actos ilícitos en nombre de la víctima. En el caso de los menores, este tipo de suplantación puede implicar el robo de su identidad digital y el uso no autorizado de su información personal lo que agrava las consecuencias al afectar tanto su privacidad como su seguridad.
- **Acceso a contenidos inapropiados:** es otro riesgo relevante para los adolescentes en línea. Los menores pueden llegar a estos contenidos a través de la curiosidad o mediante anuncios publicitarios. Aunque existen programas de control parental y clasificaciones de contenido como PEGI (Pan European Game Informativo) para los videojuegos, estas medidas no siempre son eficaces, ya que los adolescentes pueden eludir las restricciones.⁸²
- **Adicción a las redes sociales.** consiste en una dependencia excesiva a las redes sociales y a los dispositivos móviles que suele desembocar en la pérdida de las relaciones interpersonales y afectando, normalmente, al rendimiento escolar.
- **Sharenting:** hace alusión a la sobreexposición de los hijos en las redes sociales por parte de los padres. Aunque los medios de comunicación tienen prohibido mostrar la imagen de menores de edad, muchas veces se puede encontrar la imagen de los hijos en las redes sociales de sus progenitores. Esto puede crear un problema cuando los niños crecen y descubren que tienen una identidad digital en la que no participaron. En cuanto a su regulación legal, según JAVIER URRÁ ex defensor del pueblo, está en

⁸² SANCHEZ PARDO, L., CRESPO HERRADOR. G., Op. cit., pág. 32.

desarrollo, pero dicha regulación se suele implementar una vez el problema ya haya surgido, especialmente teniendo en cuenta que Internet no tiene fronteras. Asimismo, añade que *“La razón por la que la imagen del niño debe estar protegida es por el perjuicio que pueda causarle a su intimidad, dignidad y honor”*⁸³. A raíz de la sentencia de la Audiencia Provincial de Pontevedra⁸⁴ se requiere del consentimiento del otro progenitor para poder publicar fotos de un hijo menor en redes sociales, sobre todo si no comparten la custodia. Sin embargo, este consentimiento debe ser otorgado por el propio menor una vez que cumpla los 14 años.

Ante este fenómeno, algunos países de nuestro entorno como Francia han comenzado a tomar medidas contra la publicación de fotos de hijos menores sin su consentimiento, imponiendo multas y penas de prisión a los padres. De hecho, autores como ERIC DELCROIX considera que *“en pocos años, los menores podrán llevar a sus padres a juicio por publicar fotos de cuando eran más jóvenes”*⁸⁵

5. LOS PROVEEDORES DE SERVICIO EN LINEA

5.1. Actuación y responsabilidad

Los prestadores de servicios aparecen definidos en la Directiva 2000/31/CE en el artículo 2.b, definición que es reiterada en el Anexo de la LSSICE dedicado exclusivamente a las definiciones. De esta manera, se puede entender como prestadores de servicios aquellos que facilitan el acceso a Internet y al intercambio de datos, y pueden ser tanto personas físicas como jurídicas.

Estos prestadores pueden operar tanto dentro de España como dentro de la Unión Europea, o incluso fuera de esta, pero teniendo en cuenta el Espacio Económico Europeo. Su actividad es autónoma y limitada al respeto del orden público y a la dignidad de las personas, siendo la

⁸³ COBO, I. (3 de octubre de 2018). Hijos de famosos: pixelados en los medios, pero hiperexpuestos en las redes sociales. El Mundo.

⁸⁴ Sentencia de la Sección Primera de la Audiencia Provincial de Pontevedra, de 4 de junio de 2015

⁸⁵ ¿Deben los padres publicar fotos de sus hijos en las redes sociales? (30 de marzo de 2017).

Europa Press. Obtenido el 12/05/2024:

<https://www.europapress.es/portaltic/socialmedia/noticia-deben/padres-publicar-fotos-hijos-redes-sociales-20161107085948.html>

autoridad judicial la encargada de proteger los derechos personales en caso de vulneración y de restituir dichos derechos.

Por lo que, frente a las posibles injerencias que puedan surgir, la medida principal para la restitución de estos derechos consiste en localizar e identificar a la persona que los ha vulnerado. No obstante, puede ocurrir que, en diversas ocasiones, no se pueda determinar quiénes son los infractores en el ámbito digital, así que en estos casos la responsabilidad recaerá sobre los prestadores de servicios, abarcando diversos ámbitos como puede ser el civil, penal o incluso el administrativo tal y como nos indica la SAP de Barcelona 707/2010, de 29 de noviembre (Rec. 563/2006) en el Fundamento Jurídico Segundo.⁸⁶

Atendiendo a los artículos 11 y 14 a 16 de la LSSICE, la responsabilidad no solo se va a limitar al creador de la página web, sino que también impone obligaciones y responsabilidades a los prestadores de servicios, quienes deben colaborar en la retirada de los datos ilícitos cuando sean informados de su existencia.⁸⁷

Se debe añadir, en base al artículo 10, que es esencial que el prestador mantenga la información actualizada para que el usuario pueda contactarlo en caso de ser necesario. La SAP de Madrid 526/2010, de 23 de noviembre (Rec. 67/2009), en su Fundamento Jurídico Doceavo⁸⁸, establece que en caso de que esta información sea correcta, el prestador será responsable cuando no actúe como debe cuando el usuario haya contactado con él y le haya informado de la situación de intromisión de su derecho en la que se encuentra.⁸⁹

Además, la misma sentencia indica que esta responsabilidad también se extenderá a "otros casos en los que, habiendo cumplido el proveedor del servicio con su obligación de información actualizada, el perjudicado se haya puesto en contacto con el proveedor del servicio solicitando la eliminación del mensaje o dato que considera una violación de sus derechos fundamentales, y el proveedor no haya actuado diligentemente para retirar esos datos, lo que impide acceder a ellos".

