Vulnerabilidades de la infancia y adolescencia en las redes sociales y sus repercusiones jurídico-civiles

Paola Zouak Lara

Red de Universidades por la Infancia y la Adolescencia

CÁTEDRA DE INFANCIA Y ADOLESCENCIA
UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Vulnerabilidades de la infancia y adolescencia en las redes sociales y sus repercusiones jurídico-civiles

Paola Zouak Lara

edUPV
Universitat Politècnica de València

Citar como:

Zouak Lara, Paola. (2025). *Vulnerabilidades de la infancia y adolescencia en las redes sociales y sus repercusiones jurídico-civiles.* Valencia: Editorial Universitat Politècnica de València. https://doi.org/10.4995/2025.684401

Esta obra ha sido galardonada con el XI Premio de investigación sobre la infancia y la adolescencia otorgado por la Cátedra de infancia y adolescencia de la Universitat Politècnica de València y la Red de Universidades por la Infancia y Adolescencia

Edición a cargo de la Cátedra de infancia y adolescencia. Director: Vicente Cabedo Mallol

Autoría: Paola Zouak Lara

Editorial Universitat Politècnica de València, 2025
Distribución: www.lalibreria.upv.es / Ref.: 6844_01_01_01

Diseño y maquetación: Enrique Mateo | Triskelion disseny editorial

ISBN: 978-84-1396-346-4 (versión electrónica)
ISBN: 978-84-1396-300-6 (versión impresa)
DOI: https://doi.org/10.4995/2025.684401

AUTORA

Paola Zouak Lara

Graduada en Derecho por la Universidad de Granada (UGR) en 2023, finalizó sus estudios de Máster en Derecho de los Negocios en la misma la universidad en 2024. Durante su carrera investigadora ha sido becaria de colaboración y de investigación en el Departamento de Derecho Civil de la UGR. Ha obtenido diversos premios, entre los que destacan el Premio Ángel Olavarría Téllez de «Estudios Jurídicos», XIII edición; el Premio Extraordinario del Grado en Derecho 2022-2023, de la UGR; Premio Ossorio Morales al mejor Trabajo Final de Grado (TFG) de la UGR curso 2022-2023; o el Premio al Talento del Estudiantado para el Inicio de la Investigación otorgado por la UGR. Actualmente es contratada FPU en el Departamento de Derecho Civil y doctoranda.

RESUMEN

Son múltiples los estudios que se han realizado sobre los menores y las redes sociales. Sin embargo, en esta investigación se plantea un abordaje integral, analizando desde cuestiones clásicas como trasgresiones al derecho al honor, a la intimidad personal y familiar y a la propia imagen de la infancia y la adolescencia, hasta la sobreexposición de la infancia por sus progenitores en las redes sociales (*sharenting*), pasando por la creación de la figura del *kidfluencer* y otras cuestiones de actualidad, como las últimas novedades en materia de publicidad encubierta y creación de perfiles digitales o protección de datos personales desde una doble perspectiva: el niño como sujeto de protección y la persona menor de edad como posible vulneradora del derecho de protección del que son titulares otros adolescentes.

AGRADECIMIENTOS

Trabajo realizado en el marco del Proyecto de I+D+I financiado por el MICIN «Robótica, Inteligencia Artificial y Mayores: oportunidades y desafíos» (PID2023-1514410B-I00), dirigido por Inmaculada Sánchez Ruiz de Valdivia y María del Carmen García Garnica. PID2023-151441OB-I00.

Trabajo realizado como parte del Contrato Predoctoral concedido por el Ministerio de Ciencia, Innovación y Universidades.

ÍNDICE

ÍNDICE DE ABREVIATURAS

Cc.	Código civil
CE	Constitución española
CDN	Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989 Convenio de Derechos del Niño
LCD	Ley 3/1991, de 10 de enero, de Competencia Desleal
LGDCU	Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (Ley General para la Defensa de Consumidores y usuarios)
LOPD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
RBIbis	Reglamento (UE) Nº 1215/2012 del Parlamento Europeo y del Consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Reglamento Bruselas I bis)
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
RRI	Reglamento (CE) Nº 593/2008 del Parlamento Europeo y del Consejo de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales (Roma I) Reglamento Roma I
SAN	Sentencia de la Audiencia Nacional
STC	Sentencia del Tribunal Constitucional

STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea

INTRODUCCIÓN

La omnipresencia de Internet en la vida de la infancia y la adolescencia ha dado lugar a la creación de un ecosistema perfecto para el surgimiento de nuevos riesgos para estos seres que se encuentran en una situación de vulnerabilidad. Los niños y niñas de nuestra generación son por nacimiento nativos digitales, lo que supone una normalización del uso de las nuevas tecnologías en todos los aspectos de sus vidas. No es de extrañar que en este contexto hayan surgido personas que han visto la oportunidad perfecta para hacer de las redes sociales una nueva forma de trabajo.

Lo cierto es que los españoles pasan de media dos horas y media al día consultando y navegando por sus redes sociales, usándolas incluso como un medio de comunicación y, en concreto, de entre los jóvenes de 16 a 24 años, el 74% afirma seguir a los llamados *influencers* en sus redes sociales. Este fenómeno supone *a priori* la apertura de una cuenta en una red social por el niño o niña, la navegación por la red social y las consecuencias que a veces pueden derivarse, como la compra dentro de la red de un producto o el hartazgo hasta el cierre de la cuenta.

Esta nueva herramienta de las redes sociales puede tener consecuencias negativas para estas personas que se encuentran en formación y aún son muy influenciables. De hecho, que pertenezcan a generaciones nacidas en la era digital no significa que los niños, niñas y adolescentes estén preparados para enfrentarse a los riesgos que el uso de las nuevas tecnologías lleva consigo. Es por ello por lo que nuestro legislador ha ido configurando nuevos derechos para intentar proteger de una manera u otra a nuestros nativos digitales. Derechos tales como la protección de datos, el derecho de oposición o el derecho a la información, que son de creación relativamente reciente, traen su causa en la necesidad de protección frente a riesgos de los que no son conscientes esos jóvenes que solo desean comunicarse con sus amistades, oír música, visualizar vídeos y seguir a sus ídolos.

Sin embargo, estas iniciativas parecen no ser suficientes, ya que las empresas monopolizadoras de las redes sociales ingenian nuevos métodos para intentar burlar los estándares de protección que intenta instaurar la Unión Europea (en adelante, UE), lucrándose de un modo u otro del mayor dorado existente en la actualidad: el poder de los datos. Es así como se ha creado una nueva fuente de ingresos, que en un principio era invisible y que ahora se encuentra cada vez más patente en los servidores de Internet: la publicidad comportamental, creadora de un perfil online del usuario con la finalidad de dirigirle publicidad personalizada. Para ello será necesario vender los datos obtenidos en una determinada red social o motor de búsqueda a una empresa que los usará para dirigirlos a marcas concretas.

Ahora bien, ¿se encuentran los niños, niñas y adolescentes amparados por la red de protección creada por la Unión Europea? ¿Son conscientes estas personas de los mecanismos que ofrece el Derecho para protegerse ante los posibles agravios que les causen las injerencias en su privacidad? ¿Y si son los padres los que comienzan con un ataque directo a sus derechos de la personalidad, exponiéndolos en las redes sociales?[1] ¿Qué mecanismos de defensa existen contra los *influencers* que, aprovechándose de su papel idealizado venden productos que resultan no ser tan maravillosos? ¿Puede acaso el adolescente vencer en un juicio contra una empresa sita en China? ¿Ante qué tribunal deberá interponerse una demanda en situaciones transfronterizas de violación de derechos?

Múltiples son las cuestiones que se tratarán a lo largo de esta investigación, siendo el objeto de la misma las vulnerabilidades con las que se encuentran los niños y niñas, adolescentes y jóvenes en las redes sociales desde una perspectiva jurídico-civil, como sujetos titulares de diversidad de derechos conferidos en sede nacional y europea. El

[1] LÓPEZ VILLAFRANCA, P. y OLMEDO SALAR, S., "Menores en YouTube, ¿ocio o negocio? Análisis de casos en España y EUA", *El profesional de la información*, vol. 28, núm. 5, 2019, p. 2.

objetivo de la investigación es analizar si existen respuestas normativas o jurisprudenciales que logren proteger a estos sujetos de las diferentes injerencias que se puedan encontrar durante la creación de la red social, el desarrollo y disfrute de la misma y finalmente con su cierre.

La Convención de Derechos del Niño (en adelante, CDN)[2] en su artículo 16 recoge el derecho de los niños a no ser objeto de injerencias ilegales o arbitrarias en su vida privada, su familia, su honra o reputación, reconociéndoles el derecho a la protección de la ley contra esas injerencias. Para ello, se hace necesario en este trabajo el abordaje de esta cuestión desde una perspectiva integral, analizando desde cuestiones clásicas como trasgresiones al derecho al honor, a la intimidad personal y familiar y a la propia imagen de la infancia y la adolescencia, hasta la sobreexposición de la infancia por sus progenitores en las redes sociales (*sharenting*), pasando por la creación de la figura del *kidfluencer* y otras cuestiones de actualidad, como las últimas novedades en materia de publicidad encubierta y creación de perfiles digitales o protección de datos personales, desde una doble perspectiva: el niño, niña o adolescente como sujeto de protección y la persona menor de edad como posible vulneradora del derecho de protección del que son titulares otros adolescentes.

Dentro del ámbito de la protección de datos se abordarán cuestiones como el tratamiento de datos y su licitud, los derechos de los niños, niñas, adolescentes y jóvenes en las redes sociales, el régimen de responsabilidad y la cuantificación del daño cuando se ha incumplido la normativa de protección de datos y algunas cuestiones prácticas, como el famoso caso META, que aportará luz sobre nuevos conceptos e interpretaciones del derecho a la protección de datos.

[2] Disponible en el siguiente enlace: https://www.unicef.es/sites/unicef.es/files/comunicacion/ConvencionsobrelosDerechosdelNino_0.pdf

Al ser actualmente muy habitual que los propios *influencers* publiciten productos como parte de campañas que firman con grandes marcas, los principales receptores de dicha publicidad serán sus seguidores, público infantil y juvenil que no conoce las herramientas que ofrece el Derecho para defenderse ante productos que no cumplen con dichas expectativas. Cuestión que también se tratará, al igual que cuando los *influencers* son los propios jóvenes que llegan con sus mensajes a otros niños o niñas con sus vídeos atractivos. En este último caso, ¿serán los padres los que deberán responder por los daños que puedan causar sus hijos e hijas?

No debemos dejar de lado la ubicuidad que caracteriza la red. De este modo, a título ilustrativo, la sede de Twitter se encuentra en San Francisco (California, Estados Unidos); la de Tik Tok en Beijing (China); la de Instagram en California (Estados Unidos). Sin embargo, los usuarios de la red se encuentran distribuidos por todo el mundo, siendo sus edades muy dispares. ¿Deberá dirigirse el niño o niña, si ocurre alguna disputa, a un tribunal extranjero? ¿Qué mecanismos de defensa existen en sede europea para averiguar ante qué tribunal debe interponerse la demanda y qué ley será la que aplicará el juez?

Para poder estudiar estas cuestiones ha sido necesario realizar un abordaje interdisciplinar, combinando el Derecho civil con el Derecho internacional privado, que resulta esencial para poder tener una perspectiva amplia de toda la problemática que está surgiendo actualmente con estas cuestiones.

El planteamiento integral que persigue esta investigación partirá de la utilización de una metodología propia de las Ciencias jurídicas, analizando la jurisprudencia del Tribunal Supremo (en adelante, TS) español al respecto, la del Tribunal Constitucional (en adelante, TC) y también la jurisprudencia emanada del Tribunal de Justicia de la Unión Europea (en adelante, TJUE). Asimismo se estudiará la legislación actual a nivel nacional y europeo, para tener una perspectiva completa sobre la regulación de todos los problemas que identifiquemos; y se contrastará la

doctrina más autorizada sobre la materia para entender la interpretación actual sobre conceptos, preceptos y teorías, además de la identificación de fallos que se puedan apuntar en el sistema actual.

No constituye esta investigación una mera revisión de otros trabajos, sino que a lo largo de la misma se irán realizando propuestas que, desde mi punto de vista, pueden hacer avanzar el conocimiento jurídico y ofrecer soluciones a algunos de los problemas analizados. Las justificaciones que se irán desarrollando a lo largo de este estudio serán de índole teorética, mediante argumentos jurídicos respaldados por juristas de gran prestigio. Finalmente, se concluirá con una propuesta de *lege ferenda*, que podría contribuir a mejorar el panorama normativo en vigor, en aras de una potenciación de la protección digital de nuestros jóvenes.

EL FENÓMENO DE LAS REDES SOCIALES Y SU ACCESO A ELLAS POR LA INFANCIA Y ADOLESCENCIA

Las redes sociales se definen como plataformas de comunicación en línea que permiten a sus usuarios entablar contacto con personas que acceden a las mismas y compartir contenidos con ellas.[3] A pesar de que su origen se remonta a 1995, con la plataforma "classmates.com", lo cierto es que las redes sociales han experimentado un avance exponencial, especialmente desde el surgimiento de Facebook, que marcó un antes y un después, al permitir conectar a personas de todo el mundo que se podían comunicar y subir contenido visual para mantenerse al tanto de las novedades que acontecían en sus vidas. A pesar de que esta red social actualmente solo se utilice por personas de edad adulta, se han ido desarrollando otras plataformas que tienen popularidad entre los jóvenes y que cumplen un papel similar (Instagram, Tik Tok...). Según su forma de funcionar o los intereses de los usuarios, existen multiplicidad de tipos de redes sociales.

Por una parte, nos encontramos con la división en dos grupos fundamentales: las redes generalistas o de ocio, cuya finalidad es permitir la interacción entre sus miembros, entre las que se engloban plataformas tales como Facebook, Instagram o Tik Tok; y las profesionales, que pretenden poner en contacto a sus usuarios con fines puramente profesionales, como es el caso de LinkedIn.

Por otra parte, hay doctrina que las clasifica en atención al público y la temática de la propia red social, dividiéndolas en redes sociales horizontales, que son aquellas que no han sido creadas con ninguna finalidad ni para ningún tipo de usuario concreto, sino que abarcan un

[3] MORALEJO IMBERNÓN, N., *Los derechos de los menores y las redes sociales. Incluye Reglamento (UE) 2022/2065, del Parlamento Europeo y del Consejo, de 19 de octubre, de Servicios Digitales*, Tirant lo Blanch, Valencia, 2023, p. 13.

perfil general, pudiendo interactuar todos los usuarios, como es el caso de Twitter o Facebook; y redes sociales verticales, que son aquellas que se dirigen a un público muy concreto o que se han creado para cubrir una necesidad determinada. Dentro de esta tipología, dependiendo del público, se pueden dividir en redes sociales verticales profesionales, dirigidas a intercomunicar a profesionales; redes sociales verticales de ocio, dirigidas a unir a usuarios con aficiones comunes, ya sea el deporte, la música o el arte, como Depormeet o Dogster; o a permitir conocer a personas afines o amigos, como Tinder o Badoo. Finalmente, nos encontramos con las redes sociales verticales mixtas, que combinan tanto la faceta lúdica como la profesional.[4]

Sin embargo, tal y como señaló el Grupo de Trabajo sobre Protección de Datos del artículo 29, en su Dictamen 5/2009 sobre redes sociales en línea,[5] independientemente del grupo al que pertenezcan, todas ellas presentan una serie de características comunes:

- En todas ellas los usuarios deben compartir datos personales para crear su propio perfil.
- Se ponen a disposición de los usuarios herramientas para que puedan compartir contenido en línea, como fotografías, vídeos, música, comentarios…
- Obtienen la mayor parte de sus ingresos de la publicidad que alojan en la plataforma y a la que los usuarios pueden acceder posteriormente.

[4] GARCÍA GARNICA, M.C., "Responsabilidad civil y redes sociales. Especial consideración a los daños sufridos o causados por menores de edad", en LÓPEZ Y GARCÍA DE LA SERRANA, J., (dir.), *XXI Congreso Nacional sobre responsabilidad civil y seguro*, Sepín, Sevilla, 2021, p. 90.

[5] Disponible en el siguiente enlace: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf p. 5.

- El usuario tiene una lista de amigos o contactos, que pueden acceder a su contenido e interactuar con él.[6]

Todas estas características hacen que el propio concepto de "red social" resulte cada vez más atractivo. Tanto es así, que el medio de comunicación principal de la infancia y la adolescencia a día de hoy son las redes sociales, que no solo se utilizan como una vía para mantenerse al día o una herramienta de trabajo, sino que se perciben como una forma alternativa de ampliar el círculo social.

Si analizamos el funcionamiento de las plataformas digitales nos daremos cuenta de las ventajas que otorga a los más jóvenes la utilización de esta herramienta como método para conocer gente en el día a día. Para ello, es necesario realizar un símil entre el mundo real y el mundo virtual, de modo que, al igual que las personas adolescentes tienen su propio grupo de amistades reales, en el entorno digital estos amigos también existen, pero multiplicados por cien, ya que la red permite tener contacto con personas de múltiples lugares del mundo, lo cual es muy deseado por estos jóvenes, dado que el hecho de tener una larga lista de seguidores es símbolo de popularidad y éxito entre la población juvenil. Al ser tan sencillo, en ciertas redes, como darle al botón de seguir o aceptar que una persona los siga con un simple "click", no es de extrañar que el número de usuarios amigos en las redes sociales roce números astronómicos, con el consiguiente riesgo que ello supone.

Siguiendo a MORALEJO IMBERNÓN, esta apertura de los más jóvenes al mundo de las redes sociales puede dar lugar a multiplicidad de riesgos. En primer lugar, nos encontramos con los comentarios que los usuarios pueden alojar en las plataformas, que pueden tener una repercusión claramente negativa en personas que aún se están desarrollando, o la necesidad voraz de conseguir un "me gusta" en las publicaciones, ya que, de modo contrario, sería considerado un fracaso absoluto pasar desapercibido. En segundo lugar, la utilización de las redes sociales

[6] MORALEJO IMBERNÓN, N., *Los derechos de los menores… op cit*., p. 14.

genera la falsa creencia de que existen vidas ideales, debido a que, normalmente, solo se muestran las fiestas a las que se asiste, los viajes, las salidas, los momentos más felices vividos… provocando un sentimiento de angustia o vacío en los adolescentes y jóvenes, que ven cómo sus vidas no se parecen a lo que otras personas están mostrando. Este fenómeno recibe el nombre de "*toxic positivity*" y tiene una repercusión negativa en los niños y niñas, adolescentes y jóvenes que utilizan redes de ocio. En tercer lugar, la propia configuración de las redes sociales hace que el algoritmo vaya perfilando los intereses de las personas menores de edad, que pueden tener acceso a contenido que no es propio de su edad, de modo que personaliza las publicaciones que se muestran, obteniendo datos en función del tiempo que se detienen en una publicación o si han señalado que les ha gustado algo, sin tener la plataforma ningún tipo de control de edad al respecto.[7]

Lo cierto es que todos estos riesgos surgen cuando el niño, niña o adolescente ha abierto una cuenta en una red social y empieza a navegar en la misma. El elemento clave para empezar a abordar esta cuestión reside en el consentimiento, que opera en un doble sentido: el consentimiento para formalizar el contrato con la red social en sí (consentimiento del menor para abrir la red social y crearse un perfil) y el consentimiento para el tratamiento de los datos personales del niño, niña o adolescente (una vez se ha abierto la red social y durante el proceso de creación del usuario, que comprende la facultad para poder guardar información sobre la huella digital que va dejando el joven en la red social cada vez que le da a "me gusta" o hace una búsqueda en internet o hace algún comentario en alguna publicación).

[7] MORALEJO IMBERNÓN, N., *Los derechos de los menores… op cit*., p. 15.

1. El consentimiento del niño o niña para abrir un perfil en una red social

Teniendo esto en cuenta, debemos plantearnos que cuando una persona menor de edad abre una cuenta en una red social está formalizando una relación contractual. Procede estudiar la viabilidad o validez del contrato perfeccionado, para lo cual deben concurrir los elementos esenciales de cualquier contrato (art. 1261 del Código Civil, en adelante Cc): consentimiento, objeto y causa. Por lo que a nosotros nos interesa, nos detendremos exclusivamente en el consentimiento. Para que se emita un consentimiento válido de acuerdo con nuestra normativa civil es necesario que la persona tenga capacidad suficiente (que antes se denominaba capacidad de obrar plena),[8] es decir, la aptitud que poseen las personas mayores de edad para realizar actos jurídicos. Sin embargo, existen ocasiones en las que dicha capacidad no es plena, sino que presenta ciertas limitaciones, como es el caso de las personas menores de edad y de las personas con discapacidad, que necesitan de la designación de una institución jurídica que complemente, apoye o simplemente asista su propia capacidad para tomar decisiones. A esto se le suma que el artículo 1256 del Código Civil prevé que para que el consentimiento sea válido, no puede concurrir ningún vicio como pueden ser el error, la violencia, la intimidación o el dolo.

Por lo tanto, para que una persona menor de edad pueda ser usuario en una red social, este deberá otorgar válidamente su consentimiento. Sin embargo, por sí mismos, como ya hemos apuntado, los niños, niñas y adolescentes no tienen capacidad para emitirlo, sino que, *a priori*, necesitarán del complemento de la representación de sus progenitores,

[8] Esta expresión fue reformada con la entrada en vigor de la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica. *BOE* núm. 132, de 3 de junio de 2021.

tal y como establece el artículo 162 del Código Civil (por tratarse de padres o madres que ostentan la patria potestad y tienen la representación legal de sus hijos e hijas menores no emancipados).

Sin embargo, esta regla se encuentra matizada, ya que, al tratarse de menores, deberemos acudir al artículo 1263 del Código Civil, que prevé, precisamente respecto a los menores de edad no emancipados, la posibilidad de celebrar por sí mismos aquellos contratos que las leyes les permitan realizar por sí mismos relativos a servicios de la vida corriente propios de su edad conforme a los usos sociales. La doctrina ya ha señalado en reiteradas ocasiones su posición favorable a considerar que la apertura de redes sociales supone actualmente una actividad común entre nuestros jóvenes,[9] lo que hace que la infancia y adolescencia podría celebrar el contrato de apertura de un perfil en una red social por sí mismas, atendiendo a la madurez suficiente que posean estas personas, siempre y cuando se cumplan las exigencias establecidas en la normativa específica en materia de protección de datos, que estudiaremos a continuación.

2. El consentimiento del niño o niña para el tratamiento de sus datos personales en las redes sociales

La siguiente cuestión que debemos plantearnos es cuándo se supone que la infancia y adolescencia puede tener acceso a la utilización de las redes sociales y desde qué edad se permite el tratamiento de sus datos personales de acuerdo con la normativa específica (consentimiento para el tratamiento de los datos personales). Debemos partir del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo

[9] En este sentido: TORAL LARA, E., "Menores y redes sociales: consentimiento, protección y autonomía", *Derecho Privado y Constitución*, núm. 36, 2020, pp. 195-197; AYLLÓN GARCÍA, J.D., "Consentimiento de los menores de edad en las redes sociales: especial referencia a TikTok", *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, p. 587; BATUECAS CALETRIO, A., "Intimidad personal, protección de datos personales y geolocalización", *Derecho Privado y Constitución*, núm. 29, 2015, p. 68.

de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento General de Protección de Datos o RGPD).[10] Este instrumento normativo dispone en su artículo 8.1 que se considera lícito el consentimiento sobre el tratamiento de datos personales de un niño[11] cuando se le oferta directamente servicios de la sociedad de la información siempre que tenga como mínimo 16 años. En caso de que el menor tenga menos de 16 años, solo se considera lícito si el consentimiento lo otorgó el titular de la patria potestad o el titular de la tutela del menor. Sin embargo, el propio precepto continúa autorizando a los Estados miembros para que establezcan dentro de su propia normativa por ley una edad inferior a los 16 años, siempre con el límite mínimo de los 13 años. El precepto finaliza añadiendo que el responsable del tratamiento de los datos debe realizar un esfuerzo razonable para verificar que, en esos casos, el consentimiento ha sido autorizado por el titular de la patria potestad o tutela del niño, teniendo en cuenta la tecnología disponible.

En el caso de España, el legislador ha tenido tendencia a ser partidario de rebajar la edad del consentimiento de las personas menores por debajo de los 16 años, al menos hasta recientemente. Ya el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[12] preveía en su artículo 13 una serie de circunstancias para que los menores de 14 años pudieran otorgar su consentimiento por sí mismos para el tratamiento de los datos personales, a excepción de los casos en que la ley exigiera expresamente la asistencia de los titulares de la patria potestad o tutela. Por

[10] *DOUE* L 119, de 4 de mayo de 2016.

[11] La expresión "niño" para abarcar a la infancia y la adolescencia, utilizada en el Reglamento, está comenzando a modificarse en las normas más recientes en materia de protección de datos y servicios digitales, como ya veremos.

[12] *BOE* núm. 17, de 19 enero de 2008.

ejemplo, no era posible obtener datos de menores sobre información sensible, como puede ser información sobre el grupo familiar, las características del mismo, datos sociológicos, información económica… (art. 13.2 LOPD). Por lo tanto, preveía los 14 años como la edad mínima para poder otorgar eficazmente el consentimiento respecto al tratamiento de los datos personales.

Sin embargo, en el año 2017, se redactó el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, que fue criticado por el Dictamen del Consejo de Estado, en forma de Informe preceptivo de 4 de agosto de 2017,[13] ya que el artículo 8 de la primera versión del Anteproyecto contemplaba la reducción de la edad mínima de los menores para el tratamiento de sus datos a 13 años. Esta primera versión también fue duramente criticada por la doctrina, que señalaba que esta edad no proporcionaba suficiente protección a las personas menores, aún inmaduras.[14] Resultó llamativo cómo en sede europea se facilitaba una opción estatal de establecimiento de una edad diferente, concretamente entre la horquilla de 14 a 16 años y el legislador español, que ya había previsto conforme al Real Decreto 1720/2007 admitir el consentimiento a partir de los 14 años, quería incluso reducir dicha edad a los 13 años, infringiendo las indicaciones europeas y poniendo en riesgo a niños y niñas que podrían haberse visto expuestos a los peligros antes señalados sin razón aparente.

[13] Disponible en el siguiente enlace: https://www.mjusticia.gob.es/va/AreaTematica/ActividadLegislativa/Documents/1292428594738-PLOPD_MAIN_anexo_4_Informes_preceptivos.PDF

[14] En este sentido lo señalaban, MORELAJO IMBERNÓN, N., *Los derechos de los menores y las redes sociales… op cit*., p. 27; NAVARRO ORTEGA, A., y DURÁN RUIZ, F.J., "La protección jurídico-administrativa del menor y frente al menor en redes sociales y servicios de mensajería instantánea", en DURÁN RUIZ, F.J. (dir.), *Desafíos de la Protección de menores en la sociedad digital. Internet, redes sociales y comunicación*, Tirant lo Blanch, Valencia, 2018, p. 359.

Finalmente, la propuesta del Anteproyecto no triunfó y se aprobó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales[15] (en adelante, LOPD), cuyo artículo 7 dispone que "El tratamiento de datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de 14 años". Por debajo de esta edad será requerido el consentimiento del titular de la patria potestad o tutela.

No obstante, el legislador español está dando un giro a su política legislativa en aras de una mayor protección a la infancia y adolescencia. En este sentido, existe un nuevo Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales,[16] que ha sido aprobado el 4 de junio de 2024 y que volverá a modificar la LOPD, afectando al ámbito concreto de los menores de edad. La finalidad del Anteproyecto de Ley Orgánica es establecer medidas para garantizar la protección de las personas menores de edad en los entornos digitales (art. 1). Para ello, les reconoce una serie de derechos en el artículo 2, tales como el derecho a ser protegidas ante contenidos digitales que puedan perjudicar su desarrollo (art. 2.1), el derecho a recibir información suficiente y necesaria en un lenguaje y forma apropiado a su edad sobre el uso de las tecnologías y sus riesgos (art. 2.2), el derecho a la información, la libertad de expresión y a ser escuchadas (art. 2.3.) y el derecho al acceso equitativo y efectivo a dispositivos, conexión y formación para el uso de herramientas digitales (art. 2.4). Además, resulta de especial interés que este nuevo Anteproyecto parece haber atendido a las críticas doctrinales, ya que en su Disposición Adicional quinta contempla la modificación del artículo 7 de la Ley Orgánica de Protección de Datos, elevando la edad de otorgamiento del consentimiento de los menores a 16 años.

---

[15] *BOE* núm. 294, de 6 de diciembre de 2018.

[16] Disponible en el siguiente enlace: https://www.mpr.gob.es/servicios/participacion/audienciapublica/Documents/VSGT%202024/2024-0921%20APLO%20menores%20entornos%20digitales/MAIN.pdf

Por lo tanto, a modo de recapitulación, con arreglo a la normativa actualmente en vigor en España, para que un menor de edad pueda abrirse un perfil en las redes sociales, de conformidad con la normativa de protección de datos, solo existen dos opciones: que sea mayor de 14 años y él mismo se registre y otorgue su consentimiento (a la espera de lo que acontezca con el Anteproyecto); o que, siendo menor de 14 años, sean sus representantes legales los que le abran la cuenta en las redes sociales y consientan el tratamiento de sus datos. Fuera de estos dos supuestos, el consentimiento carecerá de la validez necesaria.

Llegados a este punto surgen diversas críticas de índole doctrinal. En primer lugar, se plantea la adecuación de esta edad para que un joven pueda acceder a una red social teniendo en cuenta el contenido que se puede ofrecer en la misma y los derechos que se encuentran involucrados (intimidad, imagen, honor, privacidad, protección de datos).

En segundo lugar, también es objeto de discusión el sistema de verificación de la edad por parte de las plataformas. El artículo. 8.2 del Reglamento General de Protección de Datos prevé que el responsable del tratamiento de los datos deberá hacer "esfuerzos razonables" para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.[17] Por lo tanto, como podemos observar el responsable de comprobar la autenticidad de la verificación de la edad es el responsable del tratamiento de datos (que será la red social o plataforma), dado que, de no hacerlo, el tratamiento de datos de menores edad sin

[17] Critican esta obligación impuesta por el Reglamento HERRERA DE LAS HERAS, R. y PAÑOS PÉREZ, A., *La privacidad de los menores en redes sociales. Especial consideración al fenómeno influencer*, Atelier, Barcelona, 2022, p. 60, al señalar que: "la comprobación fehaciente de la identidad de aquel que presta el consentimiento no se configura como una obligación para el prestador de servicios, sino como una sugerencia o deseo al referirse a la necesidad de que haga únicamente "esfuerzos razonables".

su consentimiento válidamente otorgado, según el art. 73 de nuestra Ley Orgánica de Protección de Datos, será calificado como infracción grave.[18]

Al igual que en el RGPD, la exigencia de que los responsables del tratamiento de los datos asuman un papel activo en la comprobación de la edad de las personas que acceden a sus cuentas y de la prestación válida del consentimiento, también viene prevista en otros ordenamientos jurídicos. Así, la *Children's Online Privacy Protection Act*[19] de Estados Unidos, prevé la inclusión de métodos de verificación en los siguientes términos, solicitando que "el operador realice esfuerzos razonables para obtener un consentimiento paterno verificable, teniendo en cuenta la tecnología disponible. Cualquier método para obtener el consentimiento paterno verificable debe estar razonablemente calculado, a la luz de la tecnología disponible, para garantizar que la persona que da el consentimiento es el padre del niño".

Sin embargo, a pesar de estas declaraciones, no se aportan medidas reales sobre qué tipo de verificación se debe realizar, lo cual resulta criticable. En todo caso, para poder llevar a cabo esta labor de verificación de datos existe una multiplicidad de posibilidades. Una de ellas puede ser la opción de señalar después de la descarga de la aplicación en una página desplegable el año de nacimiento, lo cual no resulta muy efectivo, ya que no existe ninguna comprobación posterior y se puede señalar el año que se desee. Otra posibilidad sería instalar dentro de la red social un programa que detecta en función de las expresiones que se utilizan durante las conversaciones una edad aproximada.[20] Sin embargo, tampoco esta solución ha demostrado gran eficacia, ya que

---

[18] MORALEJO IMBERNÓN, N., *Los derechos de los menores… op cit*., p. 28.

[19] Disponible en el siguiente enlace: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

[20] Este sistema ha sido mencionado por el Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, elaborado en 2009 por INTECO y la AEPD. Disponible en el siguiente enlace: https://www.uv.es/limprot/boletin9/inteco.pdf

es posible alterar el modo de comunicarse de los usuarios mediante un cambio intencionado del estilo de redacción, tanto de jóvenes que puedan aparentar ser mayores de edad, como de mayores de edad que aparenten tener menos años, con el fin de entablar una relación con usuarios más jóvenes por diversas causas, algunas no lícitas, lo cual puede resultar incluso contraproducente. Finalmente podemos encontrarnos con sistemas que solicitan al menor el envío de una copia de su DNI y una fotografía con su imagen; pero, incluso en este caso, los niños y niñas tienen fácil acceso a aplicaciones para poder modificar la fecha de su DNI o incluso obtener el documento de sus padres, fingiendo ser otras personas, por lo que tampoco resulta efectivo. Igualmente podría cuestionarse la licitud de la solicitud por parte de una plataforma de un documento que posee datos sensibles, como los que constan en el DNI.[21]

Teniendo en cuenta los derechos e intereses que están en juego, habría que sopesar, en todo caso, qué interés es el más importante y el que debe protegerse con prioridad, si el derecho a la protección de los datos de los niños, niñas y adolescentes, o el derecho al libre desarrollo de su personalidad, sin sufrir una invasión de contenidos no adecuados para

[21] En este sentido, la Agencia Española de Protección de Datos ya se ha mostrado en diversos informes reacia a la aportación de un DNI como un instrumento de identificación mediante la entrega de copias. A título ilustrativo, en el informe del Gabinete Jurídico núm. 0048/2023, p. 5, se pronunció del siguiente modo: "Es preciso subrayar que la utilización de una copia de un documento de identidad como parte del proceso de autenticación crea un riesgo para la seguridad de los datos personales y puede dar lugar a un tratamiento no autorizado o ilícito, por lo que debe considerarse inadecuada, salvo que sea estrictamente necesario, adecuado y conforme con el Derecho nacional". En esta misma línea en los últimos años la Agencia ha emitido pronunciamientos en los que ha sancionado al responsable de los datos personales por el tratamiento al solicitar una copia del DNI en los siguiente casos; en el Expediente núm. PS/00003/2021 cuando el interesado ejercía el derecho de acceso a la información; en el Expediente núm. EXP202104493 relativo a una consulta sobre los movimientos de una cuenta bancaria; en el Expediente núm. PS/00413/2021 por solicitar una fotografía del DNI del destinatario de un paquete o en el Expediente núm. EXP202302620 por solicitar una copia del DNI para un reembolso en una clínica dental. Información obtenida de la siguiente fuente: https://www.pwc.es/es/newlaw-pulse/regulacion-digital/proporcionalidad-solicitud-copia-dni-interesado.html

su edad y que pueden influir en su desarrollo emocional. Una muy buena opción que permitiría conjugar ambos derechos sería la puesta práctica de la cartera europea de identidad digital. El propósito de la misma es permitir a los usuarios de la misma, utilizar medios de identificación electrónica seguros, con los que se puede acreditar el elemento de la identidad requerido, en este caso, la acreditación de la mayoría de edad, o de la edad exigida, sin tener que dar a conocer ni la fecha de nacimiento, ni el resto de datos que constan en el DNI. Esta es la línea iniciada por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital,[22] que, aunque entró en vigor el 20 de mayo de 2024, establece un plazo progresivo para su plena implantación.

Mientras se desarrolla esta cartera europea de identidad digital y se resuelven los problemas técnicos y jurídicos que puede presentar, se podría considerar la posibilidad de instaurar el sistema Clave para el acceso de menores a las redes sociales. El sistema Clave se utiliza para identificar a los usuarios en relaciones con la Administración española. La idea es que se emplee también como método de autenticación del menor en las redes sociales. Este tipo de herramienta debe ser solicitada por el progenitor del niño o niña, de modo que podría imponerse este sistema de identificación en la plataforma de la red social para poder acceder. De esta manera, los responsables del tratamiento de los datos cumplirían con su obligación de no permitir a las personas menores el acceso a contenidos inadecuados para ellos. Asimismo, el propio Estado se aseguraría de que los menores que acceden tienen verdaderamente el consentimiento de sus padres. Con ello se lograría una colaboración entre las plataformas y el Estado para intentar proteger la seguridad de los jóvenes. Se trataría de una forma de verificación muy

[22] *DOUE* núm. 1183, de 30 de abril de 2024.

sencilla, que interconectaría a los progenitores o representantes legales de los menores con la red social, estableciendo una red de seguridad y control completa.

Es cierto que esto supondría una carga para los responsables legales de los jóvenes, ya que tendrían que dedicar su tiempo a sacar una cita con la Administración y desplazarse hasta la oficina en la que se realizan los trámites. Sin embargo, este pequeño inconveniente reportaría grandes beneficios para los menores, demostrando los progenitores con esta acción su diligencia debida, pues forma parte de la responsabilidad parental la obligación de prevenir riesgos y daños a sus hijos e hijas. Además, esta medida se considera menos intrusiva en la privacidad de los niños, niñas y adolescentes, pues evitaría que los progenitores tuvieran que realizar una labor de vigilancia sobre la actividad de sus descendientes, vigilancia que podría rozar los límites del derecho a la vida privada de las personas menores de edad y constituir una injerencia en su vida privada.[23]

De momento, esta cuestión sigue sin estar resuelta, ya que el acceso de los menores de edad a las redes sociales depende en gran parte de la atención que presten sus padres y madres al respecto y de las medidas que sus progenitores les impongan sobre su utilización; medidas que, en la práctica no suelen ser muy efectivas.

Por lo que respecta a las propias redes sociales, cada una de ellas en sus condiciones de uso contempla diferentes escenarios sobre las normas de acceso relativas a menores de edad. De este modo, tanto Instagram[24] como Facebook[25] prevén que para poder acceder a la aplicación es necesario tener mínimo 14 años. Caso distinto es TikTok,[26]

[23] SAVE THE CHILDREN, *Derechos#sinconexión. Un análisis sobre derechos de la infancia y la adolescencia y su protección en el mundo digital*, Save the Children España, 2024, p. 69. Disponible en el siguiente enlace: https://www.savethechildren.es/sites/default/files/2024-07/Informe_Derechos_SinConexion.pdf

[24] Disponible en el siguiente enlace: https://help.instagram.com/581066165581870/?locale=es_ES

[25] Disponible en el siguiente enlace: https://es-es.facebook.com/legal/terms

[26] Disponible en el siguiente enlace: https://www.tiktok.com/legal/page/row/terms-of-service/es

o Twitter,[27] que rebajan a 13 años la edad mínima para acceder a sus contenidos. Se trata esta cuestión de un hecho controvertido, y más teniendo en cuenta que los estándares de protección de datos en China, sede de TikTok, no son los mismos que se establecen en Europa. Además, estamos ante un caso flagrante de incumplimiento tanto de la normativa europea como nacional, ya que ¿qué clase de esfuerzos razonables está realizando el responsable del tratamiento de datos para comprobar que efectivamente se tiene la edad que se declara? Actualmente, solo se utiliza el desplegable del año de nacimiento y no existen controles posteriores.

Un claro ejemplo de que las plataformas tampoco se toman suficientemente en serio la protección de la infancia y adolescencia en su acceso a las redes son las sanciones que a veces se imponen a las plataformas. La ICO (*Information Commisioner's Office*), que es la autoridad británica de protección de datos ha impuesto a Tik Tok una multa de 12,7 millones de libras por haber permitido que 1,4 millones de niños británicos accedieran a la plataforma en 2020, a pesar de que la propia red social impide la creación de un usuario a los niños de esa edad. La *UK Data Protection Law* de 2022[28] prevé que la edad en la que las organizaciones pueden tratar los datos personales es 13 años, debiendo los menores de 13 años contar con el consentimiento de sus padres. Tik Tok no cumplió con ese deber de contar con el consentimiento paterno/materno, a pesar de que tenía constancia de que personas menores de 13 años accedían a la plataforma, teniendo acceso a contenidos inadecuados. En suma, la red social recopiló sus datos y los usó para rastrearlos y perfilarlos, incumpliendo igualmente las indicaciones legales. Por ello, el comisionado John Edwards puso de manifiesto que se había producido un incumplimiento del Reglamento de Protección de Datos del Reino Unido por las siguientes razones:

---

[27] Disponible en el siguiente enlace: https://x.com/es/tos

[28] Disponible en el siguiente enlace: https://commonslibrary.parliament.uk/research-briefings/cbp-9606/

- Por entender que Tik Tok había prestado sus servicios en Reino Unido a menores de 13 años y que había procesado sus datos personales sin el consentimiento ni la autorización de sus padres.
- Por no haber proporcionado información sobre cómo se utiliza la plataforma, los datos que se recopilan y la finalidad.
- Por no garantizar que los datos personales de los usuarios se tratasen de forma transparente, lícita y justa.[29]

A la vista de lo expuesto, urge que se adopten medidas legales que garanticen la efectividad de los derechos de los niños, niñas y adolescentes en el mundo digital y que las empresas asuman su obligación de diligencia debida en el cumplimiento de las obligaciones que les imponen las normas en aras de respetar, proteger y hacer efectivos los derechos de todos los niños en el entorno digital.[30] Así lo prevé el art. 45 de la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia,[31] cuando impone a las Administraciones públicas la obligación de "adoptar medidas para incentivar la responsabilidad social de las empresas en materia de uso seguro y responsable de Internet por la infancia y la adolescencia", y la de fomentar "en colaboración con el sector privado que el inicio y desarrollo de aplicaciones y servicios digitales tenga en cuenta la protección a la infancia y la adolescencia".

[29] BARBUDO FERNÁNDEZ, C., "La autoridad británica de protección de datos sanciona a TikTok con 12,7 millones de libras por tratar indebidamente datos de menores", *Diario La Ley*, núm. 71, de 2023, pp. 1-2.

[30] COMITÉ DE DERECHOS DEL NIÑO, *Observación General núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital*, CRC/C/GC/25, de 2 de marzo de 2021, párrafo 4. Disponible en el siguiente enlace: https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[31] *BOE* núm. 134, de 5 de junio de 2021.

LA INFANCIA Y ADOLESCENCIA COMO PROTAGONISTA EN LAS REDES: LOS FAMOSOS *KIDSINFLUENCERS* Y EL *SHARENTING*

1. Breve referencia al concepto de *kidinfluencer* y *sharenting*

Teniendo en cuenta las circunstancias que se deben dar para que un niño, niña o adolescente pueda acceder a una red social, el siguiente paso que siguen muchos de los adolescentes y jóvenes en España es el de convertirse en *influencers*. El término *influencer* hace referencia al sujeto que se dedica a subir un determinado contenido en sus redes sociales y que aprovechará su repercusión en la mayoría de las ocasiones para obtener una contraprestación económica a través de contenido publicitario.[32] Esta figura de los creadores de contenido lleva ya un largo recorrido, ya que comenzó con la tendencia en el año 2019 de los niños y niñas a convertirse en *youtubers* (creadores de contenido para la red Youtube), que ya no era concebida por los mismos como una mera red de entretenimiento, sino como una auténtica profesión, capaz de ser generadora de ingresos.[33]

Esta situación cambió en el año 2021, cuando los jóvenes empezaron a ver las redes sociales en su conjunto como un nuevo nicho de mercado, pasando a querer ser *influencers,* sin plantearse claramente los riesgos que esa exposición pública puede generar en personas de su edad y el papel que cumplen los padres y madres en el contenido que suben a las redes sociales sus hijos e hijas. Conceptualizando ahora a

[32] PLATERO ALCÓN, A., *Repercusiones jurídico-civiles de la actividad de los 'influencers' digitales. Especial consideración de la publicidad encubierta*, Dykinson, Madrid, 2023, p. 36.

[33] RAMOS SERRANO, M., y HERRERO DIZ, P., "Menores y YouTube: el fenómeno de los pequeños *influencers*", en MÁRTINEZ GARCÍA, A., *Imágenes de la infancia en la Comunicación y la Cultura*, Fragua, Madrid, 2022, pp. 287-288.

los *kidsinfluencers*, estos son *influencers* de unas edades comprendidas entre los 3 y los 14 años que dedican sus redes sociales a subir contenido dirigido exclusivamente a un público de una edad similar a la de ellos, siendo los directores de sus vídeos los propios padres y madres, o siendo los progenitores los que supervisan el contenido, la edición o la publicación, convirtiéndose en figuras a seguir por su público.[34]

En relación con el tipo de contenido que suele subir la infancia y adolescencia, este es variado, pero se caracteriza por el afán de intentar incluir a los seguidores en la actividad que van desarrollando, para lo cual utilizan un lenguaje sencillo, ingenioso, con humor, retos, rutinas y muestran productos patrocinados por marcas.[35] Uno de los aspectos más graves de su actividad es la imagen que desprenden estos jóvenes, especialmente en el caso de las niñas, que tienden a sexualizar su cuerpo, pudiendo provocar tanto en ellas mismas como en su público femenino trastornos cognitivos, al implantar una imagen falsa tanto de su cuerpo como de sus rutinas diarias.[36] En este ámbito no son pocas las *kidinfluencers* femeninas de entre unos 10 a 13 años que muestran en vídeos sus rutinas de belleza para ir al colegio, utilizando productos de lo más variados, la mayoría etiquetados para personas de avanzada edad (por tener efecto sobre piel madura, como arrugas). Sin embargo, la normalización del uso de este tipo de productos sobre chicas más jóvenes ha hecho que se vaya extendiendo esta práctica entre jóvenes que no sabían que "necesitaban" algo sin lo que ahora no pueden vivir.

---

[34] FERNÁNDEZ BLANCO, E., y RAMOS GUTIÉRREZ, M., "Kid influencers. Creación de contenidos de marca de la generación Alpha y sus implicaciones jurídicas", en CALDEVILLA DOMÍNGUEZ, D., *Libro de Actas del Congreso Internacional sobre Comunicación, Innovación, Investigación y Docencia*, Fórum Internacional de Comunicación y Relaciones Públicas, núm. XXI, Sevilla, 2022, p. 33.

[35] PLATERO ALCÓN, A., *Repercusiones jurídico-civiles de la actividad de los 'influencers' digitales… op cit.,* p. 112.

[36] CONDE FALCÓN, A., y DELGADO PONCE, A., "Estudio de la competencia mediática frente al impacto d ellos youtubers en los menores de edad españoles", *Pixel-Bit: Revista de medios y educación*, núm. 61, 2021, pp. 257-258.

Con este tipo de contenidos, además, se tiende a perpetuar los estereotipos asociados a las mujeres y niñas en relación con el ideal de belleza femenina.

Como se acaba de mencionar, en la mayor parte de los casos, los productos o contenidos que se suben a las plataformas cuentan con el consentimiento de los progenitores, que han formalizado contratos con marcas de carácter publicitario, por lo que sus hijos e hijas menores de edad acaban realizando tareas profesionalizantes. Para realizar este tipo de campañas publicitarias en los vídeos se colocan los productos patrocinados en ciertos lugares del encuadre de la cámara o móvil para que se vean de forma sencilla sin aparecer en primer plano. En el ámbito de las redes sociales, los vídeos en los que se está emitiendo claramente un contenido totalmente patrocinado existe la obligación de etiquetarlo como tal en la propia historia o *reel* y suele tener la forma de *unboxing,* formato en el cual el adolescente va sacando de una caja el contenido que le ha enviado la marca y lo muestra a la cámara recomendándolo mediante reseñas positivas a su público. Problemas como la publicidad encubierta en este tipo de vídeos o los daños producidos por una expectativa del producto que no se cumple en la realidad, serán tratados en el siguiente apartado de esta investigación.

Parecido a este fenómeno de los *kidsinfluencers* ha surgido una nueva corriente denominada *sharenting* (formada por el término inglés *share*, que significa compartir y *parenting*, relativo a la crianza), que hace referencia a la conducta en redes sociales de padres y madres que muestran a sus hijos e hijas en situaciones corrientes de su vida diaria, llegando a crear todo un séquito de seguidores que ansían contenido diario sobre los avances en el desarrollo de los niños y niñas y una puesta al día continua.[37]

[37] AMMERMAN YEBRA, J., "De nuevo sobre el 'sharenting' y los derechos de la personalidad de los menores de edad", en OTERO CRESPO, M., *Retos jurídicos de actualidad*, Dykinson, Madrid, 2021, p.80.

En este caso son los progenitores los titulares del perfil en la red social, pero al igual que con los *kidsinfluencers*, la imagen principal o atractivo de la cuenta siguen siendo los menores de edad.[38] Lo cierto es que lo más habitual es que los progenitores de los menores no publiquen fotografías para ponerlos en ridículo o atentar contra su dignidad u honor, sino que entre las principales finalidades se encuentran: compartir con los seguidores un sentimiento de satisfacción u orgullo por un logro conseguido por su descendiente; obtener aprobación social mediante *likes*, comentarios o aumentar el número de seguidores; obtener un beneficio económico mediante el *sharenting* con fines lucrativos. Este último objetivo sí que plantea interrogantes, entre otros, si esta situación podría considerarse una explotación laboral del adolescente, ya que la cuenta está administrada por un adulto que obtiene los ingresos en su nombre.[39] Lo llamativo de este fenómeno es que se desarrolla principalmente por las madres y en la red social Instagram, siendo escasas las cuentas de padres que muestran a sus hijos, ya que las existentes suelen actuar en pareja.[40]

Dentro de la práctica del *sharenting* podemos distinguir diversas tipologías, en función de la intensidad y las repercusiones para la infancia y adolescencia.

En primer lugar, nos encontramos con el *sharenting* social, consistente en los usos sociales del entorno del niño o niña y que no conlleva gravedad ni riesgo para aquellos. Para ello hay que tener en cuenta características tales como el número y tipo de seguidores, el número

---

[38] GARCÍA GARCÍA, A., "La protección del menor en el derecho europeo y español. El sharenting y su problemática", *Universitat Politécnica de Valencia*, núm. 10, Valencia, 2021, pp. 52-55.

[39] CASTILLO PARRILLA, J.A., "Riesgos y daños derivados del sharenting", en IVONE V., GÁLVEZ CRIADO, A., y LÓPEZ SUÁREZ, M.A., *Nuevos escenarios del derecho de familia en España e Italia. Novedades legales y jurisprudenciales*, Atelier, Barcelona, 2023, p. 111.

[40] FLORIT FERNÁNDEZ, C., *Los Menores e Internet. Riesgos y Derechos: Especial Consideración de La Nueva Ley Orgánica 8/2021, de 4 de Junio de Protección Integral de La Infancia y La Adolescencia Frente a La Violencia*, Bosch, 2022, p.2.

de archivos y la constancia con la que se suben, la configuración de privacidad del perfil, la edad del menor, el tipo de información que conoce. Esta primera tipología no supone una intromisión ilegítima en los derechos de la personalidad del menor, más allá del peligro de dar a conocer en todo momento dónde se encuentra, lo que puede alertar a los rastreadores de menores, quienes, siguiendo la pista de los niños o niñas, dado el caso, podrían llegar incluso a secuestrarlos con diversas finalidades o a utilizar la imagen de los jóvenes para elaborar contenido pornográfico o con otros fines ilícitos.

En segundo lugar, nos encontramos con el *oversharenting*, que se da cuando la actividad parental excede de los usos sociales normales y habituales para una familia con redes sociales. Es esta tipología la que entraña graves riesgos para los menores, tanto en su desarrollo personal como en los derechos de la personalidad de los que aquellos son titulares.

Finalmente, nos encontramos con el *sharenting* lucrativo, consistente en mostrar a los niños y niñas en las redes sociales con el objetivo de obtener una renta como contraprestación y que, por sus características, cabría plantearse que se puede tratar de una explotación laboral de los niños y niñas. ¿Mostrar en las redes sociales la vida de un menor de forma continua para obtener un rendimiento a cambio podría ser considerada una vulneración de los derechos de la infancia? Respondiendo a este interrogante, la doctrina afirma que se trata verdaderamente de una explotación infantil, dado que de acuerdo con el artículo 6 del Estatuto de los Trabajadores,[41] el menor no puede prestar su consentimiento para celebrar un contrato laboral hasta que no tenga 16 años.

Sobre esto, incluso el apartado cuarto de este mismo artículo, en relación con la intervención de menores de 16 años en espectáculos públicos, solo permite este tipo de trabajo en casos excepcionales y siempre que esté autorizado por la autoridad laboral. En el supuesto

[41] *BOE* núm. 255, de 24 de octubre de 2015.

que estamos tratando, se podría considerar que la actividad que llevan a cabo los niños y niñas es de carácter publicitario o artístico, ya que los padres reciben una remuneración económica por los vídeos que cuelgan en función del número de visualizaciones y del impacto en sus seguidores. De este modo actúan como empresarios o trabajadores autónomos, mientras que los menores funcionan como trabajadores de sus progenitores. La verdadera razón por la que se entiende que dicha conducta debería ser considerada una explotación laboral[42] es porque ninguna norma permite el trabajo que están desempeñando los menores en las redes; no por el hecho de que reciban o no una contraprestación económica a cambio de su trabajo, sino porque no tienen potestad para decidir si quieren o no trabajar.

Adicionalmente debe añadirse que, el fenómeno del *sharenting* produce otros inconvenientes, y es que el hecho de compartir contenido en una red social genera una huella digital para el niño, niña o adolescente, que lo acompañará durante todo su recorrido en Internet. Entre los principales riesgos de esta sobreexposición nos encontramos:

- Lesiones al derecho al honor, ocasionadas mediante la publicación de fotografías o vídeos que puedan avergonzar al niño, niña o adolescente en su futuro. Por ejemplo, en el caso de que se publique una fotografía en ropa interior, desnudo, en bañador…
- Lesiones al derecho a la intimidad, derivadas de la publicación de fotografías o vídeos que el menor de edad no querría que fueran vistas por otros usuarios en Internet, porque afectan a su esfera de privacidad.
- Lesiones al derecho a la protección de datos. El derecho a la imagen es un dato personal, por lo que es necesario el consentimiento para su publicación en las redes sociales.[43]

[42] FLORIT FERNÁNDEZ, C., "Kidfluencers: menores de edad emancipados autónomos en internet", *Actualidad Civil*, núm. 2, febrero de 2021, p. 5.

[43] CASTILLO PARRILLA, J.A., "Riesgos y daños derivados del sharenting …", *cit*., p. 112.

2. Intromisión en los llamados derechos de la personalidad: honor, intimidad e imagen

Como se ha podido deducir de lo expuesto, el principal problema que se suscita con esta situación de sobreexposición de la infancia y adolescencia es la posible vulneración de los derechos al honor, a la intimidad o la propia imagen. Estos derechos constituyen lo que se ha denominado "derechos de la personalidad" y se le reconocen a todas las personas por el mero hecho de serlo y tanto si son nacionales, como si son extranjeras. Por tanto, también las personas con discapacidad y las menores de edad son titulares de dichos derechos, independientemente de que puedan ejercerlos o que estén en disposición de otorgar su consentimiento legitimador de una posible intromisión ejercida por terceros.

El derecho al honor es un concepto jurídico que depende de los valores y las ideas sociales que se tengan en cada momento en concreto, pero su finalidad principal es proteger la reputación de una persona, especialmente de expresiones de menosprecio, escarnio o humillación, que se realicen de forma ilegítima.[44]

El derecho a la intimidad, por su parte, busca garantizar la creación de un ámbito propio o individual frente al conocimiento ajeno, lo cual comprende la facultad de excluir cualquier hecho comprendido en el ámbito propio del conocimiento de los demás individuos.[45]

Respecto al derecho a la propia imagen, este permite a su titular disponer de la representación de su propio físico de modo que se permita su identificación, de tal manera que aquel libremente puede decidir que las imágenes tengan difusión o impedir que se publiquen o reproduzcan.

[44] STC 8/2022, de 27 de enero. ECLI:ES:TC:2022:8

[45] CASTILLO PARRILLA, J.A., "Riesgos y daños derivados del sharenting…", *cit*., p. 115.

Por su parte, el derecho a la protección de datos (que debe estudiarse de forma autónoma) se diferencia del derecho a la identidad en que éste protege todo tipo de datos personales, independientemente del ámbito privado o público del que provengan. El derecho a la protección de datos es definido por la doctrina como el poder de disposición y control sobre los propios datos personales, de tal manera que se pueda decidir sobre todos los aspectos relativos a su tratamiento.[46]

La interpretación que se debe realizar sobre qué actos del *sharenting* atentan contra el derecho al honor, la intimidad y la propia imagen de los niños, niñas y adolescentes debe ser, en opinión de Castillo Parrilla, amplia, debido a que:

- Los menores son personas vulnerables por su edad y madurez.
- En la gran mayoría de ocasiones no tienen oportunidad de consentir, ya que son bebés, no tienen madurez suficiente o incluso no han llegado a nacer (caso de muestra de ecografías).
- A pesar de haber otorgado su consentimiento, es necesario valorar la edad y las circunstancias en las que lo han otorgado. Por ejemplo, ¿conocían que podían negarse a publicar cierto contenido? ¿Se les han explicado las consecuencias que puede tener publicar una fotografía en Internet? ¿Conocen el significado de la huella digital?
- El consentimiento para la publicación de una fotografía individual no debería extenderse a más información, ya que lo que puede parecer inofensivo en un primer momento puede afectar a otros ámbitos de sus vidas que no se han planteado en un primer momento.

[46] CASTILLO PARRILLA, J.A., "Riesgos y daños derivados del sharenting …", *cit*., p. 115.

- Las personas que suben las fotografías no son los propios menores, sino sus padres, que basan la popularidad de sus cuentas en la publicación de una imagen que no es suya.[47]

El reconocimiento de estos derechos de la personalidad tuvo lugar por primera vez en el artículo 12 de la Declaración Universal de Derechos Humanos de 1948,[48] adoptada por las Naciones Unidas. Este precepto señala que nadie puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación.

Más tarde, el Pacto Internacional de Derechos Civiles y Políticos,[49] de 19 de diciembre de 1966, adoptado en Nueva York y ratificado por España en 1977, recogió en su artículo 17 el derecho de todas las personas a no ser objeto de injerencias arbitrarias o ilegales en sus vidas privadas, sus familias o sus domicilios. Y, posteriormente, el 20 de noviembre de 1989, fecha de aprobación de la Convención de Derechos del Niño,[50] se dispuso expresamente en relación con los niños en el artículo 16 que, "ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación".

Un gran paso adelante se dio en el seno del Consejo de Europa con la adopción del Convenio Europeo de Derechos Humanos,[51] firmado el 4 de noviembre de 1950, que entró en vigor el 3 de septiembre de 1953, ya que reconoce en su artículo 8.1 el derecho a la vida privada y familiar.

---

47 *Ibid.*, p. 117.

48 Disponible en el siguiente enlace: https://www.un.org/es/about-us/universal-declaration-of-human-rights

49 Disponible en el siguiente enlace: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

50 Disponible en el siguiente enlace: https://www.unicef.es/sites/unicef.es/files/comunicacion/ConvencionsobrelosDerechosdelNino_0.pdf

51 Disponible en el siguiente enlace: https://www.echr.coe.int/documents/d/echr/Convention_SPA

La Unión Europea, por su parte, promulgó en 1992 la Carta Europea de Derechos del Niño,[52] adoptada en Resolución del Parlamento Europeo de 8 de julio de 1992, cuyo artículo 8.29 reconoce el derecho de los menores a no ser objeto por parte de un tercero de intrusiones injustificadas en su vida privada.

En el ámbito interno, de otro lado, nos encontramos con el artículo 18 de la Constitución española,[53] que reconoce el derecho al honor, la intimidad personal y familiar y la propia imagen.[54] Más específicamente, la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[55] les atribuye el carácter de irrenunciables, imprescriptibles e inalienables. Dicha ley les reconoce la titularidad de tales derechos y establece las condiciones en las que, de tener suficiente madurez, el niño o niña puede permitir una intromisión en dicho derecho. De no tener suficiente madurez, sus representantes legales lo suplirían, siempre y cuando pongan en conocimiento del Ministerio Fiscal la intención de emitir su consentimiento.

Pues bien, el artículo 2 de la mencionada Ley 1/1982, establece que no se apreciará la existencia de una intromisión ilegítima cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso. Esto es así, ya que, como ha reiterado el Tribunal Constitucional en múltiples ocasiones, le corresponde acotar a cada persona el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno.[56] Como ya hemos apuntado, el artículo 3 de la Ley 1/1982 establece que el consentimiento de los menores e incapaces deberá prestarse por

[52] *DOCE* nº C 241, de 21 de septiembre de 1992.

[53] *BOE* núm. 311, de 29 de diciembre de 1978.

[54] El Tribunal Constitucional en su sentencia 156/2001, de 2 de julio, ya ha reconocido el carácter independiente de cada uno de estos derechos (honor, intimidad e imagen). Esto significa que hay que atribuirle a cada uno su propio contenido. *BOE* núm. 178 Suplemento, de 26 de julio de 2001.