⁸⁶ SAP de Barcelona 707/2010, de 29 de noviembre (Rec. 563/2006) en el Fundamento Jurídico Segundo

⁸⁷ CONTRERAS NAVIDAD,S . (2012) *"La protección del honor, la intimidad y la propia imagen en Internet"*. Pamplona: Aranzadi. Página 134.

⁸⁸ SAP de Madrid 526/2010, de 23 de noviembre (Rec. 67/2009), en su Fundamento Jurídico Duodécimo

⁸⁹ CONTRERAS NAVIDAD,S . (2012) *"La protección del honor, la intimidad y la propia imagen en Internet"*. Pamplona: Aranzadi. Página 136

Sin embargo, esto solo se va a aplicar a aquellos casos claros y evidentes de violación de los derechos fundamentales del perjudicado, ya que la ley no autoriza al proveedor del servicio a actuar como juez de los contenidos de su portal de Internet.

5.2. Supuestos que provocan responsabilidad

La responsabilidad se va a clasificar teniendo en cuenta a los diferentes sujetos involucrados y la función que desempeñan cada uno de ellos. A continuación, se presentan los diferentes casos contemplados:

En este sentido, la Directiva 2000/31/CE, específicamente en sus artículos 12, 13 y 14, establece claramente las circunstancias bajo las cuales estos proveedores no serán responsables de los datos que transmiten, almacenan temporalmente o alojan.

El artículo 12 aborda la "mera transmisión de datos", indicando que el prestador no será responsable si no inicia la transmisión y no selecciona al destinatario de los datos ni altera la información transmitida. Por su parte, el artículo 13 se refiere a la "memoria tampón" o "caching", exime de responsabilidad al prestador siempre y cuando no modifique los datos y acceda a ellos según lo pactado, y no interfiera en la obtención de los datos eliminando la información que ya no debería estar en la red. Finalmente, el artículo 14 trata sobre el "alojamiento de datos" o "hosting", eximiendo de responsabilidad al prestador si no tiene conocimiento de la ilegalidad de los datos almacenados y actúa rápidamente para eliminarlos una vez tenga conocimiento de su carácter ilícito.

De manera similar, la Ley de Servicios de la Sociedad de la Información (LSSICE)⁹⁰ en sus artículos 14, 15, 16 y 17 clasifica la responsabilidad de los diferentes actores. El artículo 14 establece que los operadores de red y proveedores de acceso no serán responsables por la información transmitida salvo que ellos mismos hayan ocasionado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos sin alterar los datos. El artículo 15 señala que los prestadores que almacenan temporalmente datos para su transmisión no serán responsables si cumplen con ciertas funciones específicas como no modificar la información o respetar determinadas reglas que son aceptadas y aplicadas por el sector. El artículo 16 exime de responsabilidad a los prestadores de servicios de alojamiento

⁹⁰ Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

de datos siempre que no tengan conocimiento efectivo⁹¹ de la ilegalidad de la información y actúen diligentemente para retirarla. Por último, el artículo 17 establece que los prestadores que facilitan enlaces a contenidos no serán responsables si cumplen con los requisitos establecidos que son los mismos que los establecidos en el artículo anterior: no tener conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita y en el caso de que lo tenga actúen con diligencia para eliminarla.

La normativa, en definitiva, determina las exenciones de responsabilidad para los proveedores de servicios en Internet, siempre y cuando cumplan con los deberes de diligencia exigidos por la ley y no sean responsables de los contenidos introducidos por terceros.

5.3 Breve referencia a la Ley de Servicios Digitales

A pesar de que la Directiva 2000/31/CE sigue siendo de aplicación, en febrero de 2024 entró en vigor La Ley de Servicios Digitales⁹² que consiste en una normativa que va a actualizar la directiva anterior y tiene como objetivo crear un entorno en línea más seguro y transparente, protegiendo los derechos de los usuarios y garantizando la responsabilidad de las plataformas digitales.

Entre sus principales novedades caben destacar que impone obligaciones más estrictas para las grandes plataformas en línea que tengan más de 45 millones de usuarios dentro de la UE por lo que van a tener que implementar medidas adicionales para, de esta manera, reducir riesgos, como la desinformación o la manipulación, y estarán bajo la supervisión directa de la Comisión Europea. Además, la normativa pone importancia en la protección de los derechos fundamentales de los usuarios, garantizando un mayor control sobre sus datos y una mejor protección contra contenidos dañinos, con especial atención a la seguridad de los niños.

En definitiva, esta ley constituye un avance significativo hacia una regulación más sólida y adaptada a las realidades actuales del entorno digital, con el objetivo de equilibrar la innovación con la seguridad y la protección de los usuarios.

⁹¹ Significa tener una certeza real, y no meras sospechas.

⁹² Ley de Servicios Digitales (DSA)

6. PAPEL DE LAS AUTORIDADES

Las autoridades desempeñan un papel esencial en la defensa de los derechos de los menores en el contexto de las redes sociales. Su responsabilidad abarca tanto la esfera nacional como la internacional, e incluye la implementación de leyes y normativas, así como la promoción de políticas y programas educativos.

A nivel internacional, las autoridades colaboran con diversos organismos para desarrollar estrategias y políticas conjuntas enfocadas en la protección de grupos vulnerables como los menores. Estas entidades desempeñan un papel relevante especialmente en el ámbito digital, y su cooperación es fundamental para abordar los desafíos internacionales relacionados con el tratamiento de datos en las redes sociales. Esto implica, por tanto, la participación en conferencias y foros internacionales, así como la cooperación en investigaciones y enjuiciamientos de delitos que afectan a menores.