[55] *BOE* núm. 115, de 14 de mayo de 1982.

[56] STC 83/2002, de 22 de abril de 2002, ECLI:ES:TC:2003:14; STC 196/2006, de 3 de julio de 2006, ECLI:ES:TC:2006:196.

ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil. En caso contrario, el consentimiento se debe otorgar por escrito por su representante legal, que está obligado a ponerlo en conocimiento del Ministerio Fiscal, quien, en el plazo de 8 días, debe pronunciarse, y en caso de negarse, deberá resolver el juez. Esta regla es coherente con el artículo 162 del Código Civil, que establece la posibilidad a los menores de realizar por sí mismos actos relativos a los derechos de la personalidad de acuerdo con su madurez (como ocurría para la apertura de una cuenta por los usuarios en las redes sociales).

El interrogante que surge es qué debe entenderse por madurez suficiente, ya que en el propio Código Civil existen preceptos que otorgan madurez suficiente a los niños o niñas de 12 años,[57] mientras que otros preceptos la elevan a 14 años.[58] Aunque pudiera parecer en un primer momento que la madurez se rige por una edad concreta, la doctrina apunta que "la valoración de esta madurez exige huir de soluciones generales, para centrarse en un examen particular de las circunstancias del menor en concreto".[59] Resulta interesante la Sentencia del Tribunal Supremo de 17 de diciembre de 2013,[60] que trataba sobre el consentimiento de un menor de 17 años para que le hicieran fotografías y una entrevista en un canal de televisión. El Tribunal Supremo no entró a valorar sus condiciones de madurez en función de variables psicológicas, sino que centró la cuestión en que el menor no había otorgado expresamente su consentimiento para la realización de las fotografías, sino que solo consintió en realizar la entrevista para el canal, por lo que no se había proporcionado un consentimiento informado. Como se puede

[57] Por ejemplo, los artículos 156, 159, 161, 172, 173, 176 bis, 177, 178, 231 o 273 del Código Civil.

[58] Por ejemplo, los artículos 14, 20, 21, 23, 775 o 776 del Código Civil.

[59] MORALEJO IMBERNÓN, N., *Los derechos de los menores… op cit*., p. 56.

[60] TOL4.074.928

observar, la posición de nuestro Tribunal Supremo es claramente garantista y tiene como finalidad principal la protección de la infancia y adolescencia en cualquier situación.

Por lo tanto, si partimos de la presunción de que el menor de edad que aparece en las redes sociales, bien por ser un *influencer* o bien mediante la técnica del *sharenting*, tiene la madurez suficiente para comprender las consecuencias de sus actos,[61] dicha conducta paterna/materna de sobreexposición del niño o niña estaría en principio exonerada, ya que cuenta con el consentimiento del menor.[62] Sin embargo, parece extraño pensar que un menor de edad, que ha sido expuesto en las redes por sus progenitores de forma habitual, sea capaz de comprender los daños que puede generar en sus derechos de la personalidad el comportamiento de sus padres. En dicho caso, podríamos plantearnos que el consentimiento otorgado por el niño o niña no legitimaría la intromisión que se pueda realizar en sus derechos.[63]

3. La titularidad de los derechos a la intimidad y la imagen de los niños, niñas y adolescentes tras su fallecimiento

Como ya se ha señalado, el derecho a la intimidad y el derecho a la imagen configuran los llamados derechos de la personalidad, que tienen la característica de adquirirse desde el nacimiento, a pesar de que los niños y las niñas, debido a su edad, no puedan ejercitarlos completamente.

---

61 Sobre el tema de la privacidad en redes profundiza: GIL ANTÓN, A.M., *¿Privacidad del menor en Internet? Me gusta ¡¡¡todas las imágenes de mis amigos a mi alcance con un simple click!!!*, Aranzadi, Navarra, 2015.

62 VÁZQUEZ PASTOR, L., "Los derechos de la personalidad del menor de edad en la era digital. La dicotomía entre autonomía y protección", *Actualidad Jurídica Iberoamericana*, núm. 17, 2022, pp. 1147-1149.

63 LLAMAS BAO, C., "Hijos menores de edad en redes sociales: su protección al amparo de los artículos 18 y 39 de la Constitución española", *Revista Jurídica de la Universidad de León*, núm. 8, 2021, p. 203.

Estos derechos se encuentran especialmente protegidos en el artículo 18 de la Constitución española, debido a que el sujeto pasivo titular del mismo es una persona menor de edad, cuyo desarrollo psíquico puede quedar gravemente afectado.

La problemática que se plantea en este apartado es la posibilidad de publicar fotos en las redes sociales de una persona menor de edad que ha fallecido, no desde la perspectiva clásica de los medios de comunicación que retransmiten imágenes en eventos relacionados con personas famosas, sino desde la perspectiva de amigos y familiares que, una vez fallecido el niño, niña o adolescente, deciden publicar imágenes con él o donde aparece él solo en sus respectivas redes sociales. Y es que es bastante habitual que, en el ámbito de las redes, cuando el niño o niña tiene una notoria relevancia o los padres se dedican a exponer al menor mediante el *sharenting*, se difundan vídeos creados incluso por los propios padres con imágenes recopilatorias de la vida del menor para darle una última despedida pública. Ahora bien, debemos plantearnos si existe un derecho a la intimidad y a la propia imagen del menor fallecido.[64]

Lo cierto es que los derechos de la personalidad se extinguen con el fallecimiento de su titular, sin embargo, existe la posibilidad de ejercitar acciones por aquellos que han sido designados por el fallecido en su testamento (hecho improbable al no ser habitual que un niño, niña o adolescente piense en esas cuestiones a una edad tan temprana), o sus familiares y, a falta de estos, el Ministerio Fiscal. Así lo establece el artículo 4 de la Ley 1/1982. En el ámbito de los menores de edad, el apartado 4.4 de la cita ley establece que, además de las acciones que pueden ejercitar los representantes legales del menor, al Ministerio Fiscal le corresponde en todo caso, reforzando su papel de garante de los derechos de las personas necesitadas de una especial protección.

[64] GUTIÉRREZ SANTIAGO, P., "La llamada "personalidad pretérita": datos personales de las personas fallecidas y protección *post mortem* de los derechos al honor, intimidad y propia imagen", *Actualidad Jurídica Iberoamericana,* núm. 5, 2016, pp. 201-238.

Entrando en el análisis de los derechos de la personalidad en profundidad, con respecto al derecho a la intimidad, el Tribunal Constitucional ya estableció que, incluso cuando el titular del derecho ha fallecido, sigue subsistiendo el derecho a la intimidad familiar, otorgando a los familiares más próximos el derecho a preservar una cierta privacidad, ya que el daño que se le induzca al fallecido también puede repercutir en la propia familia. Así lo puso de manifiesto en la Sentencia de 2 de diciembre de 1988[65] (caso de la difusión en televisión de la muerte del famoso torero Paquirri).

Ahora bien, ¿qué ocurriría si son los progenitores del niño, niña o adolescente los que acceden a esas imágenes, pongamos de ejemplo, alojadas en el móvil del menor y las publican o simplemente disponen de ellas? El Tribunal Supremo, en su Sentencia de 26 de noviembre de 2014[66] tuvo ocasión de pronunciarse al respecto, en relación con unos padres que accedieron al teléfono de su hija fallecida con la asistencia de un ingeniero informático sin previa autorización judicial. En este caso, el Tribunal señaló que: "incluso en aquellos derechos personalísimos, que no se transmiten a los herederos, éstos sí suceden al fallecido en el ejercicio de las acciones para su defensa (derecho moral de autor, protección civil del honor, intimidad, imagen, etc.), lo que les faculta para acceder de forma proporcionada a la documentación de sus comunicaciones (correspondencia, correos electrónicos o telemáticos, conversaciones grabadas, etc.), en la medida en que sean necesarios para la defensa de sus intereses, incluido obviamente, para ejercitar las acciones procedentes para la reparación de los daños causados al fallecido". Esto supone que en este caso no se entendiera que se había incurrido en una violación del derecho a la intimidad de la fallecida, ya que el acceso realizado por sus padres se hizo de un modo proporcional, siendo estos sus sucesores.

[65] ECLI:ES:TC:1988:231

[66] Sentencia núm. 850/2014 de 26 noviembre (RJ 2014\6423).

Lo cierto es que, a pesar de que, por ejemplo, la Ley de protección de datos en su artículo 96.1.a) establece que los familiares de los fallecidos "podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión", el objetivo de política legislativa de la normativa actual consiste en la protección de las personas menores de edad frente a posibles injerencias de terceros, ajenos a su familia, ya que se da por hecho que un familiar no difundiría imágenes de un ser querido después de haber acontecido tales circunstancias o que, si lo hacen, esto no perjudicaría a su privacidad ni a su derecho al honor, sino que se realizaría desde el cariño y la intimidad familiar.

Esto se debe en gran parte a que el fenómeno del *sharenting* es más reciente de lo que parece, por lo que el legislador no tenía en mente escenarios tan rocambolescos como los que pueden suscitarse en el seno de las redes sociales. Desde mi punto de vista, no veo injerencia en la vida privada del niño, niña o adolescente, ni en su derecho a la imagen, a la intimidad o al honor por la publicación de quienes eran los titulares de la patria potestad del niño o joven en la publicación de una imagen de quien era su hijo o hija, más allá de una muestra de cariño o afecto sin más trascendencia jurídica. Ahora bien, podría darse el caso de que tales imágenes sean posteriormente utilizadas por las redes de delincuencia para su utilización con fines ilícitos, debiendo estas conductas ser sancionadas penalmente.

LA PUBLICIDAD ENCUBIERTA DE LOS *INFLUENCERS* Y LOS DAÑOS PRODUCIDOS A LA INFANCIA Y ADOLESCENCIA

1. El concepto de publicidad encubierta y su regulación

Una de las principales fuentes de ingresos de los *influencers* son las campañas publicitarias que realizan con marcas que, a cambio de publicitar un producto concreto en sus redes sociales, les ofrecen contratos con cantidades sustanciosas de dinero. De este modo, las marcas se aprovechan del alcance que tienen estas figuras para hacer llegar su producto al sector poblacional concreto para el que se ha realizado. Cuando esto pasa, las publicaciones que realiza el *influencer* aparecen etiquetadas como publicidad o *advertisement* y se vincula también el perfil de la marca en sí para que los seguidores puedan tener acceso directo al link de compra del producto en la web oficial. Sin embargo, puede suceder que esas campañas de publicidad se encuentren escondidas tras una forma camaleónica, pasando desapercibidas por los usuarios, que ven mostrado un producto en el perfil de su *influencer* sin indicar que se trata de publicidad. De este modo, el *influencer* da su opinión, que de forma tácita posee mayor valor para los usuarios de la red, que perciben la reseña del producto como fiel, veraz y confiable.[67] Es precisamente en este contexto de acuerdo camuflado entre la marca y el *influencer* donde nace la publicidad encubierta.

La doctrina pone de manifiesto que para tratarse de publicidad encubierta será necesario que se den tres requisitos fundamentales: que la publicidad contenga contenido comercial, que dicho contenido

[67] BENDITO CAÑIZARES, M.T., "La autenticidad de la publicidad y anunciante en la publicidad nativa y en particular, en la publicidad de los *influencers*", Revista Aranzadi Doctrinal, núm. 8, 2020, p. 222.

comercial sea imposible o muy difícil de descifrar para el usuario y que no contenga advertencias para identificar el contenido comercial, provocando un error de manera intencional en el destinatario del mensaje.[68]

Esta práctica se encuentra regulada en la Ley 3/1991, de 10 de enero, de Competencia Desleal (LCD),[69] cuyo artículo 5 considera desleal por engañosa "cualquier conducta que contenga información falsa o información que, aun siendo veraz, por su contenido o presentación induzca o pueda inducir a error a los destinatarios". A su vez, el artículo 7 establece que "se considera desleal la omisión u ocultación de la información necesaria para que el destinatario adopte o pueda adoptar una decisión relativa a su comportamiento económico con el debido conocimiento de causa".

Específicamente en el ámbito de las redes sociales y los *influencers* es escasa la regulación al respecto, ya que lo más habitual es la nueva tendencia a la creación de códigos de conducta en sectores como el de los creadores de contenido, cuya adhesión es voluntaria. En sede nacional nos encontramos con el Código de conducta sobre el uso de *influencers* en la publicidad,[70] creado en 2020, que contiene una serie de principios.

Resulta reseñable el punto 5, en el que se recalca que: "La naturaleza publicitaria de las menciones realizadas por *influencers* o de los contenidos digitales divulgados por estos, que tengan tal consideración publicitaria, deberá ser identificable para sus seguidores. En aquellos casos en los que dicha naturaleza publicitaria no sea clara y manifiesta

[68] RODRÍGUEZ TERCEÑO, J., BARTOLOMÉ ROMERO, C., y FANJUL FERNÁNDEZ, M. L., "Influencers, instagramers y publicidad encubierta", en CASTILLO ABDUL, B., *Prosumidores, emergentes, redes sociales, alfabetización y creación de contenidos*, Dykinson, Madrid, 2021, p. 815.

[69] *BOE*, núm. 10, de 11 de enero 1991.

[70] Disponible en el siguiente enlace: https://www.autocontrol.es/wp-content/uploads/2020/10/codigo-de-conducta-publicidad-influencers.pdf

a la vista de la propia mención o contenido, se deberá incluir una indicación explícita, inmediata y adecuada al medio y mensaje sobre la naturaleza publicitaria de tales menciones o contenidos".

Sin embargo y a pesar de la buena iniciativa a la hora de crear un instrumento de regulación específica, este presenta grandes inconvenientes, como su naturaleza de *soft law,* o consideraciones tales como que cuando sea la propia figura pública la que quiera realizar una reseña de forma libre, haya o no recibido una contraprestación, el Código configura que no se estaría realizando publicidad propiamente dicha, por lo que si no se indica de forma correcta esta opinión libre se convertiría en una publicidad encubierta, de forma paradójica.[71]

2. Situaciones prácticas de publicidad encubierta en redes sociales

Son muchas las situaciones prácticas en las que el Jurado de Publicidad (organismo creado por la Asociación Autocontrol, que es una organización independiente de autorregulación de la industria publicitaria en España)[72] ha emitido resoluciones resolviendo asuntos de publicidad encubierta. Tal es el caso de la Resolución de 26 de mayo de 2023, asunto "Marta Lozano Influencer. Internet". En este caso se planteaba el supuesto de una famosa *influencer* española con gran popularidad en la red de Instagram, que realizó una publicación en la que vestía un pijama y un conjunto de lencería de una famosa marca, Intimissimi, pero sin mostrar *a priori* ningún indicativo de que se trataba de publicidad, al no contener marcas etiquetadas, ni haber puesto la expresión "colaboración", "gifted", etc. Sin embargo, en la descripción de la publicación, justo al final, se encontraba la etiqueta #intimissimigirls Ad. En este caso el

[71] GARCÍA PÉREZ, F.J., "El nuevo Código de conducta sobre el uso de *influencers* en la publicidad: una buena (y esperada) noticia en el ámbito de la publicidad digital", *Actualidad Jurídica Aranzadi*, núm. 967, 2020, p. 2.

[72] Disponible en el siguiente enlace: https://www.autocontrol.es/resoluciones-del-jurado/

Jurado, en su fundamento noveno argumentó que la información que se estaba ofreciendo al público no era suficiente y no permitía identificar a primera vista que se trataba de una colaboración, por lo que se catalogó este caso como publicidad encubierta.[73]

Otra Resolución emitida por dicho Jurado fue la de 13 de enero de 2023, con el asunto "Cinco Jotas *Influencer*, Internet". Se trataba de una publicación realizada en forma de *reels* (vídeo de corta duración) alojado en la plataforma Instagram, en el perfil de una *influencer*, llamada Verónica Masterchef, que fue ganadora de un famoso concurso de televisión. En el vídeo aparecía realizando una receta en la que usaba jamón ibérico de la marca Cinco Jotas. En ningún momento del vídeo, ni en la descripción, ni verbalizándolo, hizo mención a que se trataba de una colaboración. En este caso el Jurado, en su fundamento octavo estableció que se trataba de publicidad encubierta, ya que no tapó la marca, sino que ésta estaba visible durante todo el vídeo.

Para finalizar con los ejemplos, el último que vamos a ilustrar se recoge en la Resolución de 12 de marzo de 2021, asunto "Nesquik. Internet". En esta ocasión, el famoso cocinero *influencer* Alex Chía, también en la red social de Instagram, realizó una receta a la que añadía cacao en polvo de la marca Nesquik. En ningún momento del vídeo el *influencer* dijo el nombre de la marca, ni realizó ningún comentario sobre la calidad del producto, ni lo recomendó. Es por esto por lo que el jurado estimó en esta ocasión que no se trataba de publicidad encubierta, porque el individuo solamente estaba realizando una receta y no había ningún tipo de intención publicitaria detrás.

[73] PLATERO ALCÓN, A., *Repercusiones jurídico-civiles de la actividad de los 'influencers' digitales… op cit.,* p. 152.

3. Mecanismos del derecho frente a la publicidad encubierta centrada en la infancia y adolescencia. Especial referencia a los daños y la responsabilidad

Ahora bien, no es capricho que en esta investigación hayamos introducido una mención a la publicidad encubierta. Y es que, al ser habitual en el ámbito de las redes sociales encontrarse con publicaciones colgadas por *influencers* que, de forma indirecta intentan promocionar un bien dando lugar a la publicidad encubierta, los grandes perjudicados van a ser los consumidores que adquieren el producto, produciéndose daños a través de una publicidad que resulta ser falsa. En concreto, imaginemos por un segundo la influencia que pueden tener estos personajes públicos en sus seguidores menores de edad, dirigiéndoles una publicidad sutil sobre productos que creen necesitar, al no gozar estos jóvenes de madurez suficiente como para darse cuenta de que se trata de un anuncio encubierto. Basta con pensar que, al ser la relación entre los creadores de contenido y los seguidores especialmente jóvenes una relación concebida por estos últimos como una especie de amistad, es evidente que cualquier recomendación que los creadores realicen sobre un producto, sin que les indiquen que se trata de publicidad, hará surgir entre los más jóvenes un deseo de adquirir el producto que la persona a la que admiran tiene. Es este el momento en el que los jóvenes pasan a convertirse en consumidores (personas físicas que adquieren un producto para su propio uso personal) frente al empresario, que será la marca que está publicitando el *influencer*.

Puede que resulte llamativa la relación que se acaba de establecer entre la marca y el joven, en vez de entre el *influencer* y el joven. Lo cierto es que cuando la marca firma el contrato con el creador de contenido, esto no supone una vinculación laboral de contrato de trabajo, sino una puntual colaboración entre ambos. Sin embargo, es posible que esta segunda relación (entre el *influencer* y el adolescente) se cree cuando el creador de contenido actúa bajo el control absoluto y siguiendo las

órdenes de la empresa, por ejemplo, si existe una vinculación laboral mediante un contrato de trabajo, pero no cuando existe un contrato de colaboración puntual.[74]

Incluso es posible que dicha publicidad encubierta se realice sobre un producto que sea de la propia marca del *influencer*. Y es que es muy habitual que cuando un personaje público en redes adquiere cierta relevancia, abra su propia marca dirigida al público concreto de sus seguidores, para obtener rendimientos de forma directa. En este caso, los posibles daños que pueda suscitar dicha publicidad en los seguidores deberían ser resarcidos por el *influencer*, que adopta en esta ocasión la forma de empresario, apareciendo el seguidor con su estatus de consumidor.[75]

Sin embargo, lo más habitual es que cuando se realiza la promoción de un bien, esta publicidad sea producto de un acuerdo realizado entre una empresa y un creador digital, de modo que la empresa entrega una contraprestación económica a cambio de que el *influencer* realice publicidad encubierta dentro de su contenido habitual, realizando una reseña siguiendo un guión o unas indicaciones previamente aportadas por la propia empresa. En este tipo de circunstancias no cabe considerar al creador de contenido como un empresario, ya que el producto que se muestra no es de su propiedad y el beneficio comercial de la compra del mismo no redunda en su margen de beneficio, sino en la propia compañía. Aquí es donde empiezan los problemas jurídicamente relevantes, concretamente, cuando el niño o joven adquiere el producto publicitado y, una vez en su casa, se da cuenta de que este no cumple

[74] PLATERO ALCÓN, A., *Repercusiones jurídico-civiles de la actividad de los 'influencers' digitales… op. cit.*, p. 189.

[75] VIDAL BEROS, C., "Ley General de comunicación audiovisual española. Influencers y sustentabilidad", *Cuadernos del Centro de Estudios en Diseño y Comunicación*, núm. 181, 2023, p. 95.

con las expectativas enunciadas por su ídolo. Entra en juego el Derecho. ¿Qué mecanismos ofrece el Derecho privado para aliviar los daños producidos?

En primer lugar, deberíamos acudir al artículo 61.2 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias[76] (en adelante, LGDCU), que resulta de aplicación, porque la relación entre el adolescente y la marca es una relación de consumidor y empresario, en el sentido del artículo 2 de este instrumento. El niño compra el bien en concepto de consumidor o persona consumidora vulnerable, porque lo va a utilizar para un propósito ajeno a su actividad comercial (art. 3), mientras que la marca entra dentro del concepto de empresario (art. 4), ya que sus operaciones se hacen con un propósito relacionado con su actividad comercial o empresarial. Pues bien, el artículo 61 de la LGDCU dispone que el contenido de la oferta, promoción o publicidad serán exigibles por los consumidores, aun cuando no figuren expresamente en el contrato celebrado o en el documento o comprobante recibido y deberán tenerse en cuenta en la determinación del principio de conformidad con el contrato.

Como nos encontramos en el ámbito del Derecho de consumo, al actuar el niño, niña o adolescente en este contexto como un consumidor frente al empresario, la fase contractual en la que estamos es la fase de formación del contrato. Conforme a lo estipulado en este precepto, las comunicaciones o la publicidad que realizan los *influencers* en las redes sociales sobre los productos, forman parte también del contrato que formaliza el menor con la empresa una vez compra el bien. En este sentido, ya está totalmente consolidado el hecho de que toda publicidad dirigida a los consumidores tiene carácter vinculante.[77]

---

[76] *BOE*, núm. 287, de 30 de noviembre de 2007.

[77] En este sentido profundiza: ZUBERO QUINTANILLA, S., *Las declaraciones publicitarias en la contratación,* Tirant lo Blanch, Valencia, 2017.

Pongamos por ejemplo un producto de maquillaje que es publicitado por un *influencer* como "de larga duración, dura más de 24 horas", sin embargo, los consumidores una vez lo prueban se dan cuenta de que solamente dura 5 horas. Estaríamos ante un claro engaño que ha sido cubierto por la empresa de maquillaje, que es la que en última instancia supervisa el vídeo o la imagen que va a subir el *influencer* para dar publicidad a su producto. La publicidad realizada por la persona famosa constituye un trato previo dentro del contrato con el consumidor joven, cuyo contenido forma parte del contrato.[78] Sin embargo, como ya se ha apuntado, el *influencer* no actúa de manera independiente, sino bajo las órdenes de la empresa, por lo que, a pesar de que la persona que trabaja en redes es la imagen del producto, la persona a la que se debe dirigir la acción es la empresa detrás de la promoción, hecho que resulta sin duda tedioso para un consumidor, menor de edad, sin conocimientos sobre este entramado contractual.

Sin embargo, desde el punto de vista doctrinal, hay quienes defienden[79] que existe también la posibilidad de dirigirse directamente contra el *influencer* (independientemente de la vía antes descrita), usando el mecanismo de la responsabilidad civil extracontractual, o responsabilidad tradicional del Código Civil. Para ello habría que acudir al artículo 1902 del Código Civil, que proclama que "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado", estableciendo un sistema de responsabilidad subjetivo.

Esto significa que, para que el *influencer* tuviera que indemnizar, el daño producido al consumidor promocionando de forma encubierta el producto debe haberse hecho con culpa activa u omisiva. Ahora bien, ¿cómo se podría demostrar que el creador de contenido ha actuado

[78] MARCO MOLINA, J., "El proceso de formación o conclusión del contrato", *Indret: Revista para el Análisis del Derecho*, núm. 3, 2015, p. 13.

[79] PLATERO ALCÓN, A., *Repercusiones jurídico-civiles de la actividad de los 'influencers' digitales… op cit.,* p. 193.

de forma culposa? Cuestión compleja. Para alegar la acción culposa activa la vía sería demostrando que, con su conducta en redes, durante la promoción del producto conocía perfectamente sus características y limitaciones (en el caso antes descrito, que en la propia promoción el *influencer* dijera que la duración del producto de maquillaje era de 24 horas, cuando ni se acercaba a las 24 horas que prometía). Con respecto a la actuación omisiva, no revelando cierta información que podría resultar relevante (por ejemplo, que ese producto no está indicado para pieles con tendencia acneica, porque puede resultar invasivo).

Continuando con el artículo 1902 del Código Civil, este requiere además de que se realice una acción u omisión, que el daño sea imputable al *influencer,* porque pueden darse supuestos en los que los daños no se imputen al mismo, sino, por ejemplo, a la empresa con la que trabaja, debiendo demostrar el consumidor este requisito. Traigamos a colación de nuevo el caso de los *kidsinfluencers*, siendo estos ahora los que promocionan el producto que posteriormente comprarán niños o adolescentes. Es el niño, niña o adolescente el que ha realizado la conducta generadora del daño a otros menores a través de una acción u omisión, pero ahora debería analizarse caso por caso, ya que podría ser el propio menor el que respondiese de manera directa o, de manera solidaria junto con sus padres, que no lo han supervisado de manera correcta.[80]

En este sentido, el artículo 1903 del Código Civil establece que los padres son responsables de los daños causados por los hijos que se encuentren bajo su guarda. Esto no conduce de forma automática a que sean los padres los que deban responder excluyendo por completo la responsabilidad del menor, ya que se tendría que atender a circunstancias tales como la autonomía del niño, niña o adolescente o a su madurez. En estos supuestos que implican una participación paterna/materna, se produce una inversión de la carga de la prueba, debiendo

[80] SUÁREZ FERNÁNDEZ, L., "La responsabilidad parental en los entornos digitales. Necesario equilibrio, entre acceso, control y seguridad", *Actualidad Jurídica Iberoamericana*, núm. 7, vol. 3, 2022, p. 1088.

ser los titulares de la patria potestad los que deben acreditar que han actuado de forma correcta, intentando evitar la conducta de su hijo *influencer*.

A pesar de lo expuesto y dejando a un lado a los *kidinfluencer*, si se planteara alguna demanda en base a esta responsabilidad civil extracontractual contra un *influencer* para que reparase el daño producido, éste podría alegar que el consumidor había otorgado su consentimiento al acceder a la red social y en opinión de la doctrina,[81] esto podría justificar el daño causado, ya que las principales plataformas digitales incluyen dentro de sus términos de servicio que en su funcionamiento se mostrará contenido de carácter publicitario, en la mayor parte de las ocasiones subido por *influencers* digitales.

Sin embargo, esta posición doctrinal parece bastante débil ya que, aunque se intente asimilar este consentimiento, por ejemplo, al consentimiento otorgado en sede médica (basado en la información otorgada con carácter previo al paciente, que se puede asimilar a la información otorgada con carácter previo a la red social por el usuario), el fundamento de ambas casuísticas es diferente, ya que en el consentimiento médico se informa con total claridad sobre las posibles consecuencias, efectos secundarios y secuelas de la intervención, mientras que en el acceso a redes sociales los términos y servicios por su propia configuración, extremadamente extensa y tediosa, con términos jurídicos y en un contexto digital, no se puede considerar que informan de manera adecuada a los consumidores de los posibles daños que pueden sufrir.

Finalmente, el último requisito en relación con el artículo 1902 del Código Civil es que exista una relación de causalidad entre la acción u omisión del *influencer* y el daño producido al consumidor. Para demostrar esta causalidad será necesario acudir a la teoría de la causalidad, que implica analizar la acción u omisión en atención al contexto para

[81] PLATERO ALCÓN, A., *Repercusiones jurídico-civiles de la actividad de los 'influencers' digitales… op. cit.,* p. 196.

determinar con claridad que, de todas las acciones u omisiones que hayan podido intervenir en la causación del daño, cuál es la más probable que lo originase.[82] En el caso de las redes sociales el razonamiento sería el siguiente: "el daño se le ha causado al consumidor por haber adquirido un producto pensando que tenía una serie de características anunciadas por el *influencer* y al final no las tenía. Ese daño ha sido originado, sin lugar a dudas por la conducta realizada por el *influencer*. Si o no." Ante esta argumentación, no es complicado pensar que el *influencer* podría alegar que la publicidad estaba totalmente guionizada por la empresa con la que había firmado el contrato y, por lo tanto, el daño siguiendo esta teoría habría sido producido por las instrucciones impuestas por la empresa y no por el creador en primera instancia.

Otro elemento importante a la hora de ejercitar una acción por responsabilidad extracontractual es el plazo con el que cuenta el afectado para interponer su acción. Y es que el plazo de prescripción para los daños producidos de forma extracontractual es de 1 año, lo cual resulta bastante ajustado en el tiempo en comparación con los daños derivados de responsabilidad contractual.

En conclusión, la aplicación de la responsabilidad extracontractual sería bastante complicada de encajar en el ámbito de la reclamación de daños causados por publicidad engañosa dentro de las redes sociales, por lo que si tenemos en cuenta además el precio de los productos que compran los niños y adolescentes, la reclamación por vía judicial no tendría mucho éxito. Quizá para estos casos sería necesario que se impusiera la inclusión de la plataforma de un mecanismo de resolución alternativa de litigios, como la mediación.

[82] AGUDELO MOLINA, J.D., "Causalidad e imputación. La coherencia interna de la teoría de la imputación objetiva en la responsabilidad civil", *Revista de Derecho Privado*, núm. 42, 2021, p. 337.

LA PROTECCIÓN DE DATOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES EN LAS REDES SOCIALES

En el ámbito de las redes sociales uno de los puntos fundamentales donde suelen surgir más injerencias en los derechos de los niños, niñas y adolescentes es la protección de los datos personales, ámbito en el que el Tribunal de Justicia de la Unión Europea se ha pronunciado en múltiples ocasiones para imponer multas a sus infractores. En concreto, existen tres momentos fundamentales en los que la protección de datos adquiere una importante relevancia:

El primero es en la fase inicial de registro del usuario, menor de edad, ya sean niños o adolescentes, que proporcionan información personal a la red social para poder empezar a utilizarla. Es este el momento en el que comienzan los problemas, las vulnerabilidades y la pérdida del control de dichos datos. En primer lugar, es posible que los datos que le soliciten al niño, niña o adolescente no sean excesivos, o el grado de publicidad del perfil de usuario puede resultar elevado. Tampoco nos debe extrañar que no se le informe de cuál es la finalidad de los datos que están recabando o si se va a realizar una transferencia internacional con dichos datos.

El segundo momento relevante para la protección de datos es la fase del uso, es decir, el momento en el que, una vez creada la red social, los jóvenes comienzan a utilizarla. Es en esta fase donde más proliferan los posibles riesgos, a saber: la publicidad excesiva de información personal del propio niño, niña o adolescente o de terceros (amigos, familiares, parejas), la instalación de las *cookies*, que el perfil se indexe de forma automática en un buscador de Internet sin el conocimiento del usuario, la posible recepción de ingentes cantidades de *spam* o información no deseada, la suplantación de la identidad del usuario con perfiles falsos, y un sinfín de posibilidades más.

Lo cierto es que, una vez se introduce un dato en la red, es prácticamente imposible seguirle el rastro. Es por ello que, al encontrarse el usuario en la red conectado con miles de contactos diversos, es bastante sencillo perder el control de la información, especialmente cuando son terceros los que disponen de la misma. Pongamos por ejemplo una fotografía en la que un menor etiqueta a otro, o una historia que sube con la imagen de otro amigo sin antes consultarlo.

El último momento en el que surgen riesgos derivados de la protección de datos es en el momento de cerrar la cuenta de la red social. No es extraño que puedan surgir problemas tales como que no se realice una baja efectiva, que la información siga circulando por la red, que no se cumpla el deber de supresión de los datos cuando se solicite previamente, al dejar de ser necesarios para el objetivo para el que se habían recabado.

1. El concepto de datos personales en las redes sociales y su tratamiento

La primera fuente de daños que se pueden producir para los usuarios de las redes sociales tiene su origen, como ya hemos señalado, en una infracción de los responsables del tratamiento de los datos personales o en un incumplimiento de las obligaciones establecidas por la normativa de protección de datos. Ante la gravedad de este riesgo que supone el tráfico masivo de datos actual, la Unión Europea buscó en 2016 la unificación de la normativa relativa a la protección de datos para dotar de un marco jurídico uniforme a todos los Estados Miembros. De este modo, se promulgó el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva

95/46/CE (Reglamento general de protección de datos, RGPD),[83] que recoge en sus Considerandos 4 y 7 que "el tratamiento de los datos personales debe estar concebido para servir a la humanidad" y proclama que "las personas físicas deben tener el control de sus propios datos personales".

Procede ahora realizar una aproximación general al RGPD, para estudiar sus principales disposiciones. Para asegurar el objetivo de ser útil a la humanidad, establece una serie de principios en su artículo 5, adquiriendo un modelo de responsabilidad proactiva en el que el responsable del tratamiento es responsable de que se cumplan dichos principios (art. 5.2). Para ello debe adoptar las medidas de protección técnicas y organizativas que considere adecuadas para cumplir con todos los requisitos que impone el RGPD (art. 25). En el caso de los datos relativos a menores presta una especial atención, exigiendo en el art. 8 "esfuerzos razonables" a la hora de comprobar la capacidad y la legitimación para otorgar el consentimiento; y se centra como eje principal en el principio de transparencia (art. 12). Para garantizar el control que aseguraba en los Considerandos, reconoce una serie de derechos que le corresponden a toda persona física, como es el caso del derecho de rectificación, limitación, portabilidad, cancelación y olvido (Capítulo III). Con carácter específico para el ámbito de las redes sociales otorga al interesado el derecho de eliminación, sin dilación de los datos personales que ya no sean necesarios para los fines para los que en un primer momento fueron obtenidos.

Aportadas ya unas primeras pinceladas acerca de los fines y los objetivos del Reglamento, comenzaremos a analizarlo minuciosamente.

El artículo 4.1 otorga una definición de lo que se debe entender por datos personales, esto es "toda información sobre una persona física identificada o identificable". El mismo precepto continúa señalando que

[83] *DOUE* L 119, de 4 de mayo de 2016. Disponible en el siguiente enlace: https://www.boe.es/doue/2016/119/L00001-00088.pdf

por persona física identificable se debe entender "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". De este modo, cualquier tipo de referencia o información sobre una persona física que pueda ser conectada a la misma, ya sea de modo directo o como resultado de una labor de investigación, constituye un dato personal.[84]

En el ámbito que nos ocupa, de las redes sociales, no solo constituyen datos personales los elementos que debe introducir el usuario (menor) cuando crea su cuenta, como es su fecha de nacimiento, su nombre, su correo electrónico,[85] sino también los datos que se van introduciendo durante el transcurso de la utilización de la red (comentarios, búsquedas, *likes*) e incluso los datos que introducen terceros externos (comentarios en las publicaciones del menor, fotos conjuntas, reacciones a las historias etc). Incluso también se consideran datos personales aquellos obtenidos por los anunciantes de las redes sociales, los desarrolladores y los editores, que se extraen de la dirección IP del perfil y da acceso al historial de navegador del menor en la red social y en Internet en general, abriendo paso a un gran banco de información sobre sus gustos e intereses, que hace que el anunciante pueda ofrecer publicidad personalizada.[86] A esta nueva fuente de datos se le suma también la información sobre el tipo de dispositivo, el lugar desde el que se accede a la información y los lugares más visitados, proporcionado por las *cookies*.

---

[84] En este sentido, señala MORALEJO IMBERNÓN, N., *Los derechos de los menores… op. cit*., p. 197 que "El TJUE ha entendido que la IP dinámica de un internauta constituiría un dato personal, pues unido a la información adicional que posee un proveedor de acceso a Internet, permitiría la identificación del usuario (STJUE de 19 de octubre de 2015, asunto C-582/14, caso *Breyer*)".

[85] Así lo ha estimado el TJUE en la STJUE de 6 de noviembre de 2003, asunto C-101/01.

[86] MORALEJO IMBERNÓN, N., *Los derechos de los menores… op cit*., p. 199.

Una vez esbozado el concepto de datos personales en el ámbito de las redes sociales, debemos estudiar qué se entiende por tratamiento de datos personales, que es lo que se protege en la normativa europea. De este modo, el art. 4.2 del RGPD lo define como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción". Esta definición, *a priori* tan amplia sobre el tratamiento de datos ha sido tratada por el TJUE en sus sentencias de 6 de noviembre de 2003, asunto C-101/01;[87] de 16 de diciembre de 2008 asunto C-73/07;[88] y de 13 de mayo de 2014 Caso Google Spain, asunto C-131/12,[89] en las que opta por darle un sentido extenso. En esta última sentencia, relativa a las operaciones llevadas a cabo por el motor de búsqueda de internet, que extrae, registra y organiza información para conservarla en sus servidores y posteriormente facilitar acceso a los usuarios proporcionándoles listas de resultados, el TJUE entendió que se estaba llevando a cabo un tratamiento de datos. Extrapolando esto al ámbito de las redes sociales, los prestadores del servicio pueden ser consideradores responsables del tratamiento de datos, porque ponen a disposición de los usuarios los medios y vinculan a estos los servicios de gestión de datos.[90]

Sin embargo, dentro de las redes sociales, en ocasiones, es el propio usuario menor de edad el que se convierte en sujeto que trata datos personales, cuando se incluye un comentario o se etiqueta en una fotografía. No obstante, este tipo de conductas suelen quedar dentro de lo que se denomina como "excepción personal o doméstica", que supone

87 ECLI:EU:C:2002:513

88 ECLI:EU:C:2008:727

89 ECLI:EU:C:2014:317

90 MORALEJO IMBERNÓN, N., *Los derechos de los menores… op cit*., p. 205.

una inaplicación de las disposiciones sobre protección de datos. Así lo recoge el art. 2.2. c) del RGPD, cuando establece una exclusión de su ámbito material para la "persona física en el ejercicio de actividades exclusivamente personales o domésticas". Esta misma previsión aparece también recogida en el artículo 2.2.a) de la Ley Orgánica de Protección de Datos.

Sin embargo, resulta crucial aclarar tres cuestiones fundamentales sobre esta excepción:

- La excepción no se aplica a los datos sensibles, que gozan de una especial protección y necesitan del consentimiento expreso del usuario afectado.
- Existe la posibilidad de que el sujeto afectado se oponga al tratamiento de sus datos personales incluso cuando se den los requisitos para ser considerada excepción personal.
- La inaplicación de las normas sobre protección de datos cuando se trata de una excepción personal no arrastra consigo la inaplicación de la normativa sobre derechos de intimidad, honor o imagen.[91]

Por lo tanto, para que se pueda aplicar esta excepción y quede descartada la aplicación de la normativa europea y española en materia de protección de datos, deben darse dos requisitos cumulativos:

- Que la persona que haya realizado un tratamiento de datos en la red social sea una persona física; quedan excluidas las personas jurídicas (a las que sí que les será de aplicación la normativa de protección de datos).
- Que la finalidad para la que realice dicho tratamiento sea para fines domésticos o familiares.

[91] MORALEJO IMBERNÓN, N., *Los derechos de los menores… op cit*., p. 207.

Ahora bien, el siguiente paso es averiguar qué se entiende por un fin doméstico o personal. La aclaración más cercana viene recogida en el propio Reglamento, Considerando 18, que recoge que "entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades". La Audiencia Nacional, en su Sentencia dictada por la Sala de lo Contencioso-administrativo, de 15 de junio de 2006[92] aclaró esta cuestión estableciendo que se debe interpretar este concepto como "las actividades que afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en estos ámbitos".

El TJUE, igualmente, en su Sentencia de 6 de noviembre de 2003, asunto C-101/01, caso *Lindquist*, antes citada, resolvió el caso de una catequista sueca que difundió en su página web información sensible, relacionada con la salud de otras personas que colaboraban con su iglesia. En este caso el TJUE fue tajante, al establecer que la excepción doméstica se debía interpretar en el sentido de que contempla solamente las actividades que se incluyen dentro del ámbito de la vida privada y familiar y que, en este caso, el tratamiento de los datos llevado a cabo por la catequista había sobrepasado dicho ámbito, al haber sido publicados, siendo accesibles a un grupo indeterminado de población.

En este mismo sentido se pronunció años más tarde en la STJUE de 1 de febrero de 2018, asunto C-25/17, caso Testigos de Jehová,[93] en la que se le planteaba si constituía dicha excepción doméstica el caso de un fichero creado por personas del grupo religioso Testigos de Jehová, donde se incluían datos de personas con las que habían contactado para difundir su religión. De nuevo, el TJUE argumentó que la creación de un fichero con datos sobre personas externas a la congregación no quedaba amparada por dicha excepción, dado que la predicación

[92] ECLI:ES:AN:2006:3077

[93] ECLI:EU:C:2018:551

tenía como finalidad difundir la religión entre personas que no eran de la comunidad, por lo que debían contactar con desconocidos, que son ajenos a la esfera privada de la organización.

Teniendo esto en cuenta, cabe pensar que, en el ámbito de las redes sociales pueden existir supuestos en los que los propios usuarios se pueden considerar responsables del tratamiento de datos de sus amigos o contactos en la red. El concepto de responsable del tratamiento de datos viene recogido en el artículo 4.7 del RGPD, que lo define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

Por lo tanto, la característica principal es que la persona determine los fines y los medios del tratamiento. En palabras del Grupo de trabajo del artículo 29 (art. 29 WP), creado por la Directiva 95/46/CE y que trataba cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD), en su Dictamen 1/2010, lo importante para determinar el responsable del tratamiento es que la persona en sí decida sobre elementos esenciales como el tipo de datos que se tratan, la duración o los sujetos que pueden acceder a los mismos. Por su parte, en la STJUE de 5 de junio de 2018, asunto C-210/16, caso *Wirtschaftsakademie Schleswig Holstein,*[94] se pone de manifiesto que el responsable del tratamiento lo será aun cuando no tenga acceso a los datos. Este caso versaba sobre la consideración de responsable del tratamiento de datos de un administrador de una página web. El TJUE determinó que la figura del administrador contribuía al tratamiento de datos personales, porque ponía a disposición de otra plataforma estadísticas y categorías

[94] ECLI:EU:C:2018:388

de datos de personas. Siguiendo con el GT29, en relación con las redes sociales, éste determinó en su Dictamen 5/2009 que los proveedores de servicios de redes sociales deben ser considerados responsables del tratamiento de datos de los usuarios por dos razones fundamentales:

- Por facilitar los medios que permiten que se traten los datos de los usuarios y la gestión.
- Por determinar la manera en la que se deben utilizar los datos con fines publicitarios.

Sin embargo, este Dictamen también señala que existirán algunos casos en los que los propios usuarios sean considerados responsables del tratamiento de datos de sus seguidores por no aplicarse la excepción personal del Reglamento:

- Cuando la actividad del usuario sobrepasa lo que se puede considerar como una actividad personal, es decir, pasa a ser una actividad profesionalizada, con colaboración de empresas.
- Cuando el usuario a pesar de tener un perfil en la red cerrado tiene una cantidad de seguidores no conocidos muy elevada.
- Cuando, independientemente del número de seguidores, el perfil de la persona es abierto, público a disposición de todos los usuarios de la red.

Procede desarrollar ahora cada uno de estos supuestos, que han sido tratados por la jurisprudencia europea y española.

Con respecto a la primera situación, la STJUE de 29 de julio de 2019 asunto C-40/17, caso *Fashion ID GmbH y C*[95] resolvió un procedimiento en el que el administrador de una página web de venta de moda introdujo la opción de marcar "me gusta", relacionándolo con Facebook, permitiendo recoger los datos de las personas que pasaban por la web. Lo que se planteaba en este caso es si el administrador se podía

[95] ECLI:EU:C:2019:629

considerar responsable del tratamiento de datos. El TJUE respondió argumentando que sí, debido a que cuando se inserta en una web un desvío a una red social se está contribuyendo a la recogida de datos que, de otro modo, no habría tenido lugar.

Con respecto a la segunda situación, cabe destacar que en el Dictamen no se menciona cuántos amigos constituyen un gran número de personas ni qué tipo de amigos se consideran "amigos" de verdad. La doctrina ha respondido a este segundo interrogante aportando el criterio de las "personas con las que se tiene un vínculo de amistad real o familiar".[96] La SAN de 15 de junio de 2006[97] se ha pronunciado también en los siguientes términos: "cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en estos ámbitos".

Finalmente, con respecto al último supuesto el TJUE en el caso *Lindquist* antes mencionado señaló que la excepción doméstica no se aplicaba al tratamiento de datos personales que consistiera en difundir dichos datos por Internet permitiendo su accesibilidad por un grupo indeterminado de personas. De este modo, si extrapolamos esta teoría a las redes sociales, si se tiene un perfil abierto no se puede pretender que no se acceda al contenido alojado en la propia red, ya que se está poniendo a disposición de la sociedad general. En estos casos de redes sociales, la figura del responsable del tratamiento se estira, desdoblándose en dos sujetos: el titular del perfil y el proveedor de la red social, que responderán no siempre de forma solidaria, sino en función de la participación de cada uno de ellos.

[96] MORALEJO IMBERNÓN, N., *Los derechos de los menores y las redes sociales… op cit.* p. 211.

[97] ES:AN:2006:3077

2. El menor como responsable del tratamiento de los datos personales

Pensemos en el siguiente supuesto: un menor se abre una cuenta en una red social y comienza a ganar seguidores, convirtiéndose en un *kidinfluencer*, firmando contratos con el consentimiento de sus progenitores con diversas marcas, hasta ganar cierta popularidad. Este caso se extiende más allá de la excepción personal o familiar antes mencionada, por lo que en este supuesto. El niño, niña o adolescente se estaría convirtiendo en un usuario de una red social que a su vez es responsable del tratamiento de los datos personales de sus seguidores. Cabe plantearnos si el régimen jurídico de las obligaciones de la normativa de protección de datos, a pesar de ser un menor el sujeto responsable se le impone también.

La Agencia Española de Protección de Datos (AEPD) en sus informes 0241/2011, 0184/2013 y 0197/2013 se ha pronunciado al respecto, al tener que responder a cuestiones que le planteaban precisamente cuando los usuarios, menores de edad, utilizaban las redes sociales con fines comerciales. En esos casos, la AEPD estableció una diferenciación entre los aspectos que regula la red social según sus propias normas de funcionamiento (como la política de privacidad elaborada por la propia red social, donde puede establecer especificidades acerca del tratamiento de los datos, el acceso, etc) y los aspectos sobre los que el usuario, que ahora se convierte en responsable de los datos, tiene plena libertad para actuar. Es en este segundo caso donde se le pueden exigir al usuario menor de edad ciertas obligaciones, que, en caso de incumplirse, derivarían en responsabilidad por incumplimiento.

Algunas redes sociales, como Instagram, tienen una opción que, llegado a un cierto número de seguidores se puede solicitar a la propia red social y, en caso de aceptarse, se activa. Se trata del modo de cuenta profesional, que otorga al beneficiario una serie de datos sobre el país de procedencia de sus seguidores, un rango con la edad de las

personas, el tipo de personas que ven sus historias (seguidores y no seguidores), la difusión que tienen sus historias y el impacto, el alcance general…

En primer término, dentro de los deberes que tiene el menor de edad responsable de los datos nos encontramos con el deber de informar a los afectados sobre la finalidad para la que capta los datos, la identidad y la dirección. Conjuntamente debe ofrecer la posibilidad de ejercer el derecho de acceso, rectificación, cancelación y oposición al tratamiento. Para facilitar dicha tarea, sería posible mediante la programación de un mensaje predeterminado que se le mandase a los afectados antes de otorgar el consentimiento o incluir dicha información en una parte visible de su perfil, como la descripción.[98]

Otro de los deberes que tiene el menor responsable es el de solicitar el consentimiento de sus seguidores afectados para recoger sus datos personales. No por seguir a una persona en concreto se debe entender que se está otorgando el consentimiento para el tratamiento de los datos personales, salvo que se hagan seguidores de una cuenta que claramente tiene fines comerciales y se haya anunciado como tal.[99] Precisamente todavía más, de tratarse de datos sensibles, el consentimiento debería ser explícito sobre dichos datos, ya que, como hemos anunciado anteriormente, la excepción personal no se aplica a este tipo de casos. Por su parte, el deber de solicitar autorización previa para enviar comunicaciones comerciales (conocidas como *spam*) también es relevante en estos casos.

[98] MORALEJO IMBERNÓN, N., *Los derechos de los menores y las redes sociales… op. cit.* p. 221.

[99] TRONCOSO REIGADA, A., "Redes sociales y protección de datos personales", en LÁZARO GONZÁLEZ, I.E., *Menores y nuevas tecnologías: posibilidades y riesgos de la TDT y las redes sociales*, Tecnos, Madrid, 2012, p. 94.

Igualmente, podría resultar aplicable el deber de atender las peticiones de acceso, rectificación, supresión o cancelación de datos personales siempre que se trate de información que esté al alcance del menor responsable.

Resulta interesante detenernos en el deber de confidencialidad, recogido en el artículo 5.1.f) del RGPD que conlleva la obligatoriedad de tratar los datos exclusivamente en el ámbito de la red social, sin que se puedan difundir o tratar fuera de la misma, siempre que no se cuente con el consentimiento del afectado. Este deber va de la mano del deber de seguridad, que conlleva la recomendación de cambiar de contraseña en cada red social que utilice o la renovación de la contraseña con una cierta periodicidad, para evitar ataques informáticos o fugas de información.

3. Los derechos de la infancia y adolescencia frente al responsable del tratamiento de sus datos personales

3.1. El derecho de acceso

El derecho de acceso aparece recogido en el artículo 15 del RGPD y en el artículo 13 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.[100] Su contenido habilita a su titular a solicitar información sobre el tratamiento de sus datos, por lo que su finalidad principal es permitir conocer y verificar la licitud del tratamiento de dichos datos.

De este modo, el artículo 15 del RGPD permite que se obtenga información sobre el acceso a los datos, los fines del tratamiento (15.1.a), las categorías de datos personales que se traten (15.1.b), los destinatarios o las categorías de destinatarios a los que se comunicaron o se van a comunicar los datos personales, en particular destinatarios en terceros países u organizaciones internacionales (art. 15.1.c), el plazo

[100] *BOE*, núm. 294, de 6 de diciembre de 2018.

previsto de la conservación de los datos o los criterios usados para determinar el plazo (art. 15.1.d), la existencia del derecho a solicitar del responsable la rectificación o supresión de los datos o la limitación del tratamiento (art. 15.1.e), el derecho a presentar una reclamación ante una autoridad de control (art. 15.1.f), cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen (art. 15.1.g) y la existencia de decisiones automatizadas, incluida la elaboración de perfiles, incluida información sobre la lógica aplicada, la importancia y las consecuencias de dicho tratamiento (art. 15.1.h). Además, al existir la posibilidad de transferir dichos datos a un tercer país, el precepto también contempla la obligatoriedad de informar sobre las garantías de dicha transferencia (art. 15.2).[101]

Si los datos que están siendo objeto de tratamiento han sido introducidos por el propio sujeto, basta con que este acceda a su perfil y realice las modificaciones que estime oportunas, debido a que esa información ha sido otorgada voluntariamente en el momento de darse de alta en la plataforma. Caso distinto son los datos que la plataforma ha obtenido en lo que se ha denominado por la doctrina como "colecta secundaria", es decir, aquellos datos procedentes de la actividad de delegación que lleva a cabo la red social con información sobre el historial de búsqueda, las interacciones, las cuentas bloqueadas, las imágenes que se han señalado como favoritas, las fotografías, los comentarios, los hipervínculos…). En este caso, al no haber sido otorgados dichos datos con el previo consentimiento del usuario, es necesario dirigirse frente al responsable del tratamiento de los datos. El artículo 15.3 establece que el responsable debe facilitarle al interesado una copia de los datos que se están utilizando en un plazo razonable. Sin embargo,

[101] Profundiza sobre este aspecto: ORTEGA GIMÉNEZ, A., "¿Y a la tercera va a la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EEUU", *Cuadernos de Derecho Transnacional*, vol. 16, núm.1, 2024, pp. 483-513.

si la cantidad de información que se está tratando es considerable, el responsable tiene la posibilidad de preguntar acerca de a qué datos se está interesado en acceder (considerando 63 del RGPD).

Relacionado con esta cuestión, y a pesar de la previsión del artículo 12.5 del RGPD, que contempla la gratuidad de este procedimiento, el artículo 15.3 prevé la posibilidad que tiene el responsable del tratamiento de solicitar el cobro de un canon razonable basado en los costes administrativos del procedimiento. En estos mismos términos se pronuncia el artículo 57.4 del RGPD, al establecer que: "Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control". Sin embargo, a pesar de que esta tarea pueda parecer complicada, lo cierto es que redes como Instagram, han diseñado este proceso para que los datos se expidan de manera automática mediante un sistema de descarga tras la solicitud.

3.2. El derecho de rectificación

Cuando los niños, niñas y adolescentes pasan su tiempo libre en las redes sociales, es posible que realicen comentarios que resulten ser falsos o que introduzcan datos erróneos que busquen ser modificados por el perjudicado. El derecho de rectificación permite a los usuarios perjudicados solicitar la corrección de errores y la modificación de datos que hayan quedado desfasados o sean inexactos, siendo su fin principal conseguir la veracidad de la información. Este derecho se recoge en el artículo 16 del RGPD, que declara el derecho del titular a obtener sin dilación indebida del responsable la rectificación de los datos personales inexactos, e incluso a solicitar una declaración adicional en caso de que no sea suficiente con la retirada de los datos. Este derecho se basa en el principio de calidad de los datos, que deben ser exactos y actualizados, tal y como señala el propio artículo 5.1.d): "se adoptarán todas las

medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que tratan". El artículo 19 impone la obligación al responsable del tratamiento de comunicar cualquier rectificación o supresión de los datos a cada uno de los destinatarios que lo hayan solicitado, salvo que sea imposible o exija un esfuerzo desproporcionado.

Dentro del ámbito de las redes sociales, puede pasar que los datos que se pretenden rectificar se hayan introducido por el propio solicitante de la retirada. En estos casos, las redes sociales suelen tener un apartado de Ajustes, donde se puede acceder y cambiar o corregir ciertos datos introducidos, como el nombre, la edad, el sexo. Pongamos como ejemplo una persona que ha cambiado de sexo; bastaría con que la propia persona accediera a su perfil y dentro de sus ajustes modificara su nombre y sexo, ajustándolo a la nueva realidad. Ahora bien, si la persona poseía fotografías publicadas en el perfil de otros amigos suyos, sería necesario comunicárselo para que fueran ellos los que eliminaran dichas fotografías o las modificasen.

3.3. El derecho al olvido (antes llamado de cancelación)

El derecho al olvido, recogido en el artículo 17 del RGPD otorga a su titular la potestad de solicitar la supresión de sus datos personales, incluso cuando estos hubiesen sido obtenidos con su consentimiento. Este precepto establece que el interesado puede solicitar sin dilación alguna la supresión de los datos personales al responsable cuando se dé alguna de las siguientes circunstancias:

- Que los datos ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados.
- Que el interesado retire el consentimiento que había otorgado en un primer momento.
- Que el interesado se oponga al tratamiento y no existan motivos legítimos para continuar con dicho tratamiento.

- Que los datos se deban suprimir para cumplir una obligación legal establecida en el Derecho la Unión o de los Estados miembros.
- Que los datos hayan sido obtenidos en relación con la oferta de servicios de la sociedad de la información.

Ahora bien, ¿qué razones pueden motivar a un sujeto para ejercitar este derecho en el ámbito de las redes sociales? En primer lugar, puede suceder que el usuario quiera cerrar su cuenta en la red social, de modo que prefiera eliminar todo el contenido subido hasta el momento. Por este motivo, sus datos ya no serían necesarios en relación con los fines para los que fueron recogidos (art. 17.1.a)).

En segundo lugar, también puede ocurrir que una persona que ha roto una relación de amistad o de pareja, decida que no quiere que su imagen conste en el perfil de esa otra persona. En este caso procedería el supuesto recogido en el artículo 17.1.b), relativo a la retirada del consentimiento otorgado en un primer momento. Este derecho de oposición operaría cuando no es aplicable la excepción doméstica.[102]

En tercer lugar, el derecho de olvido se relaciona en cierta manera con el derecho de oposición, recogido en el artículo 21, tal y como pone de manifiesto el artículo 17.1.c). De este modo, se reconoce el derecho de oposición a la persona afectada cuyos datos se estén tratando de acuerdo con el artículo 6.1.e) o f). El artículo 6.1.e) y f) hacen referencia al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los

[102] MORALEJO IMBERNÓN, N., *Los derechos de los menores y las redes sociales… op cit.* p. 295.

derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En cuarto lugar, resulta mucho más interesante la previsión referida al derecho al olvido de los datos obtenidos de una oferta de servicios de la sociedad de la información, cuyo origen se deriva del artículo 8.1, es decir, cuando la oferta se haya dirigido directamente a menores de 16 años. Sin embargo, Moralejo Imbernón señala que incluso dándose la circunstancia de ser menor de edad el usuario, su solicitud de retirar dicha información no será atendida cuando el tratamiento de sus datos sea necesario:

- "Para ejercer el derecho a la libertad de expresión y de información
- Para el cumplimiento de una obligación legal que requiera el tratamiento de los datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable
- Por razones de interés público en el ámbito de la salud pública
- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que la supresión de datos pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento
- Para la formulación, el ejercicio o la defensa de reclamaciones".[103]

Por lo tanto, la ponderación de cuándo debe prevalecer el derecho al olvido y cuando éste debe ceder frente al derecho a la libertad de expresión e información requiere un análisis cuidadoso y casuístico, ya que precisa poner en una balanza derechos fundamentales como son

[103] MORALEJO IMBERNÓN, N., *Los derechos de los menores y las redes sociales… op cit.,* p. 296.

el respeto a la vida privada y familiar, protegido por el artículo 7 de la Carta de los Derecho Fundamentales de la UE, la protección de datos de carácter personales (recogido en el art. 8) y, por otra parte, la libertad de expresión e información (art. 11) y la libertad de empresa (art. 16).

Precisamente sobre esta cuestión se pronunció el TJUE en su sentencia de 8 de diciembre de 2022, sobre el caso *Google*, asunto C-460/20,[104] girando sobre tres ejes fundamentales: la prevalencia del derecho al olvido frente al resto de derechos; las particularidades de las situaciones en las que la inexactitud del contenido enlazado supone un factor determinante de la ponderación entre los derechos fundamentales para determinar si procede la supresión; y cuestiones sobre la supresión de fotografías mostradas como previsualizaciones por el buscador.[105]

Con respecto a la primera cuestión, el TJUE pone de manifiesto que *a priori* se debe partir de la prevalencia de la protección de los derechos de los artículos 7 y 8 (vida privada y familiar y protección de datos) frente al derecho de acceso a la información por parte de los usuarios de una red social. Ese interés legítimo que ostentan los usuarios de la red en obtener información es precisamente el fundamento que permite la licitud del tratamiento de datos en virtud del artículo 6.1.f) del RGPD, que permitía el tratamiento de datos, recordemos, cuando sea necesario para satisfacer intereses legítimos perseguidos por el responsable del tratamiento, siempre que sobre esos intereses no prevalezcan los intereses, los derechos o las libertades fundamentales del interesado cuyos datos se están tratando.

La razón de esta prevalencia y protección del derecho al olvido se halla en que solamente cuando el contenido indexado al que lleva un enlace controvertido pueda tener interés público es cuando se debe plantear la prevalencia del derecho a la libertad de expresión y a la información,

[104] ECLI: EU:C:2022:962

[105] DE MIGUEL ASENSIO, P.A., "Derecho al olvido: precisiones en la jurisprudencia del Tribunal de Justicia sobre su ejercicio y alcance", *La Ley Unión Europea*, núm. 110, 2023, p. 2.

limitando y recortando el derecho al olvido; hasta entonces, no existe tal deber de ponderar. Incluso el Comité Europeo de Protección de Datos ya ha señalado en otras ocasiones[106] que cuando el gestor de un buscador recibe una petición de supresión de un enlace que redirige a una web donde constan datos personales, dicho enlace se tiene que eliminar salvo que el motor de búsqueda justifique que resulta estrictamente necesario que conste dicha información. Es necesario tener en cuenta que el derecho al olvido solo ampara la supresión de resultados de un buscador o motor de búsqueda cuando se encuentra información sobre un individuo introduciendo exclusivamente el nombre del afectado.