Esto es así que cabe destacar a diversos organismos internacionales:

1. **Comité Europeo de Protección de Datos (CEPD)**⁹³: Este organismo, creado por el RGPD, facilita la aplicación coherente de la normativa de protección de datos en toda la Unión Europea. Emite directrices y recomendaciones que son adoptadas por las autoridades nacionales, como la AEPD, y promueve la cooperación entre los Estados miembros.
2. **Organización para la Cooperación y el Desarrollo Económicos (OCDE)**⁹⁴: La OCDE juega un papel relevante al proporcionar un marco para la cooperación internacional en materia de protección de datos. Sus directrices sobre privacidad y flujos de datos transfronterizos son fundamentales para armonizar las políticas entre los países miembros
3. **Organización de las Naciones Unidas (ONU)**⁹⁵ La ONU, a través de su Consejo de Derechos Humanos, ha destacado la importancia de proteger la

⁹³ Página web del Comité Europeo de Protección de Datos https://www.edpb.europa.eu/role-edpb_es

⁹⁴ Página web de la Organización para la Cooperación y el Desarrollo Económicos <https://web.archive.oecd.org/espanol/index.htm>

⁹⁵ Página web de la Organización de las Naciones Unidas <https://www.un.org/es/>

privacidad de los menores en el entorno digital. Promueve iniciativas globales y recomendaciones que guían a los países en la formulación de políticas y leyes para la protección de datos personales.

A nivel nacional, corresponde a las autoridades la responsabilidad de establecer marcos legales y regulatorios que protejan los derechos de los menores en internet. Esto se materializa en la elaboración de leyes específicas que abordan aspectos como la seguridad, la privacidad o el acceso a contenidos inadecuados en las redes sociales. Un ejemplo de ello es la creación de sistemas de verificación de edad que respeten la privacidad⁹⁶ o la tipificación de delitos como la difusión no autorizada de imágenes.

Así que teniendo en cuenta lo visto anteriormente, a continuación vamos a describir el papel de algunas autoridades relevantes:

1. **Agencia Española de Protección de Datos (AEPD):** La AEPD es la autoridad encargada de garantizar y supervisar el cumplimiento de la normativa de protección de datos en España. En el contexto de los menores en las redes sociales, la AEPD se encarga de velar por la protección de la privacidad y los datos personales de los menores, investigando y sancionando posibles infracciones.
2. **Instituto Nacional de Ciberseguridad (INCIBE)**⁹⁷: El INCIBE es el organismo público español responsable de la seguridad en el ámbito digital. Ofrece recursos y herramientas de educación y concienciación dirigidas a los menores y sus familias para promover un uso seguro y responsable de las redes sociales.
3. **Ministerio de Educación y Formación Profesional**⁹⁸: El Ministerio de Educación tiene un papel importante en la educación y sensibilización de los menores sobre el uso adecuado de las redes sociales. Promueve programas de

⁹⁶ Análisis sobre la protección de los niños <https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-analisis-sobre-la-proteccion-de-ninos>

⁹⁷ Página web del Instituto Nacional de Ciberseguridad <https://www.incibe.es/>

⁹⁸ Página web del Ministerio de Educación y Formación Profesional <https://www.educacionfpydeportes.gob.es/>

formación y concienciación en las escuelas para fomentar el uso responsable de las tecnologías y prevenir riesgos.

Es fundamental que las autoridades trabajen en conjunto para abordar los desafíos relacionados con los menores en las redes sociales, adoptando medidas de protección, promoción de la seguridad y educación en el entorno digital.

6.1 Posición del Ministerio Fiscal

La figura del Fiscal, desde una perspectiva constitucional y legal, se configura como un defensor de la legalidad y protector de los más vulnerables, especialmente de los menores. En el marco de esa función protectora, el Fiscal se encarga de asegurar el respeto a la privacidad de los menores, labor que se mantiene incluso cuando los propios menores o sus progenitores hayan otorgado su consentimiento para permitir la intromisión en tales derechos. Por ello, no nos podemos olvidar, como ya hemos visto, que los menores son los titulares de los derechos al honor, a la intimidad y a la propia imagen, y no sus progenitores. Esto se establece claramente en el artículo 4 de la Ley Orgánica 1/1996⁹⁹, de 15 de enero (LOPJM).

*Se impone al Ministerio Fiscal la obligación de accionar en los casos en que la intromisión a que se refiere el art. 4 se produzca a través de un medio de comunicación. El Fiscal no tiene en este ámbito funcional una legitimación subsidiaria, sino que deberá actuar cuando proceda aun cuando el menor esté representado por progenitores que ejerzan adecuadamente la patria potestad.*¹⁰⁰

Ese artículo 4 admite la participación del Ministerio Fiscal en casos de intromisiones ilegítimas en los derechos de honor, intimidad y propia imagen de los menores y puede actuar ya sea por iniciativa propia, a solicitud del menor o de cualquier otra persona interesada.

Esta intervención no pretende que sean los progenitores los que infrinjan los derechos del menor ni tampoco implica un mal ejercicio de la patria potestad por parte de estos sino lo que pretende la ley es brindar una defensa pública en favor de los menores, garantizando una protección especial y efectiva más allá de la proporcionada por los padres. De todas maneras,

⁹⁹ Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, Artículo 4

¹⁰⁰ Instrucción 2/2006 Sobre el Fiscal y la Protección del derecho Al Honor, Intimidad y Propia Imagen de los menores

esta protección pública establecida en la LO 1/1996 debe ser valorada junto con los artículos 154 y 162.1 del Código Civil, que reconocen las facultades de la patria potestad.

Según la Ley Orgánica de Protección Jurídica del Menor (LOPJM), en su artículo 4.3, se reconoce que puede existir una intromisión ilegítima en los derechos del menor si consta el consentimiento del menor o de sus representantes legales. No obstante, esto puede resultar contradictorio con el objetivo de proteger al menor, ya que tal y como establece a Exposición de Motivos 2ª “ *la mejor forma de garantizar social y jurídicamente la protección a la infancia es promover su autonomía como sujetos* ”¹⁰¹ De esta manera , el menor tiene derecho a ser escuchado y tener su opinión considerada (artículo 9 LOPJM) lo cual es importante para en el supuesto caso de que existan conflictos de interés con sus padres o que el menor se oponga a las acciones que lleva a cabo el propio Ministerio Fiscal. Entonces para que se pueda llevar a cabo, se tiene que considerar si el menor tiene la suficiente madurez para poder ejercer este derecho por sí mismo que, en cualquier caso, será cuando tenga doce años cumplidos.¹⁰²

El Tribunal Constitucional ha defendido la necesidad de otorgar audiencia al menor en los procesos judiciales cuando tenga la capacidad suficiente para ello, ya que la omisión de este trámite puede desembocar en una violación del derecho a la tutela judicial efectiva. Por lo tanto, al intervenir, el Ministerio Fiscal se evalúa el interés superior del menor, el pleno ejercicio de la patria potestad por parte de los padres, los derechos a la información y la libertad de expresión, así como la posible vulneración de los derechos al honor, la intimidad y la propia imagen.