En concreto esta sentencia abarca la cuestión de cómo se deben tratar las situaciones en las que lo que se solicita no es la retirada de la información, sino la sustitución de una cierta información por otra, al resultar inexacta y la posibilidad de suprimir esos enlaces "equivocados". El TJUE acaba señalando que los criterios que se deben tener en cuenta para tomar la decisión son: en qué medida contribuye esa información a un debate de interés general, la importancia, el comportamiento anterior del afectado, el contenido en sí, la repercusión de esa información en su vida privada y la veracidad. Con respecto concretamente al factor de "contribuir a un debate de interés general", el TJUE recuerda que se refiere a las personas con notoriedad pública, es decir, en el caso de las redes sociales de los *influencers* o personas famosas fuera de redes, pero que tienen un gran número de seguidores. En el caso de tratarse de personas famosas o *influencers* prevalecerá el derecho a la libertad de expresión sobre el derecho a la vida privada y familiar.[107]

[106] Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD (primera parte), de 7 de julio de 2020. Disponible en el siguiente enlace: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_es.pdf

[107] DE MIGUEL ASENSIO, P.A., *"Derecho al olvido: precisiones en la jurisprudencia del Tribunal de Justicia sobre su ejercicio y alcance…", cit*., p. 3.

Con respecto a la segunda cuestión que trata la sentencia, relativa a la inexactitud del contenido al que desemboca un enlace como un elemento a tener en cuenta para ponderar entre el derecho a la vida privada y el derecho a la información, el TJUE pone de relieve que el derecho a la información no incluye la difusión de información que sea falsa o inexacta, que sea posible probarla, porque no se trate de meras afirmaciones. Cuando ocurra una situación como la descrita, el TJUE indica que al interesado le corresponde acreditar que la información es inexacta intentando evitar una carga excesiva a cualquiera del resto de las partes. Por lo tanto, se libera al interesado de aportar una resolución judicial acreditativa de dicha inexactitud permitiendo cierta flexibilidad.

Finalmente, con respecto a la última cuestión que aborda la sentencia, relativa a algunas cuestiones relacionadas con la supresión de imágenes mostradas como previsualizaciones por el buscador, al tratarse de nuevo de una ponderación entre el derecho a la información y el derecho a la vida privada, el TJUE establece que "debe atenderse de un modo determinante al contexto original de la publicación de dichas fotografías en Internet". Por ello, y teniendo en cuenta que las fotografías tienen un impacto mayor en la sociedad que un texto que se pueda encontrar en una publicación del usuario, el TJUE ha entendido que cuando al buscar a una persona aparezca directamente una fotografía que pueda redireccionar a más información sobre dicha persona física, eso implica una injerencia particularmente grave en el derecho a la imagen del afectado.

3.4. El derecho de oposición

El derecho de oposición se encuentra regulado en los artículos 6.1.e), 6.1.f) y 21 del RGPD, y otorga a su titular el derecho a oponerse en cualquier momento por motivos relacionados con su situación particular a que los datos personales relacionados con él sean objeto de tratamiento según lo dispuesto en el art. 6.1.e) y 6.1.f), incluida la elaboración de perfiles. Como hemos señalado anteriormente, los dos supuestos a los que hace referencia el artículo 6 son que los datos sean necesarios para

el cumplimiento de una misión realizada en interés público y que el tratamiento sea necesario para satisfacer intereses legítimos perseguidos por el responsable, siempre que sobre esos intereses no prevalezcan los derechos y libertades del interesado. Lo peculiar de este derecho es que exige que el particular motive su situación particular, es decir, se le obliga a razonar cuál es el interés o derecho que motiva su oposición.

El apartado segundo del artículo 21 del RGPD, relativo al segundo motivo de oposición, recoge la posibilidad de que los datos tengan por objeto la mercadotecnia directa, incluida la elaboración de perfiles. En este caso, el precepto amplía la protección, al establecer que se puede ejercer este derecho en todo momento. En el ámbito de las redes sociales, la negativa al tratamiento de datos puede ser exclusivamente a que se traten ciertos datos o incluso a que el perfil se incluya en motores de búsqueda, lo que supondría que es accesible por terceros, por lo que se estarían cediendo datos que requieren un consentimiento expreso por parte del titular.[108]

4. Régimen de responsabilidad por daños causados por una infracción de la normativa de protección de datos en el Reglamento general de protección de datos

4.1. Sujetos responsables: encargado y responsable

Si partimos de la base de que el sujeto responsable del tratamiento de datos personales ha incumplido alguno de los deberes que le confiere el Reglamento o se ha incumplido alguno de los derechos que puede ejercer el interesado con respecto al tratamiento de sus datos, el RGPD establece claramente quiénes son los sujetos responsables.

[108] Esta opinión relativa a que la inclusión del perfil en un motor de búsqueda supone una auténtica cesión de datos es defendida por: TRONCOSO REIGADA, A., *"Redes sociales y protección de datos personales…", cit*., p. 101.

El artículo 82 establece el derecho de toda persona que haya sufrido daños y perjuicios, ya sean materiales o inmateriales como consecuencia de una infracción del Reglamento a solicitar y recibir una indemnización por parte del responsable o encargado del tratamiento de dichos datos. A nivel interno, España otorga un mayor nivel de protección, ya que amplía estos sujetos (responsable y encargado) en el artículo 30 de la LOPD, de modo que abarque también la labor del representante designado en la UE por el responsable del tratamiento de los datos que, de acuerdo con el artículo 3.2 RGPD esté sujeto a esta normativa, aunque no se encuentre dentro del territorio de la UE. Es decir, se considerará responsable al representante nombrado en sede europea que trate datos sobre personas que se encuentren en España, a pesar de que este esté establecido fuera de la UE.

Ahora bien, una vez identificados los sujetos ¿qué debe entenderse por responsable y por encargado? El responsable es quien de manera individual o conjunta determina los fines y los medios del tratamiento (art. 4.7 RGPD), mientras que el encargado es quien trata los datos por cuenta del responsable (art. 4.8 RGPD). Siendo así, el encargado solo deberá responder de los daños y perjuicios que cause por el tratamiento de los datos cuando no ha cumplido con las obligaciones que el Reglamento impone de manera exclusiva a los encargados, o cuando ha actuado al margen o en contra de las instrucciones dadas por el responsable. Por su parte, el responsable responderá por los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto en el Reglamento. El régimen de responsabilidad es mayor para el responsable que para el encargado.

Si en el tratamiento de datos resultan responsables más de un responsable o encargado o tanto el encargado como el responsable son responsables de haber causado un daño, el tipo de responsabilidad será solidaria, para poder garantizar una indemnización efectiva al afectado (art. 82.4). Igualmente, este mismo precepto, en su apartado quinto prevé la posibilidad de la repetición interna, al establecer que cuando el responsable o encargado se haya hecho cargo del pago del total de la indemnización, tiene derecho a reclamarle al resto de participantes de

la conducta lesiva la parte de indemnización correspondiente a su parte de responsabilidad por los daños causados (art. 82.5). Además, desde la mencionada STJUE, de 6 de noviembre de 2003, Asunto C-101/01, se entiende que las obligaciones y las responsabilidades de los responsables del tratamiento de datos personales de terceros se aplican también a los denominados *influencers*, es decir, aquellas personas que no se encuentran amparadas por la excepción doméstica, dadas las altas cifras de seguidores que poseen; sin perjuicio de que además incurran en intromisiones en los derechos al honor, a la intimidad y a la propia imagen.[109]

4.2. Criterio de imputación

Con respecto al criterio de imputación, la normativa anterior al RGPD, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos,[110] contemplaba un régimen de responsabilidad objetiva de los responsables del tratamiento, ya que bastaba con que existiese un nexo causal entre los daños y el incumplimiento de la normativa. En el Considerando 55 se establecía incluso que solo se podía eximir al responsable si demostraba que no le era imputable el hecho perjudicial y, principalmente, si demostraba que la responsabilidad era del interesado o se había dado un hecho de causa mayor.

Sin embargo, la actual normativa no contempla causas de exoneración ni supuestos de fuerza mayor, lo que la doctrina ha interpretado como una flexibilización del criterio de imputación, pasando a ser ahora la responsabilidad *cuasiobjetiva*, por culpa levísima, que requiere de la

[109] GARCÍA GARNICA, M.C., *"Responsabilidad civil y redes sociales. Especial consideración a los daños sufridos o causados por menores de edad…", cit*., p. 99.

[110] *DOCE*, núm. 281, de 23 de noviembre de 1995.

exigencia del artículo 82.3 para que el culpable pueda exonerarse; es decir, debe demostrar que en modo alguno es responsable del hecho que ha causado los daños y perjuicios.

El responsable, para demostrar que no ha causado los daños que se le imputan, basándose en el principio de responsabilidad proactiva que se infiere del RGPD, puede acreditar su buena diligencia por diversas vías que le ofrece el propio Reglamento, tales como el nombramiento de un Delegado de Protección de Datos, que seguirá las instrucciones del responsable o encargado; la adopción de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, como puede ser la seudonimización y el cifrado de los datos personales (art. 32.1.a), la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas (art. 32.1.b), la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente técnico (art. 32.1.c) o un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento (art. 32.1.d); la notificación de las violaciones de seguridad a los interesados sin dilación indebida (arts. 33 y 34); la elaboración de planes que evalúen el impacto de los riesgos a la protección de datos (art. 35); la adhesión a códigos de conducta aprobados para contribuir a la correcta aplicación del Reglamento (art. 40).

4.3. El concepto de daños y perjuicios y su cuantificación

El RGPD contempla el concepto de daños y perjuicios en sentido amplio, en atención al principio de reparación íntegra, mediante una indemnización total y efectiva por los daños y perjuicios sufridos (tal y como señala el Considerando 146). De existir daños materiales, estos deben ser ciertos y probados. Por lo que respecta a los daños morales, estos también se encuentran incluidos en el RGPD. Este hecho es

significativo, ya que en la normativa anterior (la Directiva 95/46) solo se exigía la reparación del perjuicio sufrido, lo que hizo que la doctrina se encontrase dividida entre quienes entendían que solo se refería a los daños físicos y los que defendían la inclusión de los daños morales.[111]

La doctrina pone de relieve que lo cierto es que el TEDH ha reconocido en un mayor número de ocasiones como daño, el daño moral, en vez del físico, por lo que el paso que dio el Reglamento supone un gran avance.[112]

Profundizando en el daño moral, este debe ser determinado por los tribunales de primera instancia y no se puede revisar en casación, salvo en supuestos de arbitrariedad o situaciones manifiestamente injustas o que adolecen de un error notorio. El Tribunal Supremo ya ha sentado jurisprudencia[113] acerca de la reparación del daño moral, que en ningún caso puede ser simbólica, ya que esto redundaría en una práctica por parte del infractor consistente en continuar con su conducta, al no verse castigado. Con respecto a la valoración del daño moral esta se deberá hacer atendiendo a la gravedad de la lesión producida, la permanencia en el tiempo de la lesión, la difusión y la relevancia del medio en que se ha difundido.

Procede ahora realizar un análisis del sentido del artículo 82 del RGPD, que ha sido desgranado por el TJUE en su reciente sentencia de 11 de abril de 2024, asunto *juris* C-741/21,[114] en torno a la cual realiza una serie de reflexiones acerca de la determinación de la cuantía de la indemnización que tiene derecho a recibir la persona que sufre daños y perjuicios, ya sean materiales o inmateriales, a causa de una infracción del RGPD. En concreto responde a las siguientes cuestiones: los

[111] Así lo señala AGÜERO ORTIZ, A., "Derecho a la propia imagen y divulgación en prensa de fotos obtenidas en Facebook", *Derecho Privado y Constitución*, núm. 38, 2021, p. 59.

[112] GARCÍA GARNICA, M.C., *"Responsabilidad civil y redes sociales. Especial consideración a los daños sufridos o causados por menores de edad…", cit*., p. 102.

[113] En este sentido, la STS 512/2017, de 22 de septiembre.

[114] ECLI: EU:C:2024:288

requisitos del derecho a la indemnización; la responsabilidad en caso de error de una persona que actúa bajo la autoridad del responsable; y la determinación de la cuantía de la indemnización.

A modo de apunte, la sentencia versaba sobre una cuestión prejudicial planteada por un tribunal alemán en base a una demanda interpuesta por un abogado contra una sociedad que operaba una base jurídica de la que el abogado era cliente. El abogado reclamaba una indemnización por daños y perjuicios por haber sufrido daños como consecuencia de un incorrecto tratamiento de sus datos personales, al haber sido víctima de la mercadotecnia directa, mediante la remisión de folletos de publicidad a pesar de haber ejercido su derecho de oposición. A pesar de que pueda resultar lejano a nuestro tema de estudio, el dato que debemos tener en cuenta es que el abogado era una persona física, que bien podría tratarse de un menor de edad, por lo que todas las conclusiones extraídas de esta sentencia resultan relevantes para el caso de que este mismo supuesto se plantee siendo el afectado un niño, niña o adolescente.[115]

Comenzando a analizar la primera cuestión resuelta por el TJUE, relativa a los requisitos del derecho de indemnización, el tribunal alemán se planteaba si es posible considerar que la mera infracción del RGPD supone por sí misma un daño o perjuicio que da derecho a una indemnización de forma automática, en concreto, cuando la disposición infringida otorga un derecho subjetivo al afectado.[116]

[115] DE MIGUEL ASENSIO, P.A., "Determinación de la indemnización por daños derivados de infracciones del Reglamento General de Protección de Datos. Sentencia del Tribunal de Justicia 3ª 11 abril 2024, asunto, C-741/21: juris", *La Ley Unión Europea*, núm. 125, 2024, p. 2.

[116] DE MIGUEL ASENSIO, P.A., "Determinación de la indemnización por daños derivados de infracciones del Reglamento General de Protección de Datos. Sentencia del Tribunal de Justicia 3ª 11 abril 2024, asunto, C-741/21: juris", *La Ley Unión Europea*, núm. 125, 2024, p. 2.

Ante esta primera cuestión, el TJUE reiteró el mismo argumento que ya había defendido en su sentencia de 25 de enero de 2024, caso *MediaMarktSaturn*, asunto C-687/21,[117] en la que estableció que el derecho a una indemnización recogido en el artículo 82 requiere de la concurrencia de tres requisitos acumulativos: la existencia de unos daños y perjuicios materiales o inmateriales, la infracción del RGPD y una relación de causalidad entre los daños producidos y la infracción. Por lo tanto, la conclusión a la que se llega es que, por sí sola, la mera comisión de una infracción del RGPD, aunque otorgue un derecho a la persona física a reclamar, no constituye un daño indemnizable. Incluso si atendemos al artículo 79 RGPD, que confiere a todo interesado el "derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales", no se debe interpretar en el sentido de un derecho automático a una indemnización, sino a la vía que la norma habilita para ejecutar y hacer valer dicho derecho. Es necesario por tanto añadir un plus, consistente en la demostración de la relación entre el daño causado y el incumplimiento. En el caso concreto, la relación entre la pérdida de control de sus datos a pesar de haber ejercido el derecho de oposición y los daños causados.

En relación con la segunda cuestión resuelta, relativa la responsabilidad en caso de error de una persona que actúa bajo la autoridad del responsable de los datos, el responsable de los datos en el caso pretendía quedar exento de la responsabilidad por no ser él el responsable del hecho que desencadenó los daños, sino que lo era una persona que actuaba bajo su autoridad. Por lo tanto, su argumentación se basaba en que el artículo 82.3 establece que, si el responsable del tratamiento demuestra que de modo alguno ha causado daños y perjuicios, se encuentra exento de responsabilidad.

[117] ECLI: EU:C:2024:72

Para resolver esta cuestión, el TJUE se basa en su propia jurisprudencia anterior[118] relativa al artículo 82, que establece un régimen de responsabilidad por culpa, recayendo la carga de la prueba en el responsable del tratamiento y no en la víctima. Por ello, le corresponde a este desvirtuar la presunción de que ha tenido un papel activo en la causación del daño. La conclusión que se puede extraer sobre esta segunda cuestión es que, aunque la infracción causante de los daños sea imputable al comportamiento de un empleado que actúa orientado por el responsable del tratamiento que no actuó conforme a las indicaciones de este, esto no es óbice para excluir la responsabilidad del responsable. En palabras de la doctrina: "En caso de violación de la seguridad de los datos personales por una persona que actúe bajo la autoridad del responsable del tratamiento, éste solo puede quedar exento de responsabilidad si demuestra que no existe una relación de causalidad entre el eventual incumplimiento de sus obligaciones de que los datos sean tratados de manera que se garantice una seguridad adecuada y los daños y perjuicios sufridos por el interesado".[119]

Con respecto a la tercera cuestión, relativa a la determinación de la cuantía de la indemnización, el TJUE señala que no se deben aplicar los criterios del artículo 83 del RGPD para calcular el importe de las multas administrativas. Además, en la propia cuestión prejudicial se le preguntaba si a estos efectos era necesario tener en cuenta el número de infracciones que le afecten al interesado. El TJUE respondió separando el artículo 82, relativo al derecho de indemnización, del artículo 83, relativo a las multas administrativas, ya que señaló que su contenido es diferente. El artículo 82 tiene una finalidad compensatoria, pero no punitiva, ya que permite compensar íntegramente los daños y perjuicios sufridos, mientras que el artículo 83 sí que tiene una función punitiva. Siendo así, no es posible aplicar los criterios para determinar la cantidad

[118] STJUE de 21 de diciembre de 2023, *Krankenversicherung Nordhein*, C-667/21. ECLI: EU:C:2023:1022.

[119] DE MIGUEL ASENSIO, P.A., *"Determinación de la indemnización por daños derivados de infracciones del Reglamento General de Protección de Datos…", cit*., p. 3.

de la indemnización a los que se refiere el artículo 83 (tales como la gravedad de la infracción o el grado de responsabilidad), dado que los fines son diferentes. La finalidad del artículo 82, que solo pretende compensar, determina que el único criterio que se deba tener en cuenta sea el de los daños y perjuicios que efectivamente ha sufrido el interesado, independientemente de que se hayan cometido varias infracciones. Para obtener la cuantía exacta será necesario aplicar la normativa nacional.

Ya en la sentencia de 4 de mayo de 2023, *asunto Österreichische Post AG*, C-300/2021,[120] el TJUE señaló que: "los jueces nacionales deben aplicar las normas internas de cada Estado miembro relativas al alcance de la reparación pecuniaria, siempre que se respeten los principios de equivalencia y de efectividad del Derecho de la Unión". Por lo tanto, la primera conclusión que podemos extraer es que, al no existir una normativa uniforme en materia de cuantificación, existirán diferencias significativas entre los distintos Estados miembros. Yendo incluso más allá, al ser las redes sociales un ámbito tan hiperconectado y con alcance mundial, es habitual que se planteen resarcimientos con elementos transfronterizos.[121]

Por eso, si nos fijamos en los diferentes foros de competencia que establece el artículo 79.2. del RGPD, nos encontramos con que es común en estas situaciones internacionales ejercitar acciones contra un responsable o un encargado del tratamiento de datos para reclamar daños y perjuicios del artículo 82. En tal supuesto, se puede optar entre los tribunales de varios Estados Miembros, pues el artículo 79.2 ofrece la posibilidad de reclamar ante los tribunales de la residencia habitual del interesado o ante cualquier Estado miembro donde el responsable o el encargado tenga su establecimiento. Este aspecto no debe resultar

[120] ECLI: EU:C:2023:370.

[121] DE MIGUEL ASENSIO, P.A., "Requisitos del derecho a indemnización en el Reglamento General de Protección de Datos", *La Ley Unión Europea*, núm. 115, 2023, p. 6.

baladí, ya que dependiendo del Estado ante el que se litigue se estará eligiendo a su vez una normativa procesal aplicable al caso y unas determinadas normas de conflicto, como veremos a continuación.

5. Especial mención al caso *Meta Platforms*

El TJUE dictó el 4 de julio de 2024 su famosa sentencia *Meta Platforms e.a.,* asunto C-252/21 *(Conditions générales d'utilisation d'un résau social*),[122] que supuso un antes y un después en la interpretación de ciertas cuestiones del RGPD, al imponer a grandes empresas con relevancia patente en el mundo digital ciertas restricciones y establecer un estándar mínimo de tutela del derecho a la protección de datos. Para emitir su pronunciamiento, el Tribunal parte de la base de los riesgos que conlleva para la empresa el tratamiento de ingentes cantidades de datos personales y la amplitud del tratamiento que se lleva a cabo.

El litigio principal tiene como base el tratamiento de datos por parte de *Meta Platforms Ireland*, como prestadora del servicio de las redes sociales Facebook, Instagram y WhatsApp. Los datos objeto de tratamiento no eran exclusivamente los proporcionados por el propio usuario durante la apertura de la cuenta en la red, sino otros datos de los usuarios obtenidos de su actividad fuera de la red social, como las consultas genéricas en Internet o en otras aplicaciones de terceros. Estos datos de terceros se obtienen mediante *cookies*, interfaces integradas y otros métodos informáticos que el usuario ha consentido al aceptar las condiciones generales del servicio en la creación de su cuenta.[123]

Como señala De Miguel Asensio, esta sentencia trata las siguientes cuestiones fundamentales: la amplitud de los datos tratados y la inclusión de datos sensibles; la insuficiencia de la ejecución del contrato de

[122] ECLI: EU:C:2023:537

[123] DE MIGUEL ASENSIO, P.A., "Redes sociales y datos personales: bases jurídicas para el tratamiento e implicación de las autoridades de defensa de la competencia", *La Ley Unión Europea*, núm. 117, 2023, p. 2.

prestación de servicio de red social para fundamentar la licitud del tratamiento; y la insuficiencia del argumento de la satisfacción de intereses legítimos del operador de la red como base de licitud del tratamiento.

Con respecto a la primera cuestión, relativa a los datos personales que puede abarcar el tratamiento por parte de una red social y su relación con los datos sensibles, el artículo 9 recoge una serie de datos personales que deben ser protegidos especialmente debido a que pueden causar ciertos riesgos en derechos y libertades fundamentales. Por ello, queda prohibido su tratamiento salvo que se dé alguna de las circunstancias enumeradas en el apartado 2), entre las que se encuentra que se haya otorgado el consentimiento expreso para su tratamiento y que los datos que se estén tratando se hayan hecho manifiestamente públicos por el afectado. En concreto, se consideran datos sensibles según el artículo 9: "los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física".

En relación con esta cuestión, el primer aspecto que se aborda es, en relación al tratamiento de datos personales, en concreto a los datos relativos a las consultas que realiza el usuario en Internet, en qué medida ese tipo de tratamiento afecta a los datos sensibles o a categorías especiales de datos protegidas por el artículo 9 del RGPD. Para el TJUE lo relevante es si el tratamiento que realiza el operador de la red social permite revelar información incluida en el artículo 9, independientemente de que esa información sea exacta y de la finalidad de dicho tratamiento. Es decir, si los datos que obtiene la red social de información alojada en la propia red (pongamos que un usuario tiene cuenta en Facebook y aloja información) o en las otras redes (ese mismo usuario tiene también una cuenta de Instagram donde cuelga fotografías, interacciona con los demás usuarios dando *like*) permiten revelar información de esas categorías protegidas sobre ese mismo usuario o sobre cualquier persona física (por ejemplo, un hermano del usuario), deberemos aplicar el

artículo 9. Sobre este aspecto, en el apartado 72 de la sentencia señala el TJUE: "parece que el tratamiento de los datos relativos a la consulta de los sitios de Internet o de las aplicaciones en cuestión puede, en determinados casos, revelar tal información, sin que sea necesario que dichos usuarios introduzcan en ellos información registrándose o efectuando pedidos en línea".

Por lo tanto, una vez se ha comprobado que estamos ante el tratamiento de un dato sensible del artículo 9, el siguiente paso es valorar cuándo operan las excepciones del artículo 9.2 y, por lo tanto, es posible dicho tratamiento. Como en el ámbito de las redes sociales resulta complejo saber con certeza cuándo el interesado ha otorgado expresamente su consentimiento, el TJUE se inclina por atender a las situaciones en las que se debe entender que el interesado ha hecho público de manera manifiesta los datos personales, estando entonces ante una excepción a la prohibición del tratamiento de datos. Para identificar esas situaciones, la sentencia proporciona una serie de pautas que parten de la premisa de que solo opera la excepción cuando conste que el interesado "ha pretendido de manera explícita y mediante un acto positivo claro hacer accesibles al público en general los datos personales en cuestión" (apartado 77 de la sentencia).[124]

La primera pauta es que el mero hecho de que el usuario consulte en servidores de Internet o dentro de redes sociales cierta información, esto no significa que haya hecho manifiestamente públicos los datos, por lo que la excepción no operaría y no se podrían tratar los datos sensibles. Sin embargo, si el usuario ha realizado ciertas acciones como compartir por sus redes sociales un cierto contenido, realizar comentarios en publicaciones o ha dado me gusta a cierto contenido, todas estas acciones requieren un análisis particularizado. De modo que, cuando la configuración de la red social permita que el comportamiento

[124] DE MIGUEL ASENSIO, P.A., *"Redes sociales y datos personales: bases jurídicas para el tratamiento e implicación de las autoridades de defensa de la competencia… op. cit*., p. 4.

del usuario (los me gusta, los comentarios, las publicaciones compartidas) sea accesible al público general, al quedar visible, esto sí supondría una apertura de información del usuario, ya que es consciente de que toda la población puede ver su comportamiento. Si, por el contrario, esas interacciones solo están disponibles para un número reducido de personas, se entiende que no opera la excepción.

En palabras de De Miguel Asensio, "Solo cuando el operador de la red social ofrece al usuario una configuración individual, mediante la que puede expresar claramente con pleno conocimiento de causa su decisión de que tales datos resulten accesibles a un número ilimitado de personas, cabrá considerar que el usuario en cuestión ha hecho manifiestamente públicos esos datos que le conciernen, a los efectos del artículo 9.2º.e) RGPD".[125] Cuando no se cumpla esa publicidad manifiesta, solo es posible el tratamiento de datos sensibles por parte del operador de la red social cuando cuente con el consentimiento explícito del usuario.

La segunda cuestión resuelta por el TJUE fue la insuficiencia de la ejecución del contrato como justificante para la licitud del tratamiento de los datos. Como ya señalamos en apartados anteriores, el artículo 6.1 del RGPD contiene una lista de situaciones en las que el tratamiento de datos está permitido, y en concreto, en el ámbito de las redes sociales, el apartado b) contempla que se considera lícito el tratamiento de datos necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. Es decir, para que opere esta causa de licitud se requiere que el tratamiento se considere necesario para poder ejecutar el contrato.

[125] DE MIGUEL ASENSIO, P., "El tratamiento de datos personales por redes sociales a la luz de la sentencia Meta Platforms". Blog de Pedro de Miguel, 10 de julio de 2023. Disponible en el siguiente enlace: https://pedrodemiguelasensio.blogspot.com/2023/07/el-tratamiento-de-datos-personales-por.html

Pero ¿qué se debe considerar necesario? Pues bien, el Comité Europeo de Protección de Datos ya señaló en sus Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6.1.b) del RGPD[126] que la expresión "necesario" debe entenderse en un sentido restrictivo, de modo que no es suficiente con que el tratamiento se considere útil para ejecutar el contrato, sino que es necesario que no existan otras vías menos invasivas. De hecho, que el tratamiento de datos se mencione en el contrato no es determinante para decidir sobre la necesidad de dicho tratamiento para la ejecución del contrato, sino que el responsable debe acreditar que la ejecución del contrato no se puede llevar a cabo de manera efectiva sin dicho tratamiento. En palabras del TJUE en el apartado 98 de la sentencia comentada: "debe ser objetivamente indispensable para conseguir un fin que forme parte integrante de la prestación contractual destinada al interesado, es decir, el responsable debe demostrar "por qué el objeto principal del contrato no podría alcanzarse sin el tratamiento en cuestión".[127]

La tercera cuestión que trata el tribunal se refiere al concepto de intereses legítimos del operador como fundamento para justificar la licitud del tratamiento de datos. El artículo 6.1.f) del RGPD establece la licitud del tratamiento si es necesario para la satisfacción de intereses legítimos perseguidos por el responsable. Sin embargo, se debe ponderar este interés con los derechos del interesado. De este modo, solo se permite el tratamiento cuando los derechos del interesado no prevalezcan sobre los intereses del responsable. En este punto en concreto, el TJUE hace una mención específica a los derechos de los niños, a los que se les debe prestar una especial atención, en concreto cuando el tratamiento no se dé en circunstancias que razonablemente quepa esperar (apartados 111 y 112 de la sentencia).

---

[126] Disponible en el siguiente enlace: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_es.pdf

[127] DE MIGUEL ASENSIO, P.A., *"Redes sociales y datos personales: bases jurídicas para el tratamiento e implicación de las autoridades de defensa de la competencia…"*, *cit*., p. 6.

Ahora bien, ¿qué considera el tribunal "intereses legítimos"? En la sentencia se hace mención a la personalización de la publicidad, la mejora del producto, la información a la autoridad competente y la seguridad de la red. Resulta llamativo que, a pesar de que es posible pensar que la mercadotecnia directa pueda considerarse un interés legítimo del responsable, el TJUE rechaza esta opción cuando en la balanza de ponderación se encuentre el elemento de personalizar la publicidad a cambio de ofrecer los servicios de manera gratuita. Es decir, en redes sociales como Facebook o Instagram, que no requieren de ningún tipo de pago, el beneficio que obtienen dichas empresas es precisamente esa posibilidad de conseguir información para afinar la publicidad que se dirige a los usuarios. Y es que, como pone de manifiesto en el apartado 117 de la sentencia "pese a la gratuidad de los servicios de una red social en línea como Facebook, el usuario de esta no debería esperar razonablemente que, sin su consentimiento, el operador de esa red social trate los datos personales de ese usuario con fines de personalización de la publicidad". Esto hace que el interés del empresario en llevar a cabo una personalización deba caer frente al derecho del usuario a la protección de sus datos personales.

Habiendo tratado los aspectos fundamentales sobre los que el TJUE se pronunció en esta sentencia, procede ahora adentrarnos en el corazón de este asunto, es decir, la razón última por la que las empresas de redes sociales quieren operar con los datos de sus usuarios, lo que se ha denominado "publicidad comportamental". El Grupo de Trabajo de Protección de Datos del Artículo 29, en el Dictamen 2/2010, sobre publicidad comportamental en línea, de 22 de junio de 2010[128] definió la publicidad comportamental como "aquella publicidad que se basa en la observación continuada del comportamiento online de los individuos".

[128] Disponible en el siguiente enlace: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_es.pdf

Lo que caracteriza a la publicidad comportamental es la utilización de técnicas de segmentación que hacen que terceros puedan analizar el comportamiento del usuario en base a las acciones que realiza online (búsquedas en el servidor, los *clicks* que hace en un anuncio concreto, el tiempo que se detiene en cada publicación). De este modo, el tercero obtiene la capacidad de desarrollar un perfil del individuo, que usará para enviarle publicidad personalizada con sus intereses.

Para poder realizar esta recopilación de datos, se realiza un rastreo de la actividad a través de las *cookies* que se instalan en los servidores de búsqueda. De este modo, no se está rastreando directamente al individuo, sino que éste al hacer uso del servicio del navegador, acaba siendo objeto del rastreo de las cookies. En atención a todas estas características llegaríamos a la conclusión de que se podría definir como publicidad comportamental aquella publicidad que aparece durante la navegación en un servidor como resultado de la actividad online del sujeto desarrollada durante un tiempo en ese mismo servidor.[129] Esto ocurre porque realizando un perfil del usuario se le puede dirigir una publicidad que cause un mayor impacto cuando esté navegando por la red, optimizando los recursos de las empresas de publicidad mediante la instalación de las cookies.[130]

El artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante, LSSI)[131] señala que "Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los

[129] PÉREZ BES, F., *La publicidad comportamental online*, UOC, Barcelona, 2012, p. 13.

[130] ORTIZ LÓPEZ, P., "Cookies, fingerprinting y la privacidad digital", en LÓPEZ CALVO, J. (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer, Madrid, 2019, p. 970.

[131] *BOE* núm. 166, de 12 de julio de 2002.

fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal". Este artículo sirve para entender qué son las *cookies*, y es que ya apunta que sirven para el almacenamiento y la recuperación de datos. Pues bien, las *cookies* son "pequeños archivos de texto alfanumérico que, bien el equipo gestor de la página web, bien un tercero proveedor de publicidad coloca en el ordenador de un usuario cuando navega por la web para registrar información diversa sobre éste, incluyendo sus preferencias y hábitos, para después recuperarla y nutrir sus bases de datos para personalizar la configuración de las páginas, ofreciéndole una publicidad que se adecue a sus características propias".[132]

Al basarse el funcionamiento de las *cookies* en la minería de datos, esta actividad queda sujeta al RGPD, que impone para su válido tratamiento el otorgamiento del consentimiento del usuario. Para que dicho consentimiento sea válido, es necesario que se emita sin engaño, intimidación o violencia. *A sensu contrario*, el consentimiento no es válido cuando exista presión o una imposibilidad de ejercer la libre voluntad, ya que se estaría coartando la libre disposición del individuo. Ahora bien, ¿se considera que el consentimiento que otorgan los usuarios de la red se emite de modo forzado, porque la alternativa opuesta implica el pago de una cantidad para evitar el tratamiento de sus datos personales?

En este sentido se ha pronunciado el TJUE en su Sentencia de 22 de abril de 2021, *Facebook v. Bundeskartellamt*, C-252/21,[133] en relación con la posibilidad de negarse a la prestación del consentimiento cuando se ofrezcan opciones adecuadas. En este sentido el órgano establece que pueden existir ocasiones en las que la red impida el acceso a la web si no se aceptan las cookies, siempre que ofrezca una alternativa, que no tiene que ser gratuita. Por lo tanto, se puede deducir que se

[132] Definición extraída de: TRUJILLO CABRERA, C., "Los nuevos cookie walls: Consent or pay. A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio de 2023", *Revista de Derecho Civil*, vol. XI, núm. 2, 2024, p. 81.

[133] ECLI:EU:C:2023:537

puede ofrecer y es lícita una alternativa de pago como mecanismo que otorgue validez y licitud al consentimiento del titular, que será suficiente para legitimar el tratamiento de sus datos personales para obtener información y crearle un perfil (publicidad comportamental), siempre que esa alternativa no implique un coste sustancial o desproporcionado.

Sin embargo, esta postura ha sido duramente criticada por la doctrina,[134] ya que entienden que, si bien es cierto que el TJUE ha permitido la opción de que existan casos en los que se ofrezca una alternativa a la cesión de datos, no ha indicado que se pueda realizar en todos los casos, ni ha planteado casuísticas concretas en las que se pudiera plantear esta opción, por lo que se achaca una falta de claridad en el pronunciamiento emitido.

En segundo lugar, con respecto a la propia idea en sí, critican que se está creando una pretendida libertad en la elección de las partes, cuando la alternativa a la negativa del tratamiento de datos consiste en pagar una cantidad de dinero. En este sentido ya se ha demostrado que ante la posibilidad de usar un servicio de manera gratuita a pesar de vender los datos personales y la opción de pagar por protegerlos, los consumidores optan por la opción gratuita, lo que se ha denominado "efecto del coste cero". Este tipo de decisiones se adoptan de forma irracional sin pensar en las consecuencias, por el simple hecho de que la atracción a lo gratuito les impide valorar la realidad.[135] Profundizando más, existen evidencias de que, para el consumidor, cuando se le presentan dos opciones diferentes, siendo una a un precio reducido y otra totalmente gratuita, no se plantea siquiera la opción de precio reducido, por el mero hecho de tener un precio.[136]

---

[134] TRUJILLO CABRERA, C., *"Los nuevos cookie walls: Consent or pay. A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio de 2023…", cit*., p. 100.

[135] TAMAYO VELASCO, J., "Big data, competencia y protección de datos: el rol del Reglamento General de Protección de Datos en los modelos de negocio basados en la publicidad personalizada", *Revista de Estudios Europeos*, 2021, núm. 78, p. 186.

[136] GAL, M., y RUBINFELD, D. L., "The Hidden Costs of Free Goods: Implications for Antitrust Enforcement", *Antitrust Law Journal*, 2016, vol. 80, núm. 401, p. 528.

En el caso concreto de Meta, que tiene el monopolio en el mercado de sus redes sociales, no existen otras alternativas, por lo que la potestad de elegir entre las opciones viables es nula para el consumidor, que solo puede optar entre aceptar el servicio con las condiciones que tengan a bien imponerle o rechazar el servicio, quedando sin posibilidad de una alternativa. En este mismo sentido se ha pronunciado el Tribunal Constitucional en su sentencia 27/2020, de 24 de febrero,[137] en la que se expresa del siguiente modo: "el uso de condiciones generales empleado en este procedimiento de contratación online, sus características, y la falta de capacidad de los usuarios/consumidores para negociar el clausulado, arroja dudas relevantes sobre la existencia de una adecuada manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta indiscriminadamente". No se trata en este caso de que no exista cognoscibilidad por parte del usuario de la red de que efectivamente están tratando sus datos, ya que es bien sabido por todos que cuando se realiza una búsqueda o incluso en una conversación se apunta la necesidad de un producto, el buscador arrojará una respuesta próximamente, sino de que no se le ofrece ninguna vía asumible para poder declinar el tratamiento de sus datos en otra red.

[137] ECLI:ES:TC:2020:27

PROBLEMÁTICA DE LAS REDES SOCIALES EN LAS RELACIONES PRIVADAS INTERNACIONALES

Cuando tratamos temas relacionados con la sociedad de la información, como es el caso de las redes sociales, y más concretamente la protección de datos de la infancia y adolescencia en las redes sociales, independientemente de la perspectiva jurídico-privada que adoptemos, no podemos dejar pasar por alto las relaciones privadas internacionales que surgen en el marco digital. El Derecho internacional privado juega un papel fundamental, ya que no son pocas las ocasiones en las que al navegar por una red social se abandona la página, que puede ser española y se entra en una nueva pestaña, controlada por una empresa sometida a una jurisdicción extranjera o que puede contener elementos extranjeros.

Pongamos un pequeño ejemplo para ilustrar la situación: la empresa Kiwo es propietaria de una red social con el mismo nombre. Los usuarios se registran completando una serie de datos, como el nombre, la edad, el correo electrónico, el número de teléfono y ciertos cuestionarios sobre sus gustos para personalizar el contenido. Esa empresa, establecida en España, posteriormente vende esos datos a una empresa sita en Canadá, sin el consentimiento previo por parte de los usuarios. Cuando los usuarios (que pueden tener diversa procedencia, dado el carácter mundial de las redes sociales) descubren que se ha producido tal agravio, deciden emprender acciones legales para reclamar la tutela emanante de su derecho a la protección de datos. Ahora bien, ¿qué tribunales resultarán competentes para conocer de la demanda que interpongan? Y, de resultar competentes, ¿qué ley será la aplicable?

Este supuesto, que parece totalmente ficticio, tiene su base en un caso real, en el que la Comisión de Protección de Datos de Irlanda ha impuesto una multa de 1.200 millones de euros a Meta Platforms, que es la compañía matriz de Facebook, Instagram y Whatsapp, por haber

incumplido la normativa de protección de datos, al haber realizado una transferencia de datos desde la Unión Europea a Estados Unidos (caso ya expuesto).[138] Pues bien, desde la perspectiva del Derecho internacional privado, la problemática en relación con la protección de datos se basa en la determinación de la competencia del órgano jurisdiccional y la ley aplicable que utilizará para resolver la cuestión que se le plantee.

Sin embargo, antes de estudiar esta cuestión se hace necesario entender ante qué tipo de contrato estamos, ya que las controversias surgirán entre los usuarios de la plataforma y la red social en sí. Debemos partir de la base de que cada red social es diferente, por lo que es necesario estudiar los términos y condiciones de cada una de ellas para intentar descifrar el contrato que subyace entre el usuario y la red. Lo cierto es que las principales redes sociales como son Facebook, Instagram, Twitter, LinkedIn, Google y WhatsApp comparten una serie de características comunes, como son:

- Que la relación entre el usuario y la red social es contractual, lo que despliega efectos jurídicos.
- Que las empresas gestoras de las redes se autodefinen como proveedoras de servicios y denominan a las prestaciones objeto del contrato "servicios".
- Que la mayoría de las empresas distinguen entre los "servicios", que es todo aquello a lo que se obligan para cumplir con el contrato y el "contenido", que es la información y el material que el usuario publica cuando se abre una cuenta en la red social.
- Con respecto a los "servicios", las empresas ofrecen una gran variedad, como aplicaciones, notificaciones, correo electrónico, *web*…

[138] ORTEGA GIMÉNEZ, A., "Las nuevas tecnologías y la protección de datos de carácter personal desde el Derecho Internacional Privado: redes sociales de internet y cloud computing", *Actualidad Civil*, núm. 12, 2023, p. 4.

- Las redes sociales otorgan una licencia de *software* dentro de sus servicios para que el usuario lo utilice de forma gratuita.
- El usuario le otorga a cambio a la red social una licencia por la que se le da a la empresa el derecho a transferir su información y el contenido que el usuario sube, comprendiendo el uso, la administración, la copia, la modificación, la distribución, la publicación y el tratamiento de los datos.[139]

Por lo tanto, atendiendo a todas estas características comunes podríamos definir dicho contrato como uno de prestación de servicios.

Si se planteara un litigio en el ámbito de la UE y resultara de aplicación el Reglamento (UE) núm. 1215/2012 del Parlamento europeo y del Consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil[140] (conocido como Reglamento Bruselas I bis, RBIbis), es necesario tener en cuenta el concepto de contrato de prestación de servicios que se contempla en tal instrumento. En este sentido, el artículo 7.1.b) RBI bis, al igual que la norma a la que sucedió, el RBI, no otorgan un concepto de prestación de servicios, tal como ha señalado el TJUE.[141] En concreto, de la STJUE de 23 de abril de 2009, Asunto C-533/07, *Falco Privats-tiftung y Rabitsch,*[142] apartado 33, se desprende que el concepto de servicio tiene un contenido autónomo, lo que significa que dicha definición se debe interpretar de conformidad con los propios términos, espíritu y finalidad de la norma y con arreglo a lo que el RBI bis entiende por servicio, independientemente de que dicho

[139] SÁNCHEZ CANO, M.J., y ROMERO MATUTE, Y., "El régimen jurídico de las redes sociales y los retos que plantea el acceso a dichas plataformas", *Cuadernos de Derecho Transnacional*, vol.13, 2021, p. 1141.

[140] *DOUE* L 351. Disponible en: https://www.boe.es/doue/2012/351/L00001-00032.pdf

[141] STJUE (Sala Cuarta) 23 abril 2009, *Falco Privats-tiftung y Rabitsch*: Asunto C533/07 (ECLI:EU:C:2009:257); STJUE (Sala Cuarta) de 25 febrero 2010, *Car Trim*: Asunto C-381/08, (ECLI:EU:C:2010:90).

[142] ECLI:EU:C:2009:257

concepto difiera de la definición otorgada por la normativa interna de cada Estado miembro. Esta misma visión la comparte amplia parte de la doctrina internacional-privatista,[143] que conciben el término en un sentido amplio y más económico que jurídico, siendo la obligación principal del contrato la realización de una actividad consistente en dar, hacer o no hacer una cosa, a título oneroso, gratuito o lucrativo.[144]

Partiendo de esta base, se podría argumentar que no se podría entender que se da este contrato al no existir una remuneración dineraria al prestador de los servicios. Sin embargo, el contrato no es gratuito, ya que la contraprestación que ofrece el usuario es su licencia para que la red social realice un tratamiento de su información. Ya el TJUE ha tenido ocasión de pronunciarse al respecto[145] y entiende que el sentido de prestación no debe configurarse exclusivamente como dineraria, sino cualquier otro contenido que tenga un valor económico para el prestador de los servicios.[146]

---

[143] En este sentido: CANEDO ARRILLAGA, M.P., "Notas breves sobre la sentencia del TJUE (Sala Cuarta) de 25 febrero 2010 (Car Trim: asunto C-381/08): los contratos de compraventa y los contratos de prestación de servicios en el Reglamento 44/2001", *Cuadernos de Derecho Transnacional*, vol. 3, núm. 1, 2011, p. 266; DE MIGUEL ASENSIO, P.A., "Sobre el concepto de contrato de prestación de servicios en el DIPr. comunitario", Blog de Pedro de Miguel Asensio, 2009. Disponible en el siguiente enlace: https:// pedrodemiguelasensio.blogspot.com/2009/05/sobre-el-concepto-de-contrato-de.html

[144] CALVO CARAVACA A. L., y CARRASCOSA GONZÁLEZ, J., *Derecho Internacional Privado*, vol. II, Comares, Granada, 2018, p. 924.

[145] STJUE (Sala Primera) de 19 de diciembre de 2013, *Corman-Collins SA vs. La Maison du Whisky SA*: C/9-12. ECLI:EU:C: 2013:860

[146] SÁNCHEZ CANO, M.J., y ROMERO MATUTE, Y., *"El régimen jurídico de las redes sociales y los retos que plantea el acceso a dichas plataformas…"*, *cit.,* p. 1142.

1. La determinación de la competencia judicial internacional en materia de redes sociales en el ordenamiento jurídico español

1.1. Perspectiva general bajo el prisma del Reglamento (UE) 1215/2012 (Reglamento Bruselas I bis)

Para determinar la competencia judicial internacional de un tribunal español cuando se plantee un caso en materia digital existe una amplia variedad de normas de origen comunitario, convencional y autónomo, por lo que se hace necesario establecer un orden o prelación en su aplicación. Nos encontramos con el Reglamento (UE) 1215/2012 (RBI bis); el Convenio relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Convenio de Lugano);[147] La Ley Orgánica 7/2015, de 21 de julio por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial[148] (LOPJ). Para saber cuándo debe aplicarse una norma u otra será necesario atender a las cláusulas de compatibilidad previstas en el artículo 73 del RBI bis y en el artículo 64.2 a) del Convenio de Lugano, que conducen a priorizar el domicilio del demandado en Noruega, Islandia o Suiza o bien la existencia de un acuerdo de sumisión expresa a favor de los tribunales de Noruega, Islandia o Suiza como elemento determinante de la aplicación del Convenio de Lugano con preferencia al RBI bis.

La fundamentación de la competencia de los tribunales en un foro u otro del RBI bis o del Convenio de Lugano, según el caso, dependerá de cuál sea el petitum de la demanda y de cómo se califique el mismo. Partiendo de una pretensión en la que se reclame una indemnización por daños y perjuicios por vulnerar el derecho a la protección de datos dentro de una red social, los criterios que atribuyen competencia a los tribunales de Estados miembros de la Unión Europea tanto en el

[147] *L 339*.

[148] *BOE* núm. 174, de 22 de julio de 2015

RBI bis como en el Convenio de Lugano, con carácter general, son los siguientes: el foro del domicilio del demandado (art. 4), es decir, los tribunales del Estado miembro en el que tenga su domicilio el causante del daño (independientemente del lugar en el que se haya producido el daño); el foro de la sumisión expresa o tácita (arts. 25 o 26), el foro del lugar donde deba cumplirse la obligación que sirve de base a la demanda (art. 7.1 RBI bis), así como el foro del lugar en el que se haya producido o pueda producirse el hecho dañoso (art. 7.2), que atribuye competencia a los tribunales del Estado miembro del lugar en el que nace la responsabilidad.

Si la petición de indemnización por daños y perjuicios derivados de la vulneración del derecho a la protección de datos es objeto de una calificación extracontractual, esto implicará la puesta en funcionamiento del foro correspondiente al lugar en que se ha producido el hecho dañoso (arts. 7.2 RBI bis o 5.2 Convenio de Lugano), entendido este en un doble sentido: como el lugar donde se ha producido el acto causal generador del daño o como el lugar donde se manifiestan las consecuencias lesivas. Debe advertirse que este foro de competencia solo será posible aplicarlo cuando el demandado se encuentre domiciliado en un Estado miembro de la UE, pues, en caso contrario, en virtud del artículo 6 del RBI bis o 4 del Convenio de Lugano, habrá que fundamentar la competencia en las normas de origen autónomo de cada Estado miembro, en el caso de España, en la LOPJ.

La doctrina pone de manifiesto que el país donde ocurre el hecho dañoso debe interpretarse en el sentido del país donde efectivamente se materializa el daño, o el país donde ocurre el hecho causal o el país donde se encuentra el fichero de datos.[149] Y es que, el TJUE ha venido entendiendo que el foro del lugar donde se realiza el acto causal permite reclamar por la totalidad de los daños que se le hayan generado

[149] ORTEGA GIMÉNEZ, A., *"Las nuevas tecnologías y la protección de datos de carácter personal desde el Derecho Internacional Privado: redes sociales de internet y cloud computing…", cit.*, p. 6.

al usuario, mientras que el tribunal del lugar donde se manifiestan las consecuencias lesivas solo permite conocer a dicho tribunal por los daños causados en su territorio, lo que obligaría al perjudicado a tener que interponer una multiplicidad de demandas para reclamar por los daños causados en cada uno de los lugares. Puesto que los daños que se generan en el mundo digital se extienden por múltiples países debido al alcance global de internet, el criterio del "mosaico" ha sido sustituido por el del "centro de intereses del perjudicado", lo que permite interponer la demanda ante un órgano jurisdiccional vinculado al usuario de internet, para que conozca de la totalidad de los daños que se le hayan generado.[150] Estas reglas que parecen tan bien definidas tienen sus matices, ya que, por ejemplo, si el hecho ilícito consiste en recoger datos en España para almacenarlos en un fichero en otro país, por ejemplo, Francia, el lugar del daño será tanto España como Francia.

Ahora bien, puesto que, pese a la producción del daño, existe un contrato entre dos partes, es más lógico calificar como contractual la pretensión de indemnización por los daños y perjuicios causados por el tratamiento de los datos, especialmente, si hay que recurrir al contrato para determinar el alcance de la ilicitud de la conducta.[151] En este caso, la competencia de los tribunales para conocer de esta indemnización derivada de la infracción de los derechos del usuario puede venir determinada por el foro del artículo 7.1 del RBI bis o artículo 5.1 del Convenio de Lugano, que la otorga a los tribunales del país donde se haya cumplido o deba cumplirse la obligación que sirve de base a la demanda y, tratando el contrato de una prestación de servicios, tal lugar será aquel en el que, según lo pactado en el contrato, hayan sido o deban ser prestados los servicios. Es decir, si seguimos con el ejemplo anterior, si según el contrato los datos se debían tratar en Francia y allí son objeto

[150] CEDEÑO HERNÁN, M., "La tutela transfronteriza de los derechos de la personalidad en la Unión Europea", *Cuadernos de Derecho Transnacional* (Marzo 2021), vol. 13, Nº 1, pp. 110-133.

[151] DE MIGUEL ASENSIO, P., "Competencia y Derecho aplicable en el Reglamento General sobre Protección de datosde la Unión Europea", *REDI*, vol. 69, 2017, p. 96.

de un tratamiento ilícito, los tribunales franceses serán competentes, independientemente de que también lo sean los tribunales del país del domicilio del demandado o los tribunales ante los que se hayan sometido expresa o tácitamente las partes.[152]

En este segundo supuesto, es decir, cuando se realice una calificación contractual de la pretensión, los foros que operarían cuando se presente una reclamación por daños y perjuicios por vulnerar el derecho a la protección de datos en las redes sociales, en los casos en que tal vulneración derive de un incumplimiento contractual por parte de la empresa, son, por orden:

- Los tribunales elegidos por las partes por sumisión expresa o tácita (arts. 25 y 26 RBI bis) (arts. 23, 24 Convenio de Lugano), pudiendo derogarse un posible acuerdo de sumisión expresa exclusivo, a través de la posterior sumisión tácita del demandado.
- No existiendo dicho acuerdo, de manera alternativa, cualquiera de estos otros tribunales:
    - Los tribunales del Estado miembro del domicilio del demandado (arts. 4 RBI bis o 2 Convenio de Lugano).
    - Los tribunales del Estado miembro del lugar donde se haya cumplido o debiera cumplirse la obligación que sirve de base a la demanda (art. 7.1 RBI bis) (art. 5.1 Convenio de Lugano), siempre que el demandado esté domiciliado en un Estado miembro de la UE.

Por lo que se refiere al foro de la sumisión expresa, el acuerdo de sumisión es un pacto que realizan las partes para someter el litigio a la jurisdicción de un determinado órgano jurisdiccional, otorgándole competencia para conocer del asunto. Esta sumisión se puede realizar de

[152] ORTEGA GIMÉNEZ, A., *"Las nuevas tecnologías y la protección de datos de carácter personal desde el Derecho Internacional Privado: redes sociales de internet y cloud computing…", cit.*, p. 6.

dos formas: mediante un acuerdo expreso que realicen las partes (sumisión expresa) o mediante ciertas conductas que denoten la voluntad de las partes de someterse a un determinado órgano jurisdiccional (sumisión tácita). En materia de protección de datos, ni el RBI bis ni el Convenio de Lugano presentan especialidades. Por lo que respecta a la LOPJ, esta dispone que, "en aquellas materias en que una norma expresamente lo permita, los Tribunales españoles serán competentes cuando las partes, con independencia de su domicilio, se hayan sometido expresa o tácitamente a ellos" (art. 22 bis LOPJ).

El Reglamento Bruselas I bis exige para que el acuerdo de sumisión expresa sea válido que se formalice de forma escrita o verbalmente, pero con confirmación escrita (art. 25.1.a RBI bis); que se realice en una forma que se ajuste a los hábitos que las partes tengan establecidos (art. 25.1.b RBI bis) o en una forma conforme a los usos comerciales o que las partes conozcan o deban conocer (art. 25.1.c RBI bis). La peculiaridad del acuerdo de sumisión expresa contemplado en el artículo 25 del RBI bis radica en que tiene carácter exclusivo y solo puede ser derogado por sumisión tácita de las partes, a no ser que estas hayan dispuesto que el acuerdo no sea exclusivo. Se entiende que las partes se han sometido tácitamente a un órgano jurisdiccional cuando el demandante interpone una demanda y el demandado comparece sin impugnar su competencia (art. 26 RBI bis).

Estos foros concurren con los previstos en el artículo 79.2 del RGPD cuando el interesado ejercite una acción frente al responsable o encargado del tratamiento de datos por infracción de alguna obligación impuesta por el RGDP. Recordamos que este precepto atribuye competencia a los tribunales del Estado miembro en el que el responsable o encargado del tratamiento tenga un establecimiento. Este lugar puede coincidir o no con el domicilio del demandado, pues el domicilio es, según el artículo 63 del RBI bis, el lugar en el que la sociedad tenga su sede estatutaria, su administración central o su centro de actividad principal, mientras que el RGPD utiliza un concepto amplio y flexible de establecimiento, entendiendo que este se encuentra en cualquier lugar donde se realice una actividad real y efectiva, aunque sea mínima,

ejercida mediante una instalación estable.[153] Estos tribunales del lugar donde se halle el establecimiento del demandado podrán conocer de la totalidad del daño causado al interesado. Igualmente, el artículo 79 del RGPD habilita al interesado a que interponga la demanda ante los tribunales de su propia residencia habitual, lo que requiere no la simple presencia del usuario en ese lugar, sino una cierta duración y estabilidad suficiente en ese país. Este foro debe entenderse también en el sentido de que habilita al tribunal de la residencia habitual del interesado para conocer de la totalidad de los daños que se le hayan generado y no solo los que se hayan producido en el país de su residencia habitual.[154]

Ahora bien, siendo los perjudicados por el tratamiento de datos los niños, niñas y adolescentes, bien puede considerarse que se trata de consumidores, lo que obliga a tener en consideración, además de las reglas de competencia del artículo 79 del RGPD los foros de protección de consumidores previstos en el régimen de Bruselas I bis y en el Convenio de Lugano.

1.2. El pacto de sumisión expresa en el ámbito de las redes sociales cuando se opera con usuarios considerados consumidores

Aplicando la teoría a la práctica, lo cierto es que la mayor parte de las grandes redes sociales realizan una distinción entre los usuarios que residen dentro y fuera de la UE, estableciendo cláusulas de sumisión expresa que otorgan la competencia a tribunales concretos. Todas las redes sociales parten de la base de acordar la atribución de competencia al tribunal del lugar donde está domiciliado el usuario de la red, para conocer de las disputas que tengan que ver con la utilización del servicio por el usuario y para el resto de cuestiones, a los tribunales del lugar donde se halle el domicilio del prestador del servicio, aunque presentan

[153] DE MIGUEL ASENSIO, P., "Competencia y Derecho aplicable en el Reglamento General sobre Protección de datos…", *cit*., p. 97.

[154] *Ibid.,* p. 99.

especialidades. En el caso de Facebook[155] e Instagram,[156] en las condiciones de uso se aprecia un pacto de sumisión expresa en favor de los tribunales de Irlanda, eso sí, para aquellos consumidores residentes dentro de la UE, ya que las condiciones cambian dependiendo del país de residencia del usuario. En el caso de Twitter,[157] para las personas residentes fuera de la UE se establece un pacto de sumisión expresa en favor de los tribunales de California, en Estados Unidos, mientras que si el usuario se encuentra en la UE acepta someterse a la jurisdicción de los tribunales irlandeses. Más interesante resulta sin duda el caso de Tik Tok,[158] que establece que la resolución de conflictos deberá ser resuelta por el Centro de Arbitraje Internacional de Singapur, imponiendo el arbitraje de modo imperativo, formándose el Tribunal por tres árbitros y siendo el idioma el inglés.

Pues bien, en todas estas redes sociales se incluye un acuerdo de sumisión expresa, que como ya hemos visto, es "un acuerdo que celebran las partes de una relación jurídica para someter los litigios que pudieran surgir o que ya hubieran surgido en relación con la misma, a los órganos jurisdiccionales de un determinado Estado".[159] Ahora debemos plantearnos si todos estos acuerdos son válidos o si pueden ser considerados abusivos.

Se debe partir de la base de que esta investigación se va a hacer desde la óptica de los usuarios de las redes sociales residentes en la UE (niños, niñas, adolescentes y jóvenes que residen en la UE) y que se trata de consumidores. En las cláusulas que las plataformas utilizan en

[155] Condiciones de uso disponibles en el siguiente enlace: https://es-es.facebook.com/legal/terms

[156] Condiciones de uso disponibles en el siguiente enlace: https://help.instagram.com/581066165581870/?locale=es_ES

[157] Condiciones de uso disponibles en el siguiente enlace: https://x.com/en/tos

[158] Condiciones de uso disponibles en el siguiente enlace: https://www.tiktok.com/legal/page/row/terms-of-service/es

[159] RODRÍGUEZ BENOT, A., *Manual de Derecho internacional privado*, Tecnos, Madrid, 2024.

sus contratos, se dispone que se otorga competencia a los tribunales del domicilio del consumidor. Por otro lado, todas las redes sociales mencionadas, salvo Tik Tok, tienen empresas filiales cuyo domicilio está en Irlanda.

La eficacia de estos acuerdos de sumisión expresa depende de que se respeten las condiciones previstas en los foros de protección del RBI bis contenidas en los artículos 17 y siguientes. Para empezar, el art. 18 estipula que cuando sea el consumidor el que interpone la acción, este podrá hacerlo ante los órganos jurisdiccionales del Estado miembro donde está domiciliada la otra parte contratante o ante los órganos jurisdiccionales de su propio domicilio como consumidor. Si es la empresa de redes sociales la que quiere interponer una acción contra el consumidor, éste solo puede interponerla ante los órganos jurisdiccionales del Estado miembro donde está domiciliado el consumidor). Ahora bien, existiendo un pacto de sumisión expresa que reúna los requisitos del artículo 19 del RBI bis, este acuerdo de sumisión expresa prevalecerá sobre los foros del artículo 18 mencionados.

El artículo 19 del RBI bis relativo a los pactos de sumisión expresa en el marco de los contratos de consumo establece tres requisitos para que el acuerdo de sumisión expresa con un consumidor sea válido: 1- que sea posterior al nacimiento del litigio. 2- que permita al consumidor ampliar las opciones del país en el que interponer la acción, además de los mencionados en el art. 18; 3- o que, habiéndose celebrado el contrato entre el consumidor y la red social estando ambos domiciliados en el mismo Estado miembro cuando celebraron el contrato, el acuerdo otorgue competencia a los tribunales de ese Estado miembro.

Ahora bien, ¿en qué sentido debe interpretarse el concepto de consumidor y cuando se considera que una persona es consumidor? El TJUE en reiterada jurisprudencia[160] ya ha puesto de manifiesto que se

[160] STJUE 14 marzo 2013, C-419/11, ECLI:EU:C: 2013:165; STJUE 25 enero 2018, C-498/16, ECLI:EU:C:2018:37; STJUE 23 diciembre 2015, C-297/14, ECLI:EU:C:2015:844

entiende por consumidor la persona física que realiza un acto de consumo, es decir, que adquiere un bien o servicio para un uso personal y no profesional. Debemos tener en cuenta que esta es una definición general de consumidor, que debe ser interpretada en el sentido del RBI bis, que solo protege con las reglas especiales de los artículos 18 y 19 al consumidor que contrate una venta a plazos de mercaderías, o un préstamo a plazos u otra operación de crédito vinculada a la financiación de la venta de tales bienes o al llamado consumidor pasivo, nuevo concepto que hace referencia al consumidor cuya otra parte contratante ejerza actividades comerciales en el Estado miembro del domicilio del consumidor o, por cualquier medio, dirige sus actividades a ese Estado miembro que recibe ofertas o publicidad en su propio domicilio, no aquel que se traslada a formalizar el contrato a otro país.[161] Esta cuestión debe captar toda nuestra atención, ya que dependiendo de que el usuario sea un consumidor o no lo sea en el sentido expresado por el TJUE, el pacto de sumisión expresa será o no válido, según se reúnan los requisitos mencionados en el art. 19 o no.