En este contexto, es importante destacar la Ley de Jurisdicción Voluntaria¹⁰³ la cual aborda el derecho al honor, la intimidad y la propia imagen del menor, y regula los casos en los que el Ministerio Fiscal se opone al consentimiento prestado por el representante legal del menor lo que conllevara a tomar una decisión al órgano judicial correspondiente.

En resumidas cuentas, el Fiscal actúa como garante de la privacidad de los menores, aun cuando ellos o sus padres se expongan voluntariamente, siempre y cuando dicha exposición

¹⁰¹ Exposición de Motivo 2ª de la Ley Orgánica 1/1996 de 15 de enero, de protección Jurídica del Menor

¹⁰² Ley Orgánica de Protección Jurídica del Menor (LOPJM) Artículo 9.2

¹⁰³ Ley de la Jurisdicción Voluntaria

pueda considerarse una intromisión ilegítima en sus derechos, ya sea por menoscabar su honra, reputación o ser contraria a sus intereses.

6.2 Labor de los abogados

En un entorno tan reciente como es la protección de datos, es de vital importancia que los abogados se especialicen en este ámbito para asesorar y manejar los conflictos emergentes que afectan a los derechos de privacidad de los clientes. Aunque ni el Estatuto General (EGAE)¹⁰⁴ ni el Código Deontológico de la Abogacía Española¹⁰⁵ mencionan específicamente la protección de datos como un área de especialización, ambos establecen principios que obligan a los abogados a actuar con diligencia, mantener una formación continua y garantizar la defensa de los derechos fundamentales, incluyendo la privacidad. Esto refuerza la necesidad de abordar los retos actuales relacionados con la protección de datos personales.

Por lo tanto, cuando se vulneren los derechos del cliente o de sus hijos, se debe acudir directamente a la AEPD presentando una denuncia. Este proceso de denuncia ante la Agencia Española de Protección de Datos (AEPD) se divide en dos etapas.

En la primera fase, se realizan investigaciones preliminares donde la AEPD examina la documentación y las pruebas presentadas sin que exista un plazo específico establecido por ley. En la segunda fase, se inicia el procedimiento sancionador, el cual puede conllevar diversas acciones como la imposición de sanciones, emitir apercibimientos, sustituir la sanción o el archivo del caso si no se encuentra responsabilidad o se han cumplido las medidas correctivas requeridas.

Los interesados tienen la posibilidad de impugnar esta resolución presentando un recurso de reposición ante la directora de la AEPD en un plazo máximo de un mes, o interponiendo un recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.¹⁰⁶ Este momento marca el acceso a la jurisdicción y subraya la importancia del papel del abogado en el proceso.

¹⁰⁴ Estatuto General de la Abogacía Española

¹⁰⁵ Código Deontológico de la Abogacía Española

¹⁰⁶ Resolución 1870/2017 de 21 de agosto de 2017, Procedimiento N° PS/00082/2017

Antes de presentar la denuncia, el interesado debe ejercer sus derechos ARSULIPO, que incluyen el derecho de acceso, rectificación, supresión, limitación del tratamiento, oposición e información, enviando una solicitud al responsable del tratamiento. Es crucial recopilar todas las pruebas pertinentes que respalden la vulneración o infracción denunciada para aumentar las posibilidades de éxito.

Una vez recabada la documentación necesaria, se debe completar el formulario de denuncia disponible en la página web de la AEPD. Este formulario debe detallar *“nombre y apellidos del interesado y, en su caso, de la persona que le represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones; hechos, razones y petición en la que se concrete, con toda claridad, la solicitud; lugar y fecha; firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio; identificación de los presuntos responsables; y todos aquellos documentos o cualquier otro tipo de prueba o indicio que permita corroborar los hechos denunciados”*¹⁰⁷ Finalmente, el formulario y la documentación deben ser presentados ante la AEPD, ya sea de forma telemática mediante el registro electrónico con certificado digital, o de manera presencial en la sede de la Agencia en Madrid. Las sanciones¹⁰⁸ que impone la AEPD tras resolver la denuncia son de naturaleza administrativa y no incluyen por lo tanto indemnizaciones. Sin embargo, si la vulneración ha causado un perjuicio, especialmente en los derechos de honor, intimidad y propia imagen, se debe recurrir a los tribunales ordinarios para buscar una compensación y denunciar al infractor.¹⁰⁹

En aquellos casos en los que se produzca una violación grave que involucren conductas delictivas, se debe recurrir a un proceso penal atendiendo a lo previsto en la Ley de Enjuiciamiento Criminal¹¹⁰ o la Ley de Responsabilidad Penal de los Menores.

¹⁰⁷ Canal del ciudadano AEPD:

<http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciaciudadano/index-ides-idphp.php>

¹⁰⁸ Reglamento (UE) 2016/679, Art 86.

¹⁰⁹ Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) publicada en el BOE núm.294 de 6 de diciembre de 2018, Referencia: BOE-A-2018-16673, Art.27 y 76.

¹¹⁰ Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal

7. MEDIDAS DE PREVENCIÓN DE LOS MENORES DE LOS RIESGOS DE LAS REDES SOCIALES

La página web de la AEPD ofrece recursos educativos para niños, padres y personas cercanas a ellos en relación a la protección de datos personales. Estos recursos son útiles para familias, educadores y escuelas, y brindan información y orientación sobre este tema.