Si no existe acuerdo de sumisión expresa válido de conformidad con el art. 19 del RBI bis y es el consumidor el que interpone la demanda, el art. 18 le ofrece la posibilidad de interponer la demanda ante cualquiera de estos tribunales: el del Estado miembro del domicilio de la red social (Irlanda en la mayoría de casos) o el del Estado miembro de su propio domicilio. Todo ello, como se ha indicado, salvo que exista un pacto de sumisión expresa con los requisitos del art. 19. En caso de que sí exista acuerdo de sumisión expresa y cumpla el requisito del art. 19.3 del RBI bis, al ofrecer la posibilidad de atribuir competencia a los tribunales del Estado miembro donde estén domiciliados el consumidor y la otra parte contratante, permitirá demandar ante los tribunales del Estado miembro del domicilio del propio consumidor, por lo que no resultaría abusivo.

[161] STJCE 11 julio 2002, *Gabrie*l, Asunto C-96/00, ECLI:EU:C:2002:436; STJUE 7 diciembre 2010, *Pammer,* asuntos acumulados C-585/08 y C-144/09 (ECLI:EU:C:2010:740).

A estos efectos, para determinar si un pacto de sumisión expresa es abusivo hay que atender a lo dispuesto en los artículos 67.2 y 90 de la LGDCU, según los cuales, es abusiva "La previsión de pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor y usuario, al lugar del cumplimiento de la obligación o aquél en que se encuentre el bien si éste fuera inmueble".

Ahora bien, ¿qué pasaría si el usuario de la red social fuese un consumidor activo, no pasivo? En ese caso, dejarían de ser aplicables las previsiones protectoras contenidas en los artículos 17 y siguientes del RBI bis, aplicándose el régimen general contenido en el Reglamento. Los mecanismos que tendría para poder interponer una demanda, en ese caso, serían: un acuerdo de sumisión expresa a favor de los tribunales de un Estado miembro, de conformidad con el art. 25 del RBI bis, que ya no impone límite alguno en cuanto a la posibilidad de elegir a cualquier órgano jurisdiccional, pues ya no regirían los límites del art. 19. Además, podría recurrir a los foros generales del art. 4, domicilio del demandado (la red social), es decir, Irlanda[162] (en la mayoría de los casos) o el foro del art. 7.1.b) de los tribunales del Estado miembro del lugar en el que, según lo acordado en el contrato, se haya prestado o se deba prestar el servicio (en tal caso, siempre que el demandado esté domiciliado en un Estado miembro, lo que es el caso, ya que la empresa tiene su domicilio en Irlanda). Si no se hubiera pactado el lugar de prestación del servicio, habría que acudir al apartado c) de dicho artículo que nos remite al a) (lugar en el que se haya cumplido o deba cumplirse la obligación que sirva de base a la demanda). La doctrina ya ha puesto de manifiesto la dificultad que puede entrañar determinar en un contrato de prestación

[162] En este sentido habría que acudir al art. 63 del RBI bis, que nos da una definición de qué se debe interpretar por el domicilio de una sociedad o persona jurídica, entendiendo como tal: (a), su sede estatutaria; (b), su administración central o (c), su centro de actividad principal. En concreto, el apartado 2 del mismo artículo establece para el caso de Irlanda, que el concepto de sede estatutaria debe equipararse a una *registered office*, o *place of incorporation* (lugar de constitución) o, en caso de que no exista, el lugar conforme a cuya legislación se haya efectuado la *formation* (creación) de la sociedad o persona jurídica.

de servicios online qué debe entenderse por ese lugar, ya que la finalidad principal del art. 7.1 es establecer una conexión entre el tribunal del foro y el contrato, pues, por proximidad geográfica, debería estar familiarizado con esa tipología contractual. En un contrato de prestación de servicios la obligación que sirve de base a la demanda (art. 7.1.a) y el lugar de prestación del servicio es el que hayan pactado las partes.[163] Y, para los casos en que estas no hayan pactado expresamente dicho lugar, el TJUE afirma que se debe entender que dicho lugar es aquel en el que se prestan los servicios realmente.[164]

Recapitulando, hay que afirmar que, tratándose de usuarios consumidores protegidos por el RBI bis, en la medida en que las cláusulas que incorporan acuerdos de sumisión expresa previstos por las plataformas no establecen como única opción para el consumidor la necesidad de interponer la demanda ante los tribunales irlandeses, sino que reconocen también el foro del propio domicilio del consumidor, no se pueden considerar abusivos estos acuerdos de sumisión expresa, ya que lo que hacen en último término es ampliar los foros de competencia de los tribunales a los que pueden acudir.[165]

El Tribunal de Justicia de la Unión Europea en la sentencia de 25 de enero de 2018, caso C-498/16, *Schrems,*[166] ha tenido ocasión de pronunciarse acerca de cuestiones relacionadas con las demandas de

[163] DE MIGUEL ASENSIO, P. A., "El lugar de ejecución de los contratos de prestación de servicios como criterio atributivo de competencia", en FORNER DELAYGUA, J., GONZÁLEZ BEILFUSS, C., y VIÑAS FARRÉ, R. (coords.), *Entre Bruselas y La Haya. Estudios sobre la unificación internacional y regional del Derecho internacional privado. Liber amicorum Alegría Borrás*, Dykinson, Madrid, 2013, pp. 291-307.

[164] En este sentido: STJUE 10 septiembre 2015, *Ferho*, Asunto C-47/14, ECLI:EU:C:2015:574; STJUE (Sala Tercera) 15 junio 2017, *Kareda*: Asunto C-249/16, ECLI:EU:C:2017:472; STJUE 11 marzo 2010, *Wood Flour*, Asunto19/09, ECLI:EU:C:2010:137; STCE 9 julio 2009, *Air Baltic*, Asunto C-204/2008, ECLI:EU:C:2009:439; y STJUE 7 marzo 2018, *Air Nostrum*, Asuntos acumulados C-274/16, C-447/16 y C-448/16, ECLI:EU:C:2018:160

[165] SÁNCHEZ CANO, M.J., y ROMERO MATUTE, Y., *"El régimen jurídico de las redes sociales y los retos que plantea el acceso a dichas plataformas…", cit.,* p. 1146.

[166] ECLI:EU:C:2018:37.

usuarios de redes sociales por infracción de las normas de protección de datos personales por parte de los prestadores o encargados, cuando los usuarios son consumidores. Este caso versaba sobre una reclamación por daños en forma de indemnización por parte de un ciudadano austriaco con conocimientos sobre la legislación de protección de datos y Facebook. El TJUE se centra en interpretar ciertas cuestiones relativas a la protección de consumidores en el ámbito del Reglamento Bruselas I (en concreto los artículos 15 a 17). Sin embargo, esta doctrina jurisprudencial sigue plenamente vigente, ya que esos artículos se corresponden con los actuales artículos 17 a 19 del RBI bis.

Estos preceptos (arts. 17 a 19 RBI bis) otorgan un régimen de protección en el ámbito de la competencia judicial internacional en materia de consumo, como hemos señalado en apartados anteriores. El art. 17.1 RBI bis establece que solamente se aplica para los contratos celebrados por una persona, en concreto el consumidor, para un uso que se considere ajeno a su actividad profesional. En el caso resuelto en esta sentencia el TJUE configura la interpretación de consumidor en el contexto de las redes sociales. El ciudadano austriaco se abrió un perfil con fines exclusivamente privados y con un nombre de usuario ficticio, teniendo un total de 250 amigos. Sin embargo, a medida que avanzó el tiempo creó una página de Facebook donde informaba sobre su ligio contra la empresa, difundiendo información sobre protección de datos y haciendo publicidad de los libros sobre esta materia.[167]

La cuestión que se le plantea al TJUE era si el consumidor pierde su condición tras publicar libros sobre los derechos que ostenta, realizar charlas remuneradas sobre aspectos digitales de la red. Es decir, de lo que se trataba era de decidir si la finalidad personal que tenía en el uso de la plataforma al principio cuando creó la cuenta había pasado a ser una finalidad profesional del usuario, al obtener remuneración por

[167] DE MIGUEL ASENSIO, P.A., "Demandas frente a redes sociales por daños en materia de datos personales: precisiones sobre competencia judicial", *La Ley Unión Europea*, núm. 56, 2018, p. 4.

la actividad que desarrollaba y eso hacía que perdiera la condición de consumidor. El TJUE se pronunció estableciendo que el concepto de consumidor en el ámbito de las redes sociales se debe interpretar de modo restrictivo, por lo que las normas de protección del consumidor solo resultan de aplicación cuando la finalidad del contrato sea personal y no cuando se use la plataforma para fines profesionales. Es normal que en el uso de una red social el estatuto de consumidor pueda fluctuar al cambiar la actividad del usuario en la red y que solamente se puede invocar la condición de consumidor cuando el uso es no profesional y se ha mantenido en el tiempo. Lo relevante es que no se haga un uso esencialmente profesional de la plataforma y que el mismo se mantenga en el tiempo. Además, afirmó que el momento que se debe tener en cuenta para apreciar la condición de consumidor es el de la interposición de la demanda y no el momento de celebración del contrato (la apertura de la cuenta en la red social). Resulta interesante la puntualización que realiza el TJUE al señalar que es irrelevante la especialización del usuario en los servicios de la red, y es que el concepto de consumidor es independiente de los conocimientos que tenga el usuario sobre la normativa de protección de datos.[168]

Queda por resolver el campo de actuación de las reglas de competencia contenidas en el artículo 79 del RGPD en un caso en el que se ejerciten acciones civiles derivadas de la infracción de normas sobre protección de datos personales del RGPD por consumidores. Es decir, si se aplican en tal caso los foros del RBI bis o los del art. 79 del RGPD. Como se ha indicado, el art. 79.2. atribuye a los interesados la posibilidad de demandar al responsable o al encargado del tratamiento de los datos ante los tribunales de cualquier Estado en el que tenga un establecimiento la red social, o bien ante los tribunales de su propia residencia habitual. La doctrina afirma que los foros del RGPD se aplican de manera complementaria a los del RBI bis cuando el petitum de la demanda esté relacionado con la infracción de las normas del RGPD,

[168] *Ibid*., p. 7.

para no privar del efecto útil a los foros del artículo 79 del RGPD.[169] Así se desprende del artículo 67 del RBI bis, según el cual, "El presente Reglamento no prejuzgará la aplicación de las disposiciones que, en materias particulares, regulan la competencia judicial, el reconocimiento o la ejecución de las resoluciones contenidas en los actos de la Unión o en las legislaciones nacionales armonizadas en ejecución de dichos actos".

Pudiendo aplicarse también los foros del artículo 79 del RGPD para las demandas interpuestas por usuarios consumidores, debe recordarse que este precepto hace referencia a los tribunales del Estado miembro en el que el responsable o encargado del tratamiento de datos tenga cualquier establecimiento y no a los tribunales del Estado miembro del "domicilio", como, en cambio, hace el RBI bis. Asimismo, debe tenerse en cuenta que, en el RGPD, el concepto de establecimiento se debe entender en sentido amplio, flexible, como el lugar en el que se desarrolle cualquier actividad real y efectiva, por mínima que sea, siempre que la instalación sea estable, no siendo necesario que la acción se refiera al tratamiento que tiene lugar en el establecimiento concreto del país en el que se va a interponer la demanda.

La duda que subsiste es si el consumidor puede recurrir indistintamente a cualquiera de los Reglamentos o tendrían prioridad los foros del art. 79 del RGPD siempre que la acción verse sobre una infracción de las obligaciones impuestas por el RGPD, subsistiendo los foros del RBI bis en los demás casos. Esta segunda opción me parece más acertada, teniendo en cuenta el criterio de especialidad del RGPD.

[169] *Ibid.,* p. 9.

2. La determinación de la ley aplicable en materia de redes sociales en el ordenamiento jurídico español

Una vez se ha determinado la competencia de un tribunal sito dentro de la UE, el siguiente paso será averiguar qué ley resultará aplicable al caso. La respuesta dependerá igualmente, de cómo se califique la pretensión.

Cuando la reclamación tenga carácter contractual, el punto de partida será el Reglamento núm. 593/2008 del Parlamento europeo y del Consejo de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales (Reglamento Roma I),[170] que presenta la característica de ser de aplicación universal (art. 2), lo que significa que la ley designada por las normas de conflicto del Reglamento deberá aplicarse, aunque se trate de la ley de un Estado no miembro de la UE. Respecto a la ley aplicable, de conformidad con el artículo 3, será la ley elegida por las partes, siempre que se trate de una ley estatal y en vigor. No es necesario que la ley elegida guarde vinculación con el asunto. Si las partes no han elegido ninguna ley, en dicho caso se deberá acudir al artículo 4, que establece en relación con los contratos de prestación de servicios, la aplicación de la ley de la residencia habitual del prestador de los servicios,[171] sin que quepa acudir al reenvío, por lo que el Derecho aplicable será el Derecho material de dicho país. No obstante, esta ley puede quedar descartada en beneficio de la ley con los vínculos más estrechos (art. 4.3).

También el RRI establece en el art. 6 normas específicas para los contratos de consumo, de tal manera que se aplicará la ley del país en que el consumidor tenga su residencia habitual, siempre que el empresario ejerza o dirija sus actividades a dicho país. El apartado segundo de dicho artículo establece la prevalencia de la autonomía de la voluntad

[170] *DOUE* núm. 177, de 4 de julio de 2008. Disponible en el siguiente enlace: https://www.boe.es/buscar/doc.php?id=DOUE-L-2008-81325

[171] AGUILAR GRIEDER, A. H., "Alcance de los controvertidos artículos 3 y 4 del Reglamento (CE) núm. 593/2008: Perspectiva de lege lata y propuestas de lege ferenda", *Cuadernos de Derecho Transnacional*, vol. 6, núm. 1, 2014, pp. 45-67.

de las partes en la elección de la ley aplicable a los contratos de consumo. No obstante, según el artículo 6.2 del RRI, la ley que elijan las partes no puede suponer una pérdida de protección del consumidor, de modo que la ley elegida no puede privar al consumidor de la protección que le otorgarían las disposiciones no derogables de la ley de su residencia habitual. Además, para que dicho pacto de elección de ley sea válido es necesario que se den los requisitos del artículo 3.

Ahora bien, si el problema que se está intentando dirimir girara en torno a la protección de datos, sea cual sea la ley aplicable al contrato, el tribunal del Estado miembro de la Unión Europea que conociera del asunto, deberá aplicar imperativamente las reglas del RGPD, siempre que el asunto se incardine en su ámbito de aplicación territorial, que viene fijado en el artículo 3 del RGPD. Así lo dispone el artículo 9.2 del Reglamento Roma I, que obliga al tribunal del foro a aplicar las normas imperativas del foro, siendo las normas del RGPD normas del foro.

Para determinar el ámbito de aplicación territorial del RGPD hay que acudir a su artículo 3. De conformidad con este precepto, las normas del RGPD deben aplicarse para el tratamiento de datos personales en el contexto de actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no (art. 3.1.). Por establecimiento deberá entenderse a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable (Consideración 2 del RGPD). Igualmente, deberán aplicarse las normas del RGPD imperativamente, cuando el tratamiento de datos afecte a interesados que residan en la Unión cuando el responsable o encargado no esté establecido en la UE, siempre que las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la UE, aunque no se les requiera su pago, o cuando el tratamiento esté relacionado con el control de su comportamiento, en la medida en que este tenga lugar en la UE (art. 3.2 RGPD).

Por otro lado, cuando la reclamación verse sobre un aspecto extracontractual, no será aplicable el Reglamento (CE) núm. 864/2007 del Parlamento Europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales (Roma II),[172] puesto que las infracciones de las normas de protección de datos no están reguladas en este Reglamento. Así se desprende de su artículo 1.2. g), que excluye de su ámbito de aplicación las "obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación". En particular, la solicitud de indemnización por daños y perjuicios derivados del tratamiento de los datos personales por el responsable o encargado de dicho tratamiento infringiendo las normas del RGPD encajan en el concepto de difamación.[173]

Tales cuestiones deberán resolverse conforme al art. 10. 9 del Código Civil, que remite a la ley del lugar donde hubiere ocurrido el hecho del que deriven. La doctrina interpreta que esta ley es la del lugar en el que sufre el daño la persona perjudicada, que será la ley de su residencia habitual o centro de intereses.[174]

3. Nuevos métodos de resolución alternativa de conflictos: El "Tribunal Supremo de Facebook"

Dada la saturación del sistema judicial a la hora de resolver conflictos, por la ingente cantidad de asuntos que deben llevar, la idea de resolver las disputas relativas a usuarios en una red social se está haciendo cada vez más popular, a través de una modalidad de medios alternativos de resolución de conflictos. Estos han ido evolucionando dada la celeridad necesaria en el ámbito digital y han dado lugar a los llamados medios

[172] *DOUE* L 199, de 31 de julio de 2007.

[173] DE MIGUEL ASENSIO, P.A., "Competencia y Derecho aplicable en el Reglamento General sobre Protección de datos…", *cit.* p. 105.

[174] Ibid., p. 106.

de resolución de disputas en línea. Se trata de digitalizar el arbitraje, la mediación o la negociación. Sin embargo, aunque el sistema tiene indudables ventajas, como la rapidez y la especialización del órgano, también presenta inconvenientes, como el precio elevado del procedimiento y la necesidad de crear un órgano de apelación y la privatización de la administración de justicia.

En todo caso, en 2020 Facebook creó lo que denominó en un primer momento como "Tribunal Supremo de Facebook", y que, posteriormente, ha pasado a llamarse "Junta de Supervisión", mediante el documento "Carta de la Junta de Supervisión".[175] Este órgano toma decisiones de modo independiente sobre cuestiones en las que surjan conflictos entre la libertad de expresión y los derechos a la privacidad, la seguridad, la veracidad dentro de la red social de Facebook e Instagram. El artículo 2 le otorga potestad para poder conocer de recursos de revisión contra decisiones que tome Facebook sobre el usuario cuyos datos se han retirado o sobre la persona que solicitó la retirada cuando no forme parte de la red. Este órgano puede negarse a resolver un asunto que pueda tener implicaciones penales o administrativas.

El Tribunal tiene competencia para conocer sobre cualquier caso relacionado con contenidos de Facebook e Instagram sin tener en cuenta la localización de la víctima, ni la del creador de contenido. Con respecto a la composición del órgano está conformado por once miembros como mínimo, pudiendo llegar a cuarenta, elegidos por un periodo de tres años renovable hasta en tres ocasiones, con experiencia demostrada en temas como las nuevas tecnologías, los contenidos digitales y la gobernanza de datos, la libertad de expresión, el discurso cívico o la seguridad. Esto garantiza una especialización de sus miembros para la resolución del conflicto.

[175] SÁNCHEZ FRÍAS, A., "El Tribunal Supremo de Facebook: ¿un nuevo paso hacia la justicia sin Estado", *Cuadernos de Derecho Transnacional*, vol. 12, núm. 2, p. 1398.

Para comenzar el procedimiento la persona interesada tiene que presentar su requerimiento ante un panel designado de la Junta, que puede solicitar información adicional a Facebook. El órgano toma las decisiones por consenso o, en su defecto, por mayoría y, para ello, no aplica ni interpreta la ley de ningún Estado, sino que tomas las decisiones conforme a la política de contenidos y valores de Facebook, que se convierte así en una especie de "lex electrónica", formada por normas sobre seguridad, contenido inaceptable, integridad y autenticidad y respeto de la propiedad intelectual.[176] El carácter de estas normas no es jurídico, sino de principios o valores sociales, configurados por la comunidad que se ha desarrollado a lo largo del tiempo en la red social. Esta lex electrónica también incorpora otras normas internacionales sobre protección de derechos humanos.

Con respecto a los efectos que despliegan las decisiones, estas van más allá del caso sobre el que han decidido, pues tienen valor de precedente para otros casos que se consideren sustancialmente similares.

Por lo tanto, estaríamos ante un tribunal universal privado en materia de protección de derechos fundamentales, competente para conocer de daños producidos a los particulares por el contenido alojado o retirado de la red social.[177] Desde mi punto de vista esta iniciativa *a priori* positiva y novedosa presenta una serie de inconvenientes.

En primer lugar, a pesar de que se mencione en el documento fundacional el número aproximado de integrantes y su especialización por el conocimiento de numerosas materias, en ningún punto se hace referencia a la forma de elección, los criterios y los requisitos de los participantes. Para formar parte de un órgano que va a tomar decisiones que afectan a derechos de la personalidad, como son la imagen o el honor, es necesario que dicho tribunal lo configuren juristas, familiarizados

[176] SÁNCHEZ FRÍAS, A., *"El Tribunal Supremo de Facebook: ¿un nuevo paso hacia la justicia sin Estado…, cit.*, p. 1401.

[177] *Ibid.*, p. 1403.

con conceptos relacionados con el Derecho y con un criterio uniforme. Al no mencionarse los criterios de selección de los candidatos, este sistema induce a pensar que no existe objetividad y, por lo tanto, no genera seguridad a las partes. Se debería pasar por un proceso selectivo, posiblemente un examen para demostrar conocimientos y exigirse a los candidatos un compromiso de desempeñar su función con absoluta imparcialidad.

En segundo lugar, las competencias que ostenta el tribunal son muy limitadas, ya que solo se contempla la revisión de contenido que se solicita retirar o revisar, quedando fuera de su competencia otras cuestiones relevantes, como la indemnización por daños derivados del tratamiento de datos.

En ningún punto se establece en base a qué criterios se va a proceder a aceptar a trámite las solicitudes y cuándo se van a rechazar, por lo que el criterio puede resultar de lo más arbitrario para los usuarios, aportando un plus de inseguridad a la solicitud.

Al concretar que las normas en las que el jurado va a basar su decisión son de *soft law*, parece obvio que este sistema no va a resultar tan proteccionista como resultaría acudir a la vía judicial para un ciudadano de la Unión Europea, ya que no será posible alegar instrumentos garantistas como los Reglamentos o Directivas, cuya finalidad tuitiva es elevada. Esto es posible relacionarlo con la ejecutividad, ¿se asimilan las resoluciones dictadas a las emitidas en un proceso de mediación? Porque en ese caso no se excluye la vía judicial y en caso de disconformidad lo único que se habría hecho es ralentizar la solución final y mientras tanto dilatar el proceso.

Otro aspecto muy importante desde mi punto de vista es la publicidad absolutamente nula que se le ha dado a esta vía de resolución de conflictos, que no se menciona dentro de la propia red social. ¿Qué utilidad va a tener un mecanismo que no conocen los propios afectados o, que, de conocer, no saben utilizar? No existe una web específica o un apartado dentro de la misma en la que se publiquen las resoluciones

que dictan, ni el mecanismo que utilizan. Esta falta de transparencia hace que nos planteemos la objetividad, funcionalidad y calidad de un instrumento tan limitado en cuanto a su objeto y función tuitiva.

CONCLUSIONES

1. Las redes sociales son medio de comunicación principal de la infancia y la adolescencia a día de hoy, que no solo se utilizan como un medio para mantenerse al día o una herramienta de trabajo, sino que se perciben como una forma alternativa de ampliar el círculo social. Sin embargo, a pesar de las ventajas que aportan, no están exentas de importantes riesgos, entre los que destacan los de tipo psíquico, derivados de los comentarios que se pueden alojar en las plataformas con repercusión negativa en la mente de los niños; la asunción de una falsa creencia de que existen vidas ideales, fenómeno conocido como "*toxic positivity*"; el acceso por parte de nuestros adolescentes a contenidos que no son propios de su edad debido al perfilado de la propia plataforma.

2. Para que los niños, niñas y adolescentes tengan acceso a una red social es necesario que otorguen un doble consentimiento: el consentimiento para abrirse una cuenta y crearse un perfil, por un lado y, por otro, el consentimiento para el tratamiento de sus datos personales.

3. El consentimiento del niño, niña o adolescente para crearse una cuenta en una red social trae causa de la relación contractual que formaliza con la propia red y se basa en el artículo 1261 del Código Civil, como elemento contractual. Ese consentimiento no será necesario completarlo con el parental, dado que el artículo 1263 Cc permite que las personas menores de edad puedan celebrar contratos que las leyes les permitan realizar por sí mismas sobre servicios de la vida corriente propios de su edad, y la apertura de una cuenta en una red social se ha considerado como tal.

4. Con respecto al consentimiento para el tratamiento de los datos personales de los niños, niñas y adolescentes cuando se abren un perfil en una red social, el RGPD permite que lo otorguen de forma autónoma cuando tengan como mínimo 16 años, dejando a los Estados establecer su propio margen entre 13 y 16 años. España en su LOPD lo ha establecido en 14 años, por lo que los menores de 14 años necesitarán el consentimiento parental/maternal. Sin embargo, en junio de 2024 se ha aprobado el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, que prevé elevar la edad de 14 años para emitir un consentimiento válido en materia de protección de datos a 16 años.

5. Para controlar el acceso de los menores a las redes sociales, las plataformas no han realizado ningún esfuerzo razonable (como exige el art. 8.2 RGPD), a pesar de existir iniciativas doctrinales (autorización parental con un DNI, control del lenguaje en la red) lo que supone que existan menores que acceden a una red a la que no deberían tener acceso, con sus respectivas consecuencias negativas.

6. El término *influencer* hace referencia al sujeto que se dedica a subir un determinado contenido en sus redes sociales y que aprovechará su repercusión en la mayoría de las ocasiones para obtener una contraprestación económica a través de contenido publicitario. Esta práctica, realizada en un primer momento solamente por adultos, ha pasado a popularizarse entre jóvenes de edades entre 3 y 14 años, pasando a denominarse *kidinfluencers*, con el consentimiento de los padres, que firman contratos con marcas para obtener patrocinios. Fenómeno parecido es el *sharenting*, en el que el titular de la cuenta es el progenitor que se lucra con la vida de sus hijos, mostrándola abiertamente. Este tipo de situaciones han sido catalogadas desde el Derecho laboral como una explotación laboral, ya que los padres obtienen

una contraprestación económica por el rendimiento que generan sus hijos, que no tienen permitido trabajar según el artículo 6 del Estatuto de los Trabajadores, y en la mayoría de ocasiones no cuentan con el permiso del Ministerio Fiscal, como exige la ley.

7. Esa sobreexposición de la infancia y adolescencia en las redes sociales puede provocar lesiones en los llamados derechos de la personalidad, configurados por el derecho al honor, a la intimidad y a la imagen, ya que en la mayoría de las ocasiones estos menores no tienen capacidad para consentir, no ostentan la madurez suficiente y el consentimiento otorgado a una cierta edad sobre un contenido concreto puede cambiar en un futuro, con la desventaja de que el contenido alojado en Internet, ha dejado una huella digital que refleja la identidad del menor.

8. Los progenitores de los niños, niñas y adolescentes son los titulares de las acciones por posibles lesiones a sus derechos a la personalidad cuando los menores han fallecido, por lo que, de publicarse fotografías o vídeos en las redes sociales que atenten contra el derecho a la imagen, al honor o a la privacidad, podrían solicitar su retirada. Sin embargo, en la práctica son los propios padres y amigos los que suben contenido sobre los niños, niñas y adolescentes, sin intención de atentar contra la propia identidad de los menores, por lo que en realidad no se ejercitan.

9. Cuando los *influencers* operan en las redes sociales, es habitual que muestren entre su contenido la denominada publicidad encubierta, es decir, aquella publicidad con contenido comercial, que es difícil de descifrar para el usuario, provocando confusión al pensar que la reseña o comentario sobre un cierto producto es veraz, sincera y fiel. Esto provoca un impulso en los niños, niñas y adolescentes que los lleva a desear adquirir el producto que se está publicitando para acercarse en cierto sentido a su ídolo. Esta práctica se encuentra prohibida por los artículos 5 y

7 de la LCD y por el Código de conducta sobre el uso de *influencers* en la publicidad. Sin embargo, este último instrumento es de adhesión voluntaria y presenta los problemas típicos de las normas de *soft law* en cuanto a su ejecutividad.

10. Cuando los *influencers* publicitan un producto, creando unas expectativas en la infancia y adolescencia con su adquisición, se está producido un daño y el sujeto que deberá responder puede variar: como norma general responderá la marca detrás de la publicidad que realiza el *influencer*, pero si existe una vinculación laboral mediante un contrato de trabajo entre la marca y el *influencer*, éste último responderá, al igual que si el propio creador de contenido es el propietario de la marca. La generación del daño se basa en el carácter vinculante que tiene la publicidad en el perfeccionamiento de un contrato, especialmente cuando se encuentra sometido a la normativa de consumo (LGDCU), como es el caso. Una vía de responsabilidad por la que el menor en vez de dirigirse contra la marca podría dirigirse contra el *influencer* sería la responsabilidad extracontractual del artículo 1902, pero en la práctica presenta graves problemas probatorios, como la relación de causalidad, la conducta dolosa o por culpa y la intencionalidad del creador de contenido, sumado a la escasa cuantía de los productos que adquieren los menores y que excluyen la viabilidad económica de recurrir a la vía judicial. Cuando sean los *kidinfluencers* los que realizan este tipo de prácticas, habrá que estudiar detenidamente el caso para determinar la responsabilidad solidaria de los progenitores o incluso la responsabilidad individual del menor.

11. La protección de datos es otro talón de Aquiles de las redes sociales, ya que plantea vulnerabilidades tanto en la creación de la red social (con la solicitud de datos en la apertura de la cuenta), como durante el uso de la misma (por publicidad excesiva de

información personal por parte del niño, niña o adolescente, la aceptación de las cookies, la indexación de forma automática del perfil en un buscador, la recepción de *spam*) y el cierre de la cuenta (el derecho al olvido, la supresión de la cuenta).

12. La regulación de los datos se encuentra en el RGPD y se entiende por datos personales toda información sobre una persona física identificada o identificable (ar. 4). Sin embargo, no resulta de aplicación a la llamada "excepción doméstica", es decir, aquellas situaciones en las que se comparten datos con un fin personal, familiar, entre un ámbito o círculo cerrado. En el ámbito de las redes sociales los proveedores de las redes serán los llamados responsables del tratamiento de datos, que vienen a ser los sujetos llamados a responder por daños provocados por infracciones de la normativa de protección de datos. Cuando son las propias personas menores de edad quienes adquieren una cierta popularidad, permitiéndoles las propias redes sociales obtener datos sobre sus seguidores (procedencia, alcance, inclinaciones), se considerarán también responsables del tratamiento de datos y deberán responder por los daños causados, incluso siendo menores de edad.