En esta página, concretamente en el apartado que recibe el nombre de “Tú decides en internet”¹¹¹ se ofrecen recursos como videos y guías para que los menores utilicen Internet de manera segura. También se proporcionan números de contacto para informar a la Agencia sobre cualquier problema que puedan enfrentar en Internet.

A continuación, vamos a analizar los recursos que ofrece esta página para los educadores, para los familiares e incluso para los propios jóvenes.

7.1 Medidas educativas

En cuanto a los educadores, distinguimos la Guía para centros educativos¹¹². Esta guía es un recurso dirigido a educadores que aborda la protección de datos en el entorno escolar. Se centra, principalmente, en los datos de los alumnos, progenitores, profesores y personal del centro, y subraya la importancia de cumplir con las exigencias de protección de datos tanto en la recopilación, publicación y comunicación de la información de los alumnos. También aborda el tratamiento de las imágenes de los alumnos, que juegan un papel fundamental en la protección de datos en la actualidad. El uso de estas imágenes para la promoción y difusión de actividades del centro en perfiles y páginas de redes sociales se ha convertido en una forma de destacar entre otras ofertas educativas.

A mayores, nos encontramos con otras dos guías específicas dirigidas tanto para los educadores como para las familias que abordan los problemas a los que los menores pueden enfrentarse en internet y cómo advertirles de los mismos. Explican de manera detallada las distintas conductas delictivas que pueden ocurrir y ofrecen distintos métodos y estrategias para hacerlas frente.

¹¹¹ Página web de “Tú Decides en Internet” <https://www.tudecideseninternet.es/>

¹¹² Guías centro educativos <https://www.aepd.es/guias/guia-centros-educativos.pdf>

7.2 Herramientas tecnológicas de control parental

En relación a los padres y tutores, la Agencia Española de Protección de Datos establecen una serie de recomendaciones¹¹³ para hacer frente a dichos riesgos:

1. Educar a los menores sobre los riesgos para su privacidad y su seguridad en el uso de tecnologías móviles fomentando con ello un uso responsable de la misma.
2. Reducir el tiempo que los menores pasan usando dispositivos conectados.
3. Informarles de que es necesario tomar medidas por su propia seguridad.
4. Utilizar sistemas operativos, proveedores de internet y otros terceros que proporcionen opciones de control parental para supervisar el uso de dispositivos móviles.
5. Configurar las distintas opciones de control parental, las cuales incluyen funcionalidades como el filtrado de contenido, limitación de horarios, bloqueo de aplicaciones, detalles de uso de las redes sociales, localización GPS, etc.
6. Utilizar navegadores y aplicaciones en su versión infantil que son alternativas que pueden ser menos intrusivas.
7. Considerando que algunas herramientas tienden a bloquear excesivamente, es importante mantener la opción de desbloquear contenido a solicitud del menor y estar dispuesto a negociar con ellos los filtros y restricciones a aplicar puesto que un exceso de bloqueo podría llegar resultar contraproducente

7.3 Indicaciones para los operadores de servicio en línea

A mayores, la Agencia también va a llevar a cabo una serie de recomendaciones para la industria, es decir, a los prestadores de servicio¹¹⁴. Algunas de esas recomendaciones son:

1. Minimización de datos. Las aplicaciones deben permitir a los padres activar y desactivar funciones según sus necesidades, sin tratar datos de funcionalidades desactivadas.

¹¹³ Recomendaciones para padres y tutores <https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteccion-del-menor-en-internet.pdf>

¹¹⁴ Recomendaciones para la industria <https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteccion-del-menor-en-internet.pdf>

2. Reducción de permisos. De forma similar al punto anterior, se deben implementar mecanismos para evitar solicitar permisos innecesarios. Por ejemplo, si no se usa la función de GPS, la aplicación no debería acceder a datos de geolocalización en un segundo plano.

3. Gestión de librerías de terceros. s aplicaciones deben informar sobre el uso de bibliotecas de terceros que gestionen datos personales y obtener un consentimiento válido antes de su uso. Deben evitarse las transferencias de datos sin una base legal adecuada y sin informar a los usuarios.

4. Garantías en los servicios en la nube. Las aplicaciones deben informar sobre el uso de bibliotecas de terceros que gestionen datos personales y obtener un consentimiento válido antes de su uso. Deben evitarse las transferencias de datos sin una base legal adecuada y sin informar a los usuarios.

5. Aplicación de medidas de seguridad. Teniendo en cuenta el volumen, categorías y el perfil de los individuos, se deberían de maximizar las medidas aplicando los más altos estándares de seguridad.

En general, estas guías lo que pretenden es facilitar una educación en la protección de datos personales, animando a los jóvenes a no compartir información excesiva con el público general de Internet y a ser conscientes de los posibles riesgos que enfrentan.

8. CONCLUSIONES

El avance de las nuevas tecnologías ha transformado la vida diaria de las personas impactando de manera significativa en ámbitos como la educación, la comunicación y el entretenimiento. Por tanto, regular los problemas derivados del uso de Internet y las redes sociales se ha convertido en uno de los retos jurídicos más importantes del siglo XXI.

PRIMERA

El impacto de Internet en la vida de los menores es innegable, afectando su desarrollo en múltiples dimensiones. Aunque el entorno digital ofrece oportunidades educativas y sociales, también expone a los menores a riesgos que pueden comprometer su seguridad y bienestar. Debido a su falta de madurez, los menores suelen desconocer los peligros asociados al uso inadecuado de las redes sociales y plataformas digitales, lo que los convierte en un grupo especialmente vulnerable.

Por ello, es fundamental garantizar una protección especial para los menores en el marco jurídico, priorizando su derecho a la intimidad y la protección de sus datos personales. Este enfoque debe estar sustentado en el principio del interés superior del menor, reconocido en diversas normativas internacionales y nacionales, como eje central de cualquier legislación o política pública. Solo así será posible asegurar un entorno digital más seguro y respetuoso con los derechos de los menores.