13. Ante la situación de vulnerabilidad que presentan los niños, niñas y adolescentes en las redes sociales, el legislador los ha provisto del derecho de acceso, rectificación, olvido y oposición.

14. El RGPD recoge como sujetos responsables al responsable y al encargado, que pueden en su caso tener responsabilidad solidaria, por daños físicos y morales, siendo el régimen de responsabilidad *cuasiobjetiva*, por culpa levísima. Para cuantificar la cantidad de la indemnización el TJUE ha precisado que es necesario atender a la normativa nacional del Estado en cuestión, no siendo posible aplicar criterios análogos a la cuantificación de multas administrativas que contempla el propio Reglamento.

15. El caso *Meta Platforms*, resuelto por el TJUE ha supuesto un gran hito en la UE por establecer una clara barrera protectora en materia de protección de datos. De modo que se considera ilícito el tratamiento de datos por parte de una red social que consiste en la obtención de información e imágenes que posteriormente en otra red social revela información de categorías protegidas sobre ese mismo usuario o sobre cualquier persona física, siempre que el interesado no haya hecho públicos de manera manifiesta dichos datos (por tener un gran impacto en la red social o haberlos publicado en abierto en un perfil no privado).

16. Otro de los elementos principales del caso *Meta Platforms* y de las redes sociales en general es el poder que otorgan los datos para poder ser revendidos a empresas que estudian la publicidad comportamental, es decir, aquella publicidad que se ofrece al usuario como consecuencia de la información obtenida a través de cookies que acepta el internauta durante la navegación y que aporta información sobre sus gustos, principalmente. Esto les permite a las empresas dirigir publicidad personalizada a los sujetos, de modo que eleva las probabilidades de realizar una venta. El TJUE se ha pronunciado en la sentencia C-252/21 sobre la licitud de la alternativa de pago a la negativa a aceptar las *cookies*, siempre que dicha alternativa no conlleve un coste sustancial o desproporcionado.

17. El contrato que se celebra entre los usuarios de las redes sociales y las propias redes sociales es de prestación de servicios, siendo válido dentro del ámbito de aplicación del RBI bis los pactos de sumisión expresa, incluso cuando el usuario se considere un consumidor pasivo, siempre que además del tribunal elegido por la red social se permita la elección del tribunal del domicilio del consumidor usuario de la red (lo que suele suceder en la práctica, al preverse así en las condiciones de uso de las redes sociales, por lo que no hay ningún peligro). Con respecto a la ley aplicable, los acuerdos de ley aplicable en el ámbito del Reglamento Roma

l correrán la misma suerte, siendo válidos siempre que la elección de la ley aplicable no prive al consumidor de la protección que le otorgarían las disposiciones imperativas de la ley de la residencia habitual del consumidor. Esto exige que se le informe al consumidor de que la elección de la ley aplicable no implica que se dejarán de aplicar tales disposiciones imperativas.

18. A modo de conclusión final es necesario realizar una reflexión general. El papel de los progenitores en el control de los niños, niñas y adolescente tiene una mayor repercusión que una legislación restrictiva y punitiva. El hecho de que se conciban medidas para controlar el consentimiento y la edad no repercute tan positivamente como una actitud parental que busque mantener al margen de las redes sociales a los menores en los primeros años de su infancia y adolescencia. El mejor modo de abordar esta cuestión comienza con la educación, la sensibilización y la concienciación. Reeducar a los menores en su crecimiento personal para que no requieran de la aprobación de la sociedad para sentirse bien, con la suficiente inteligencia emocional para no necesitar mostrar todo lo que les acontece en busca de validación externa reportaría grandes beneficios para nuestros niños, que no necesitarían vivir para las redes sociales, sino que se valdrían de ellas. La solución no consiste en retirar la tecnología de los niños, niñas y adolescentes, convirtiéndolos en "exiliados digitales", sino en centrarnos en la educación digital y presentarla como una herramienta.

19. Sin embargo, como se ha ido desarrollando durante esta investigación, muchos siguen siendo los ámbitos donde hay lagunas y pueden darse posibles vulneraciones y ataques contra derechos de los menores de edad, por lo que aún queda por trabajar.

PROPUESTAS

Para intentar combatir las principales problemáticas identificadas, propongo las siguientes medidas a tener en cuenta:

1. La creación de un sistema de autenticación de la edad de acceso a las redes sociales, controlado por la propia Agencia Española de Protección de Datos. Este sistema podría usar un método parecido al establecido en el sistema de verificación Clave, de modo que se controle mediante un certificado digital emitido por el propio Gobierno. Se podría implementar esta medida en todas las redes sociales con sede en España o que operen en España, para mantener protegidos a todos los usuarios españoles. De este modo, sería el propio Estado el que acreditaría que verdaderamente se tiene la edad que se declara y serían los padres los que deben solicitar la expedición de este certificado emitido por la Administración correspondiente, pasando por una serie de controles y trámites previos, conectando a las propias redes sociales con el Gobierno en cierta medida para conseguir una mayor seguridad entre los niños y jóvenes.
2. El otorgamiento de una insignia de calidad a las redes sociales que cumplan con los estándares de protección de datos en sede europea, para acreditar que existe verdaderamente un cumplimiento en el tratamiento de los datos y que no están realizando injerencias en los derechos de los menores. De este modo se motivaría a las diferentes compañías de redes sociales a cumplir con los requisitos que se establezcan para conseguir la insignia y así mantener un cierto renombre dentro del sector, asegurando a su vez unos estándares de protección.
3. La implementación por parte de las empresas de redes sociales de un sistema de Inteligencia Artificial para detectar expresiones emitidas por los *influencers* que puedan vincularse con reseñas. Así, si dichas reseñas no están etiquetadas correctamente como

publicidad, se podría cerrar la cuenta del creador de contenido a modo de castigo punitivo por haber incurrido en una violación de la Ley de Competencia Desleal, siendo una nueva sanción el cierre de su cuenta.

BIBLIOGRAFÍA

AGUDELO MOLINA, J.D. 2021. "Causalidad e imputación. La coherencia interna de la teoría de la imputación objetiva en la responsabilidad civil", *Revista de Derecho Privado*, núm. 42, pp. 321-353. https://doi.org/10.18601/01234366.n41.11

AGÜERO ORTIZ, A. 2021. "Derecho a la propia imagen y divulgación en prensa de fotos obtenidas en Facebook", *Derecho Privado y Constitución*, núm. 38, pp. 119-155. https://doi.org/10.18042/cepc/dpc.38.04

AGUILAR GRIEDER, A. H. 2014. "Alcance de los controvertidos artículos 3 y 4 del Reglamento (CE) núm. 593/2008: Perspectiva de lege lata y propuestas de lege ferenda", *Cuadernos de Derecho Transnacional*, vol. 6, núm. 1, 2014, pp. 45-67.

AMMERMAN YEBRA, J. 2021. "De nuevo sobre el 'sharenting' y los derechos de la personalidad de los menores de edad", en OTERO CRESPO, M., *Retos jurídicos de actualidad*, Dykinson, Madrid, 2021, pp. 80-84. https://doi.org/10.2307/j.ctv282jgcd.16

AYLLÓN GARCÍA, J.D. 2022. "Consentimiento de los menores de edad en las redes sociales: especial referencia a TikTok", *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, pp. 580-609.

BARBUDO FERNÁNDEZ, C. 2023. "La autoridad británica de protección de datos sanciona a TikTok con 12,7 millones de libras por tratar indebidamente datos de menores", *Diario La Ley*, núm. 71, de 2023, pp. 1-2.

BATUECAS CALETRIO, A. 2015. "Intimidad personal, protección de datos personales y geolocalización", *Derecho Privado y Constitución*, núm. 29, pp. 47-82. https://doi.org/10.18042/cepc/dpc.29.02

BENDITO CAÑIZARES, M.T. 2020. "La autenticidad de la publicidad y anunciante en la publicidad nativa y en particular, en la publicidad de los *influencers*", *Revista Aranzadi Doctrinal*, núm. 8, pp. 217-250.

CALVO CARAVACA, A.L., y CARRASCOSA GONZÁLEZ, J. 2018. *Derecho Internacional Privado*, vol. II, Comares, Granada.

CANEDO ARRILLAGA, M.P. 2010. "Notas breves sobre la sentencia del TJUE (Sala Cuarta) de 25 febrero 2010 (Car Trim: asunto C-381/08): los contratos de compraventa y los contratos de prestación de servicios en el Reglamento 44/2001", *Cuadernos de Derecho Transnacional*, vol. 3, núm. 1, 2011, pp. 263-269.

CASTILLO PARRILLA, J.A. 2023."Riesgos y daños derivados del sharenting", en IVONE V., GÁLVEZ CRIADO, A., y LÓPEZ SUÁREZ, M.A., *Nuevos escenarios del Derecho de familia en España e Italia. Novedades legales y jurisprudenciales*, Atelier, Barcelona, pp. 107-133.

CEDEÑO HERNÁN, M. 2021. "La tutela transfronteriza de los derechos de la personalidad en la Unión Europea", *Cuadernos de Derecho Transnacional* (Marzo 2021), vol. 13, núm. 1, pp. 110-133. https://doi.org/10.20318/cdt.2021.5954

CONDE FALCÓN, A. y DELGADO PONCE, A. 2021. "Estudio de la competencia mediática frente al impacto d ellos youtubers en los menores de edad españoles" *Pixel-Bit: Revista de medios y educación*, núm. 61, pp. 257-270. https://doi.org/10.12795/pixelbit.74234

DE MIGUEL ASENSIO, P.A. 2009. "Sobre el concepto de contrato de prestación de servicios en el DIPr. comunitario". Disponible en el siguiente enlace: https:// pedrodemiguelasensio.blogspot.com/2009/05/sobre-el-concepto-de-contrato-de.html.

DE MIGUEL ASENSIO, P. A. 2013. "El lugar de ejecución de los contratos de prestación de servicios como criterio atributivo de competencia", en FORNER DELAYGUA, J., GONZÁLEZ BEILFUSS, C., y VIÑAS FARRÉ, R. (coords.), *Entre Bruselas y La Haya. Estudios sobre la unificación internacional y regional del Derecho internacional privado. Liber amicorum Alegría Borrás*, Dykinson, Madrid, pp. 291-309.

DE MIGUEL ASENSIO, P. 2017. "Competencia y Derecho aplicable en el Reglamento General sobre Protección de datos de la Unión Europea", *REDI*, *69*, pp. 75-108. https://doi.org/10.17103/redi.69.1.2017.1.03

DE MIGUEL ASENSIO, P.A. 2018. "Demandas frente a redes sociales por daños en materia de datos personales: precisiones sobre competencia judicial", *La Ley Unión Europea*, núm. 56, pp. 1-8.

DE MIGUEL ASENSIO, P.A. 2023. "Requisitos del derecho a indemnización en el Reglamento General de Protección de Datos", *La Ley Unión Europea*, núm. 115, pp. 1-8.

DE MIGUEL ASENSIO, P.A. 2023. "Redes sociales y datos personales: bases jurídicas para el tratamiento e implicación de las autoridades de defensa de la competencia", *La Ley Unión Europea*, núm. 117, pp. 1-12.

DE MIGUEL ASENSIO, P.A. 2023. "Derecho al olvido: precisiones en la jurisprudencia del Tribunal de Justicia sobre su ejercicio y alcance", *La Ley Unión Europea*, núm. 110, pp. 1-6.

DE MIGUEL ASENSIO, P.A. 2024. "Determinación de la indemnización por daños derivados de infracciones del Reglamento General de Protección de Datos. Sentencia del Tribunal de Justicia 3ª 11 abril 2024, asunto, C-741/21: *juris*", *La Ley Unión Europea*, núm. 125, 2024, pp. 1-5.

FERNÁNDEZ BLANCO, E. y RAMOS GUTIÉRREZ, M. 2022. "Kid influencers. Creación de contenidos de marca de la generación Alpha y sus implicaciones jurídicas", en CALDEVILLA DOMÍNGUEZ, D., *Libro de Actas del Congreso Internacional sobre Comunicación, Innovación, Investigación y Docencia*, Fórum Internacional de Comunicación y Relaciones Públicas, núm. XXI, Sevilla, 2022.

FLORIT FERNÁNDEZ, C. 2021. "Kidfluencers: menores de edad emancipados autónomos en internet", *Actualidad Civil*, núm. 2, febrero de 2021, pp. 1-15.

FLORIT FERNÁNDEZ, C. 2022. *Los Menores e Internet. Riesgos y Derechos: Especial Consideración de La Nueva Ley Orgánica 8/2021, de 4 de Junio de Protección Integral de La Infancia y La Adolescencia Frente a La Violencia*, Bosch. https://doi.org/10.2307/j.ctv2zp4s0q

GAL, M. y RUBINFELD, D. L. 2016. "The Hidden Costs of Free Goods: Implications for Antitrust Enforcement", *Antitrust Law Journal*, *80*(401), 1-59.

GARCÍA GARCÍA, A. 2021. "La protección del menor en el derecho europeo y español. El *sharenting* y su problemática", *Universitat Politécnica de Valencia*, núm. 10, Valencia.

GARCÍA GARNICA, M.C. 2021. "Responsabilidad civil y redes sociales. Especial consideración a los daños sufridos o causados por menores de edad", en LÓPEZ Y GARCÍA DE LA SERRANA, J., (dir.), *XXI Congreso Nacional sobre responsabilidad civil y seguro*, Sepín, Sevilla, 2021, pp. 87-156.

GARCÍA PÉREZ, F.J. 2020. "El nuevo Código de conducta sobre el uso de *influencers* en la publicidad: una buena (y esperada) noticia en el ámbito de la publicidad digital", *Actualidad Jurídica Aranzadi*, núm. 967, pp. 1-10.

GIL ANTÓN, A.M. 2015. *¿Privacidad del menor en Internet? Me gusta ¡¡¡todas las imágenes de mis amigos a mi alcance con un simple click!!!*, Aranzadi, Navarra.

GUTIÉRREZ SANTIAGO, P. 2016. "La llamada "personalidad pretérita": datos personales de las personas fallecidas y protección post mortem de los derechos al honor, intimidad y propia imagen", *Actualidad Jurídica Iberoamericana,* núm. 5, pp. 201-238.

HERRERA DE LAS HERAS R. y PAÑOS PÉREZ A. 2022. *La privacidad de los menores en redes sociales. Especial consideración al fenómeno influencer*, Atelier, Barcelona, 2022.

LLAMAS BAO, C. 2021. "Hijos menores de edad en redes sociales: su protección al amparo de los artículos 18 y 39 de la Constitución española", *Revista Jurídica de la Universidad de León*, núm. 8, pp. 203-219. https://doi.org/10.18002/rjule.v0i8.7080

LÓPEZ VILLAFRANCA, P. y OLMEDO SALAR, S. 2019. "Menores en YouTube, ¿ocio o negocio? Análisis de casos en España y EUA", *El profesional de la información*, vol. 28, núm. 5, pp. 1-12. https://doi.org/10.3145/epi.2019.sep.20

MARCO MOLINA, J. 2015. "El proceso de formación o conclusión del contrato", *Indret: Revista para el Análisis del Derecho*, núm. 3, pp. 1-64.

MORALEJO IMBERNÓN, N. 2023. *Los derechos de los menores y las redes sociales. Incluye Reglamento (UE) 2022/2065, del Parlamento Europeo y del Consejo, de 19 de octubre, de Servicios Digitales,* Tirant lo Blanch, Valencia.

NAVARRO ORTEGA, A. y DURÁN RUIZ, F.J. 2018. "La protección jurídico-administrativa del menor y frente al menor en redes sociales y servicios de mensajería instantánea", en DURÁN RUIZ, F.J. (dir.), *Desafíos de la Protección de menores en la sociedad digital. Internet, redes sociales y comunicación*, Tirant lo Blanch, Valencia, pp. 341-383.

ORTEGA GIMÉNEZ, A. 2023. "Las nuevas tecnologías y la protección de datos de carácter personal desde el Derecho Internacional Privado: redes sociales de internet y cloud computing", *Actualidad Civil*, núm. 12, pp. 1-24.

ORTEGA GIMÉNEZ, A. 2024. "¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EEUU", *Cuadernos de Derecho Transnacional*, *16*(1), pp. 483-513. https://doi.org/10.20318/cdt.2024.8432

ORTIZ LÓPEZ, P. 2019. "Cookies, fingerprinting y la privacidad digital", en LÓPEZ CALVO, J. (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer, Madrid, pp. 961-972.

PÉREZ BES, F. 2012. *La publicidad comportamental online*, UOC, Barcelona.

PLATERO ALCÓN, A. 2023. *Repercusiones jurídico-civiles de la actividad de los 'influencers' digitales. Especial consideración de la publicidad encubierta*, Dykinson, Madrid.

RAMOS SERRANO, M. y HERRERO DIZ, P. 2022. "Menores y YouTube: el fenómeno de los pequeños influencers", en MÁRTINEZ GARCÍA, A., *Imágenes de la infancia en la Comunicación y la Cultura*, Fragua, Madrid, pp. 287-300.

RODRÍGUEZ BENOT, A. 2024. *Manual de Derecho internacional privado*, Tecnos, Madrid,. https://doi.org/10.69592/5-6673-N1-SEGUNDO-SEMESTRE-2024-ART-3

RODRÍGUEZ TERCEÑO, J., BARTOLOMÉ ROMERO, C. y FANJUL FERNÁNDEZ, M. L. 2021. "Influencers, instagramers y publicidad encubierta", en CASTILLO ABDUL, B., *Prosumidores, emergentes, redes sociales, alfabetización y creación de contenidos*, Dykinson, Madrid, pp. 813-843.

SÁNCHEZ CANO, M.J. y ROMERO MATUTE, Y. 2021. "El régimen jurídico de las redes sociales y los retos que plantea el acceso a dichas plataformas", *Cuadernos de Derecho Transnacional*, *13*, pp. 1139-1148. https://doi.org/10.20318/cdt.2021.6023

SÁNCHEZ FRÍAS, A. 2020. "El Tribunal Supremo de Facebook: ¿un nuevo paso hacia la justicia sin Estado", *Cuadernos de Derecho Transnacional*, *12*(2), pp. 1386-1405. https://doi.org/10.20318/cdt.2020.5676

SUÁREZ FERNÁNDEZ, L. 2022. "La responsabilidad parental en los entornos digitales. Necesario equilibrio, entre acceso, control y seguridad", *Actualidad Jurídica Iberoamericana*, núm. 7, vol. 3, pp. 1076- 1097.

TAMAYO VELASCO, J. 2021. "Big data, competencia y protección de datos: el rol del Reglamento General de Protección de Datos en los modelos de negocio basados en la publicidad personalizada", *Revista de Estudios Europeos*, núm. 78, pp. 183-202.

TORAL LARA, E. 2020. "Menores y redes sociales: consentimiento, protección y autonomía", *Derecho Privado y Constitución*, núm. 36, pp. 179-218. https://doi.org/10.18042/cepc/dpc.36.05

TRONCOSO REIGADA, A. 2012. "Redes sociales y protección de datos personales", en LÁZARO GONZÁLEZ, I.E., *Menores y nuevas tecnologías: posibilidades y riesgos de la TDT y las redes sociales*, Tecnos, Madrid, pp. 83-113.

TRUJILLO CABRERA, C. 2024. "Los nuevos cookie walls: Consent or pay. A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio de 2023", *Revista de Derecho Civil*, vol. XI, núm. 2, pp. 75-112.

VÁZQUEZ PASTOR, L. 2022. "Los derechos de la personalidad del menor de edad en la era digital. La dicotomía entre autonomía y protección", *Actualidad Jurídica Iberoamericana*, núm. 17, pp. 1112-1153.

VIDAL BEROS, C. 2023. "Ley General de comunicación audiovisual española. Influencers y sustentabilidad", *Cuadernos del Centro de Estudios en Diseño y Comunicación*, núm. 181, pp. 181-199. https://doi.org/10.18682/cdc.vi181.9244

ZUBERO QUINTANILLA, S., *Las declaraciones publicitarias en la contratación,* Tirant lo Blanch, Valencia, 2017.

JURISPRUDENCIA

Tribunal de Justicia de la Unión Europea

STJUE de 11 de abril de 2024, asunto C-741/21, *Juris*, ECLI: EU:C: 2024:288

STJUE de 25 de enero de 2024, asunto C-687/21, *MediaMarktSaturn,* ECLI: EU:C:2024:72

STJUE de 4 de julio de 2023, C-252/21, asunto *Meta Platforms e.a.,* ECLI: EU:C:2023:537

STJUE de 4 de mayo de 2023, asunto C-300/2021, *Österreichische Post AG*, ECLI: EU:C:2023:370

STJUE de 21 de diciembre de 2023, C-667/21, *Krankenversicherung Nordhein*, ECLI: EU:C:2023:1022

STJUE de 8 de diciembre de 2022, asunto C-460/20, *Google*, ECLI: EU:C:2022:962

STJUE de 22 de abril de 2021, asunto C-252/21, *Facebook v. Bundeskartellamt*, ECLI:EU:C:2023:537

STJUE de 29 de julio de 2019, asunto C-40/17, *Fashion ID GmbH y C,* ECLI:EU:C:2019:629

STJUE de 7 marzo de 2018, asuntos acumulados C-274/16, C-447/16 y C-448/16, *Air Nostrum*, ECLI:EU:C:2018:160

STJUE de 1 de febrero de 2018, asunto C-25/17, caso Testigos de Jehová. ECLI: EU:C:2018:551

STJUE de 25 de enero de 2018, asunto C-498/16, *Schrems*, ECLI:EU:C: 2018:37

STJUE de 15 de junio de 2017, asunto C-249/16, *Khareda*, ECLI:EU:C: 2017:472

STJUE de 23 de diciembre de 2015, asunto C-297/14, ECLI:EU:C:2015:844

STJUE de 19 de octubre de 2015, asunto C-582/14, *Breyer*, ECLI:EU:C:2016:779

STJUE 10 septiembre de 2015, asunto C-47/14, *Ferho*, ECLI:EU:C:2015:574

STJUE de 13 de mayo de 2014, asunto C-131/12, Caso *Google Spain*, ECLI:EU:C:2014:317

STJUE de 19 de diciembre de 2013, asunto C-9/12, *Corman-Collins SA vs. La Maison du Whisky SA,* ECLI:EU:C: 2013:860

STJUE de 14 de marzo de 2013, asunto C-419/11, ECLI:EU:C: 2013:165

STJUE de 7 de diciembre de 2010, asuntos acumulados C-585/08 y C-144/09, *Pammer*, ECLI:EU:C:2010:740

STJUE de 11 de marzo de 2010, asunto 19/09, *Wood Flour*, ECLI:EU:C:2010:137

STJUE de 25 de febrero de 2010, asunto C-381/08, *Car Trim*, ECLI:EU:C:2010:90

STCE de 9 de julio de 2009, asunto C-204/2008, *Air Baltic*, ECLI:EU:C:2009:439

STJUE de 23 de abril de 2009, asunto C-533/07*, Falco Privats-tiftung y Rabitsch.* ECLI:EU:C:2009:257

STJUE de 16 de diciembre de 2008, asunto C-73/07, ECLI:EU:C:2008:727.

STJUE de 6 de noviembre de 2003, asunto C-101/01, *Lindquist*. ECLI:EU:C:2002:513

STJCE de 11 de julio de 2002, asunto C-96/00, *Gabriel*, ECLI:EU:C:2002:436

Jurisprudencia nacional

Tribunal Constitucional

STC 8/2022, de 27 de enero de 2022, ECLI:ES:TC:2022:8

STC 27/2020, de 24 de febrero de 2020, ECLI:ES:TC:2020:27

STC 196/2006, de 3 de julio de 2006, ECLI:ES:TC:2006:196

STC 83/2002, de 22 de abril de 2002, ECLI:ES:TC:2003:14

STC 156/2001, de 2 de julio. *BOE* núm. 178 Suplemento, de 26 de julio de 2001.

STC 231/1988, de 2 de diciembre de 1988, ECLI:ES:TC:1988:231

Tribunal Supremo

STS 512/2017, de 22 de septiembre de 2017, ECLI:ES:TS:2017:3322

STS 850/2014 de 26 noviembre de 2014, ECLI:ES:TS:2014:5174

Audiencia Nacional

SAN de 15 de junio de 2006. ECLI:ES:AN:2006:3077

LEGISLACIÓN

Legislación nacional

Normativa de fuente europea

Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital. *DOUE* L 1183, de 30 de abril de 2024. Disponible en el siguiente enlace: https://www.boe.es/doue/2024/1183/L00001-00056.pdf

Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *DOUE* L 119, de 4 de mayo de 2016. Disponible en el siguiente enlace: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Reglamento (UE) núm. 1215/2012 del Parlamento europeo y del Consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. *DOUE* L351. Disponible en el siguiente enlace: https://www.boe.es/doue/2012/351/L00001-00032.pdf

Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I). DOUE núm. 177, de 4 de julio de 2008. Disponible en el siguiente enlace: https://www.boe.es/buscar/doc.php?id=DOUE-L-2008-81325

Reglamento (CE) núm. 864/2007 del Parlamento europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales. *DOUE* L 199/40. Disponible en el siguiente enlace: https://www.boe.es/doue/2007/199/L00040-00049.pdf

Normativa de fuente nacional

Constitución Española. *BOE* núm. 311, de 29 de diciembre de 1978. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia. *BOE* núm. 134, de 5 de junio de 2021. Disponible en el siguiente enlace: https://www.boe.es/eli/es/lo/2021/06/04/8/con

Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica. *BOE* núm. 132, de 3 de junio de 2021. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2021-9233

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *BOE* núm. 294, de 6 de diciembre de 2018. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Ley Orgánica 7/2015, de 21 de julio por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *BOE* núm. 174, de 22 de julio de 2015. Disponible en el siguiente enlace: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-8167

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *BOE* núm. 166, de 12 de julio de 2002. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley 3/1991, de 10 de enero, de Competencia Desleal. *BOE* núm. 10, de 11 de enero de 1991. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-1991-628

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. *BOE* núm. 115, de 14 de mayo de 1982. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. *BOE* núm. 255, de 24 de octubre de 2015. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. *BOE* núm. 287, de 30 de noviembre de 2007. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *BOE* núm. 17, de 19 enero de 2008. Disponible en el siguiente enlace: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. Disponible en el siguiente enlace: https://www.mpr.gob.es/servicios/participacion/audienciapublica/Documents/VSGT%202024/2024-0921%20APLO%20menores%20entornos%20digitales/MAIN.pdf

Normativa internacional

Carta Europea de Derechos del Niño, adoptada en Resolución del Parlamento Europeo de 8 de julio de 1992. *DOCE* nº C 241, de 21 de septiembre de 1992. Disponible en el siguiente enlace: https://bienestaryproteccioninfantil.es/carta-europea-de-los-derechos-del-nino-doce-no-c-241-de-21-de-septiembre-de-1992/

Convención de Derechos del Niño de 20 de noviembre de 1989. Disponible en el siguiente enlace: https://www.unicef.es/sites/unicef.es/files/comunicacion/ConvencionsobrelosDerechosdelNino_0.pdf.

Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966, adoptado en Nueva York y ratificado por España en 1977. Disponible en el siguiente enlace: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Convenio Europeo de Derechos Humanos, firmado el 4 de noviembre de 1950, en vigor desde el 3 de septiembre de 1953. Disponible en el siguiente enlace: https://www.echr.coe.int/documents/d/echr/Convention_SPA

Declaración Universal de Derechos Humanos de 1948, elaborada por las Naciones Unidas. Disponible en el siguiente enlace: https://www.un.org/es/about-us/universal-declaration-of-human-rights

OTROS RECURSOS

Children's Online Privacy Protection Act. Disponible en el siguiente enlace: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Código de conducta sobre el uso de *influencers* en la publicidad. Disponible en el siguiente enlace: https://www.autocontrol.es/wp-content/uploads/2020/10/codigo-de-conducta-publicidad-influencers.pdf

COMITÉ DE DERECHOS DEL NIÑO, *Observación General núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital*, CRC/C/GC/25, de 2 de marzo de 2021, disponible en el siguiente enlace: https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Dictamen 2/2010, sobre publicidad comportamental en línea, de 22 de junio de 2010 del Grupo de Trabajo de Protección de Datos del Artículo 29. Disponible en el siguiente enlace: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_es.pdf

Dictamen 5/2009 sobre redes sociales en línea del Grupo de Trabajo sobre Protección de Datos del artículo 29. Disponible en el siguiente enlace: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD (primera parte), de 7 de julio de 2020. Disponible en el siguiente enlace: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_es.pdf

Directrices 2/2019 sobre el tratamiento de datos personales en virtud del art. 6.1.b) del RGPD. Disponible en el siguiente enlace: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_es.pdf

Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, elaborado en 2009 por INTECO y la AEPD. Disponible en el siguiente enlace: https://www.uv.es/limprot/boletin9/inteco.pdf

Informe preceptivo de 4 de agosto de 2017 del Consejo de Estado sobre el Anteproyecto de Ley Orgánica de Protección de Datos de carácter personal. Disponible en el siguiente enlace: https://www.mjusticia.gob.es/va/AreaTematica/ActividadLegislativa/Documents/1292428594738-PLOPD_MAIN_anexo_4_Informes_preceptivos.pdf

SAVE THE CHILDREN, *Derechos#sinconexión. Un análisis sobre derechos de la infancia y la adolescencia y su protección en el mundo digital*, Save the Children España, 2024. Disponible en el siguiente enlace: https://www.savethechildren.es/sites/default/files/2024-07/Informe_Derechos_SinConexion.pdf

ISBN: 978-84-1396-346-4

Vulnerabilidades de la infancia y adolescencia en las redes sociales y sus repercusiones jurídico-civiles

Paola Zouak Lara

Son múltiples los estudios que se han realizado sobre los menores y las redes sociales. Sin embargo, en esta investigación se plantea un abordaje integral, analizando desde cuestiones clásicas como trasgresiones al derecho al honor, a la intimidad personal y familiar y a la propia imagen de la infancia y la adolescencia, hasta la sobreexposición de la infancia por sus progenitores en las redes sociales (*sharenting*), pasando por la creación de la figura del *kidfluencer* y otras cuestiones de actualidad, como las últimas novedades en materia de publicidad encubierta y creación de perfiles digitales o protección de datos personales desde una doble perspectiva: el niño como sujeto de protección y la persona menor de edad como posible vulneradora del derecho de protección del que son titulares otros adolescentes

CÁTEDRA DE INFANCIA Y ADOLESCENCIA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

edUPV
Universitat Politècnica de València

Red de Universidades por la Infancia y la Adolescencia