SEGUNDA

La falta de educación digital es otro problema crucial. Muchos jóvenes no son plenamente conscientes de las consecuencias a largo plazo de su exposición en el entorno digital. Normalizan conductas perjudiciales, como la sobreexposición o la publicación de información sensible, lo que puede derivar en riesgos como el ciberacoso, el grooming o el uso indebido de sus datos personales.

Además, este desconocimiento no solo afecta a los menores. Los padres y tutores, en muchos casos, tampoco cuentan con las herramientas necesarias para guiar a sus hijos en el uso seguro de Internet. La brecha generacional en el conocimiento digital dificulta que los adultos detecten o prevengan comportamientos peligrosos en los menores. Esta carencia educativa

contribuye al incremento de conflictos en redes sociales, desde problemas de convivencia escolar hasta situaciones legales complejas.

Para abordar este problema, es fundamental implementar una estrategia que incluya campañas de sensibilización, programas educativos en escuelas y formación específica para padres, menores y docentes. Estas iniciativas deben enfocarse en fomentar un uso responsable de las redes sociales, identificar riesgos digitales y prevenir conductas perjudiciales. Para ello, el Estado debe promover estas medidas, integrándolas en los planes educativos mediante charlas, debates y formación docente, además de ofrecer materiales informativos para las familias, fortaleciendo su papel como guías en la educación digital de los menores.

TERCERA

El consentimiento y la madurez de los menores son cuestiones complejas que adquieren una relevancia especial en el ámbito digital, donde sus derechos de personalidad, como la intimidad, el honor y la propia imagen, están en constante riesgo. La legislación española establece una edad mínima para que los menores puedan consentir de forma válida en la cesión de datos (actualmente fijada en 14 años), pero no ofrece criterios claros para evaluar la madurez necesaria para tomar decisiones informadas. Esta falta de claridad crea incertidumbre tanto para los menores como para sus representantes legales.

Por otro lado, a pesar de la existencia de normativas específicas para proteger a los menores frente a intromisiones ilegítimas, como el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), estas leyes no establecen diferencias sustanciales entre menores y adultos en cuanto a las medidas de protección. Esto resulta problemático porque los menores, debido a su edad y desarrollo cognitivo, son más vulnerables a sufrir vulneraciones en plataformas digitales, como el uso indebido de su imagen o la difusión de información sensible.

Es por ello por lo que se necesita una legislación más sólida que garantice que los menores puedan tomar decisiones informadas en el ámbito digital mediante criterios claros sobre su madurez. Además, se debe reforzar la protección en las plataformas tecnológicas, exigiendo herramientas como controles parentales, sistemas fiables de verificación de edad y restricciones de acceso a contenidos inapropiados. Es imprescindible establecer mecanismos de supervisión y sanción efectivos que aseguren el cumplimiento de las normativas, así como

fomentar la colaboración entre legisladores y plataformas para desarrollar sistemas que detecten y notifiquen vulneraciones de derechos, facilitando la intervención de las autoridades.

Por último, la legislación debe ser flexible y actualizarse constantemente para afrontar los retos que plantean tecnologías emergentes como la inteligencia artificial, garantizando la seguridad y el bienestar de los menores en un entorno digital en constante cambio.

CONCLUSIÓN FINAL

En definitiva, a pesar de que España cuenta con una amplia legislación sobre la materia, sigue teniendo un largo camino por recorrer acerca a la protección de los menores en las redes sociales, y es un problema que no desaparecerá, ya que los avances tecnológicos no se detendrán. Hace años, era impensable que nuestra sociedad se enfrentara a estos problemas, y el sistema legal no ha sido capaz de prevenirlos. Por lo que ahora, al ser conscientes de los mismos, se deben buscar soluciones efectivas y anticiparse a los nuevos desafíos que puedan surgir en el futuro, para construir un entorno digital que priorice el bienestar de las generaciones más jóvenes.

9. BIBLIOGRAFÍA

- ANDREU MARTÍNEZ, M.^a B. *La protección de datos personales de los menores de edad*, Thomson Reuters, Aranzadi S.A Navarra. 2013
- AYLLON GARCIA, J.D., en “*Consentimiento de los menores de edad en las redes sociales: especial referencia a Tiktok*”. Pp 580-601. Disponible en: 24.-Jesús-Daniel-Aillón-580-609.pdf (revista-aji.com)
- BARRIO ANDRÉS, M. *Los derechos digitales y su regulación en España, la Unión Europea e Iberoamérica* (Cuadernos de la Cátedra de Relaciones Privadas Internacionales Universidad Miguel Hernández de Elche-Ilustre Colegio de Abogados de Orihuela, Cuaderno n.º 1). Ed: Colex (2023) pp 35-53
- BATUECAS CALETRÍO, A.: *El control de los padres sobre el uso que sus hijos hacen de las redes sociales, En torno a la privacidad y protección de datos en la sociedad de la información*, Editorial Comares, Granada (2015)
- BONILLA SÁNCHEZ, J.J.: *Personas y derechos de la personalidad*, Ed. Reus, Madrid, 2010
- COBOS, P. S. (2007). Cap. III “*Los derechos del interesado*”. Buenas prácticas en protección de datos. Fundación Dintel.
- CONTRERAS NAVIDAD, S. *La protección del Honor, la intimidad y la propia imagen*, Pamplona: Thomson Reuters, Aranzadi.
- DÁVARA FERNÁNDEZ DE MARCOS, L. (2017) *Menores en internet y redes sociales: Derecho aplicable y deberes de los padres y centros educativos*. Ed. Agencia Estatal Boletín Oficial del Estado, Madrid, (2017) Disponible: <https://www.aepd.es/sites/default/files/2019-10/menores-en-internet.pdf>
- DÍEZ-PICAZO, L Y PONCE DE LEÓN, L; GULLÓN BALLESTEROS, A. *Sistema de Derecho Civil. Volumen I*. Edición Tecnos, Madrid (1997)
- GARCÍA SAN MIGUEL, L., “*Estudio sobre el derecho a la intimidad*”, Techos, Madrid, 1992,
- GITRAMMA GONZALEZ, M. (1967). *Voz “imagen, (derecho a la propia)”*. En Nueva enciclopedia jurídica. Tomo XI (p. 326). Barcelona (Año)
- LASARTE ÁLVAREZ, CARLOS: *Principios de Derecho civil. Derecho de Familia*, Tomo sexto, Decimosexta edición. Ed. Marcial Pons, Madrid 2015

- MACENAITE, M., & KOSTA, E. (2017). Consent for processing children's personal data in the EU: Following in US footsteps? *Information & Communications Technology Law*, 26(2).
- MATE SATUÉ L.C. (2016) ¿*Qué es el derecho al olvido?*, *Revista de Derecho civil* (ISSN 2341-2216, vol3, nº2), pp. 187-222.
- MÚRTULA LAFUENTE, V. (2016). *Valoración del interés superior del menor a la hora de adoptar medidas civiles en situaciones de conflicto parental*. Madrid: Dykinson.
- O'CALLAGHAN MUÑOZ, X., *Libertad de expresión y sus límites: honor, intimidad y propia imagen*, cit., p.194, Edersa, Madrid, 1991
- RODRÍGUEZ AYUSO, J.F, *Garantía Administrativa de los derechos del interesado en materia de protección de datos personales*, , Bosch Editor, capítulo primero, pág.58.
- REQUENA, F (1989), “*El concepto de red social*”. *Reis*,48, pp.137-152
- ROJAS, M. A. (2014). *Análisis de un problema deóntico respecto del derecho a la intimidad de los menores de edad y el alcance del ejercicio de la patria potestad en la utilización de internet y las redes sociales*. *Ratio iuris Revista de Derecho Privado*, núm. 2, paginas 96-107
- SANCHEZ PARDO, L., CRESPO HERRADOR. G., en “*Los adolescentes y las Tecnologías de la Información y Comunicación*”. Disponible on-line en <https://digital.csic.es/bitstream/10261/132633/1/TICPadres.pdf>
- DE URANO CASTRILLÓN, EDUARDO, “*Derechos de la personalidad en Internet*”, *Revista Aranzadi Doctrinal*, núm. 9/2010, Aranzadi, Pamplona, 2010.

LEGISLACIÓN

- Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales
- Código Deontológico de la Abogacía Española
- Constitución Española 1978
- Estatuto General de la Abogacía Española
- Exposición de Motivo 2ª de la Ley Orgánica 1/1996 de 15 de enero, de protección Jurídica del Menor.
- Informe 466/2004 sobre la Comunicación a los padres de las calificaciones de sus hijos menores de edad.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

- 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
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.
- Ley 15/2015, de 2 de julio, de la Jurisdicción Voluntaria
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor
- Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales
- Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley de Servicios Digitales (DSA)
- Instrucción 2/2006 Sobre el Fiscal y la Protección del derecho Al Honor, Intimidad y Propia Imagen de los menores
- La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSCIE)
- Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.
- Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial
- Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.
- Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.
- Real Decreto 1720/2007 del 21 de diciembre, que aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999.

TEXTOS NORMATIVOS

- Federal Trade Commission. (1999). *Children's Online Privacy Protection Rule ("COPPA")*. <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (Última consulta 03/10/2024)

- Federal Trade Commission. (2013). *Children's Online Privacy Protection Rule: Final Rule Amendments to Clarify the Scope of the Rule and Strengthen Its Protections for Children's Personal Information*.
https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf (Última consulta 03/10/2024)
- Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*. Proclamada por la Resolución 217 A (III), de 10 de diciembre de 1948, de la Asamblea General de las Naciones Unidas. <https://www.un.org/es/universal-declaration-human-rights/> (Última consulta 04/10/2024)
- Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de dichos datos*. (Última consulta 07/10/2024)
- Parlamento Europeo y Consejo de la Unión Europea. (2018). *Reglamento (UE) 2018/1807 sobre la libre circulación de datos no personales en la Unión Europea*. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81888> (Última consulta 07/10/2024)
- Comisión Europea. (n.d.). *Documentación del Grupo del Artículo 29*. http://ec.europa.eu/justice/dataprotection/article29/documentation/opinion/recommendation/index_en.htm#maincontentSec15 (Última consulta 4/10/2024)

JURISPRUDENCIA

○ AUDIENCIA PROVINCIAL

- Sentencia de la Sección Primera de la Audiencia Provincial de Pontevedra. Núm. 208/2015 de 4 de junio de 2015. Vlex. (ECCLI: ES:APP:2015:208)
- Sentencia de la Audiencia Provincial de Madrid. Núm. 526/2010, de 23 de noviembre Vlex (ECLI: ES:APM:2010:10661^a)
- Sentencia Audiencia Provincial de Barcelona Fundamento jurídico segundo Núm. 707/2010, de 29 de noviembre Vlex (Rec. 563/2006). (ECCLI:ES:APB:2010/707)

○ TRIBUNAL CONSTITUCIONAL

- Sentencia Tribunal Constitucional. Pleno Núm. 292/2000, de 30 de noviembre. Vlex (ECLI:ES:TC:2000:292)

- Sentencia del Tribunal Constitucional. Sala primera Núm. 254/1993 de 20 de julio. Vlex (ECLI:ES:TC:1993:254)
- Sentencia del Tribunal Constitucional. Sala segunda Núm. 94/1998, de 4 de mayo. Vlex (ECLI:ES:TC:1998:94)
- Sentencia Tribunal Constitucional. Núm. 196/2004, de 15 de noviembre. Vlex (Rec. 1322/2000). (ECLI:ES:TC:2004:196)

- TRIBUNAL SUPREMO

- Sentencia del Tribunal Supremo. Núm. 518/2012 de 24 de julio de 2012 Vlex (ES:TS:2012:518)
- Sentencia Tribunal Supremo. Sala Primera. Núm 7669/1986 de 4 de noviembre de 1986. Fundamento Jurídico 7º Vlex (ECCLI:ES:TS:1986:7669)

DISPOSICIONES COMUNITARIAS

- Consejo de Europa. (1997). Resolución 509 sobre "Derechos humanos y los nuevos logros científicos y técnicos". <https://www.coe.int/en/web/conventions/full-list/conventions/treaty/209> (Última consulta 13/10/2024)
- Consejo de Europa. (1987). Recomendación R (87) 15 del Comité de Ministros a los Estados miembros dirigida a regular la utilización de los datos de carácter personal en el sector de la policía. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680051f92 (Última consulta 12/09/2024)
- Consejo de Europa. (1999). Recomendación R (99) 5 relativa a la protección de la intimidad en internet. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805bc1a8 (Última consulta 14/09/2024)
- Grupo de Trabajo del Artículo 29. (2009). Dictamen 2/2009 sobre la protección de datos personales de los niños. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp164_es.pdf (Última consulta 13/10/2024)

- Grupo de Trabajo del Artículo 29. (2009). Dictamen 5/2009 sobre las redes sociales. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf (Última consulta 18/06/2024)

RECURSOS DE INTERNET

- Albalegal Abogados. (s.f.). *Historia de la protección de datos*. <https://www.albalegal.es/historia-de-la-proteccion-de-datos/> (Última consulta 18/09/2024)
- The Social Media Family. (s.f.). *IX-INFORME-RRSS-THESMF.pdf*. <https://thesocialmediafamily.com/IX-INFORME-RRSS-THESMF.pdf> (Última consulta 18/09/2024)
- Agencia Española de Protección de Datos (AEPD). (2020). *Nota técnica sobre la protección del menor en Internet*. <https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteccion-del-menor-en-internet.pdf> (Última consulta 8/10/2024)
- El informe sobre las tendencias digitales, redes sociales y mobile <https://wearesocial.com/es/blog/2022/01/digital-report-2022-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/> (Última consulta 4/10/2024)
- Demografía de Instagram en 2022: las estadísticas más importantes <https://blog.vtutor.com/es/marketing-digital/demografia-de-instagram-en-2022-las-estadisticas-mas-importantes/> (Última consulta 5/10/2024)
- Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI). (2022). *El uso de las tecnologías por los menores en España*. <https://www.ontsi.es/es/publicaciones/uso-nuevas-tecnologias-menores-Espana-2022> (Última consulta 10/10/2024)
- COBO, I. (2018, 3 de octubre). Hijos de famosos: pixelados en los medios pero hiperexpuestos en las redes sociales. El Mundo, <https://www.elmundo.es/loc/famosos/2018/10/03/5badfd68268e3e88488b45fd.html> (Última consulta 09/10/2024)
- Derechos ARCO [Derechos ARCO ¿Qué son? Nuevos derechos del RGPD \(ARSULIPO\) \(protecciondatos-lopd.com\)](https://protecciondatos-lopd.com/) (Última consulta 11/07/2014)
- Guía para centros educativos. <https://www.aepd.es/es/documento/guia-centros-educativos.pdf> (Última consulta 18/09/2024)

- Guías para menores <https://www.aepd.es/guias/estrategia-menores-aepd-lineas-accion.pdf> (ultima consulta 12/10/2024)
- Guías para la privacidad y seguridad en Internet <https://www.aepd.es/guias/guia-privacidad-y-seguridad-en-internet.pdf>
- Gutiérrez Mayo, E. (2020). El fiscal como protector de la privacidad de los menores. Lawyerpress. <https://www.lawyerpress.com/2020/05/06/el-fiscal-como-protector-de-la-privacidad-de-los-menores/> (Última Consulta 23/09/2024)
- Redacción Depor a 24 de noviembre de 2019. Obtenido de <https://depor.com/depor-play/tecnologia/la-ley-coppa-en-youtube-que-es-como-afectara-a-los-canales-y-todo-sobre-la-polemica-de-la-nueva-regulacion-estados-unidos-usa-nnda-nnlt-noticia/> (Última consulta 24/09/2024)
- Canal del ciudadano AEPD: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciaciudadano/index-ides-idphp.php> (Última Consulta 12/10/2024)
- Protección del menor en Internet (aepd.es) <https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteccion-del-menor-en-internet.pdf> (Última consulta 8/10/2024)
- ¿Deben los padres publicar fotos de sus hijos en las redes sociales? (30 de marzo de 2017). Europa Press. <https://www.europapress.es/portaltic/socialmedia/noticia-deben/padres-publicar-fotos-hijos-redes-sociales-20161107085948.html> (Última consulta 27/09/2024)
- Aprobado el Reglamento europeo de Protección de Datos: nuevas reglas adaptadas a la era digital · Noticias Jurídicas (juridicas.com) <https://noticias.juridicas.com/actualidad/noticias/11018-aprobado-el-reglamento-europeo-de-proteccion-de-datos:-nuevas-reglas-adaptadas-a-la-era-digital/> (Última consulta 01/07/2024)
- Pagina Agencia Española de Protección de Datos: <https://www.aepd.es/> (Última consulta 12/07/2024)
- Página web Tú decides en Internet- Jóvenes <https://www.tudecideseninternet.es/> (Última consulta 13/07/2024)

- Página web del Instituto Nacional de Ciberseguridad <https://www.incibe.es/> (Última consulta 13/07/2024)
- Página web del Ministerio de Educación y Formación Profesional <https://www.educacionfpydeportes.gob.es/> (Última consulta 13/07/2024)
- Página web del Comité Europeo de Protección de Datos https://www.edpb.europa.eu/role-edpb_es (Última consulta 13/07/2024)
- Página web de la Organización para la Cooperación y el Desarrollo Económicos <https://web-archive.oecd.org/espanol/index.htm> (Última consulta 13/09/2024)
- Página web de la Organización de las Naciones Unidas <https://www.un.org/es/> (Última consulta 13/07/2024) (Última consulta 13/07/2024)