FACULTAD DE DERECHO

DESAFÍOS ACTUALES DE LA REGULACIÓN DE PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Autor: Iñigo de Garay Velasco

5º E-3 A

Área de Derecho Civil

Tutora: Reyes Corripio

Madrid Abril, 2024

Resumen

En un mundo cada vez más conectado y digitalizado, las redes sociales han aparecido como plataformas que dominan la comunicación global, conectando a miles de millones de usuarios y facilitando el intercambio de información a una escala sin precedentes. Esta expansión trae consigo una serie de retos significativos en términos de privacidad y protección de datos personales, donde las legislaciones como la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y el Reglamento General de Protección de Datos (RGPD) de la UE buscan proporcionar un marco para salvaguardar los derechos de los individuos.

Sin embargo, a pesar de estos esfuerzos regulatorios, las prácticas de las redes sociales continúan presentando desafíos que ponen a prueba la efectividad de estas regulaciones. El manejo de datos personales, la vigilancia de la conformidad con las normativas vigentes y el equilibrio entre la protección de la privacidad y otros intereses sociales, como la libertad de expresión y la innovación tecnológica, son cuestiones complejas que requieren soluciones continuas y adaptativas. Este Trabajo de Fin de Grado busca explorar estos desafíos en profundidad, proporcionando un análisis crítico de la situación actual y proponiendo mejoras y soluciones para reforzar la protección de datos en el ámbito de las redes sociales, enfatizando la necesidad de una evolución legislativa que acompañe el ritmo acelerado de la tecnología digital.

Palabras Clave: Privacidad, redes sociales, protección de datos, RGPD, LOPDGDD, consentimiento, derecho al olvido.

Abstract

In an increasingly connected and digitalized world, social networks have emerged as platforms that dominate global communication, connecting millions of users and facilitating the exchange of information on an unprecedented scale. This expansion brings with it significant challenges in terms of privacy and personal data protection, where legislation such as the LOPDGDD and the EU RGPD aim to provide a framework to safeguard individual rights.

However, despite these regulatory efforts, the practices of social networks continue to pose challenges that test the effectiveness of these regulations. The management of personal data, monitoring compliance with current regulations, and balancing privacy protection with other social interests, such as freedom of expression and technological innovation, are complex issues that require ongoing and adaptive solutions. This Final Degree Project seeks to explore these challenges in depth, providing a critical analysis of the current situation and proposing improvements and solutions to strengthen data protection in the realm of social networks, emphasizing the need for legislative evolution that keeps pace with the rapid advancement of digital technology.

Key words: Privacy, social networks, data protection, RGPD, LOPDGDD, consent, right to oblivion.

ÍNDICE

LISTA DE ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

BOE: Boletín Oficial del Estado

CCAA: Comunidad Autónoma

CE: Constitución Española

CEPD: Comité Europeo de Protección de Datos

DNI: Documento Nacional de Identidad

G29: Grupo de trabajo del Artículo 29

LOPDGDD: Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales

OCDE: Organización para la Cooperación y Desarrollo Económico

RAE: Real Academia Española

RGPD: Reglamento General de Protección de Datos

SRS: Servicios de Redes Sociales

TFG: Trabajo de Fin de Grado

TFUE: Tratado de Funcionamiento de la Unión Europea

TJUE: Tribunal de Justicia de la Unión Europea

UE: Unión Europea

I. INTRODUCCIÓN

1. CONTEXTO Y RELEVANCIA DEL TEMA

La Real Academia Española (RAE, en adelante) define una red social como una "*plataforma digital de comunicación global que une a numerosos usuarios*"[1]. Actualmente, en un mundo globalizado, más de 5.350 millones de personas, aproximadamente el 66,2% de la población mundial, utilizan redes sociales[2]. Six Degrees, creada en 1997, se reconoce como la primera red social de este tipo. No obstante, el auge de las redes sociales comenzó con el desarrollo del concepto de blogging a principios de los años 2000, impulsando el lanzamiento de plataformas como LinkedIn o MySpace. Desde ese momento, el crecimiento de las redes sociales ha continuado ininterrumpidamente, con Facebook destacándose como una de las más dominantes a nivel mundial[3].

Con la revolución tecnológica que el mundo está experimentando, el derecho a la intimidad y la protección de datos se ha convertido en una preocupación. Con el aumento de las redes sociales y su presencia en el día a día, la cantidad de información personal disponible en Internet ha crecido de forma exponencial lo que ha provocado grandes desafíos en relación con la privacidad y la seguridad de datos de los usuarios. La intersección entre la privacidad, la protección de datos y las tecnologías emergentes es un campo de estudio crítico, ya que afecta a individuos, organizaciones y la sociedad en su conjunto[4].

El creciente uso de redes sociales ha transformado la forma en que las personas interactúan, comunican y comparten información. Mientras que estas plataformas ofrecen oportunidades sin precedentes para la expresión personal y la conexión social, también plantean riesgos significativos para la privacidad y la protección de datos de los usuarios.

---

[1] Real Academia Española: *Diccionario de la lengua española*, 23.ª ed. (consultado en https://dle.rae.es/red?m=form#GExglxC; última consulta 28/03/2024).
[2] Fraguela, N., "El número de usuarios de internet en el mundo crece un 1,8% y alcanza los 5.350 millones (2024)", *Marketing for eCommerce*, 31 de enero de 2024 (disponible en https://marketing4ecommerce.net/usuarios-de-internet-mundo/; última consulta 28/03/2024).
[3] Boyd, D. M., & Ellison, N. B., "Social network sites: Definition, history, and scholarship", *Journal of Computer-Mediated Communication*, vol. 13, n.1, p.210.
[4] Warren, S.D. & Brandeis, L.D., "The Right to Privacy", *Harvard Law Review*, vol. 4, n. 5, 1890, p. 197.

La naturaleza omnipresente de la recopilación de datos y el análisis de big data por parte de empresas tecnológicas ha exacerbado estos riesgos, haciendo que la regulación efectiva sea más crucial que nunca[5].

En España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD, en adelante) y el Reglamento 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 (RGPD, en adelante) representan esfuerzos significativos para abordar estos desafíos, estableciendo un marco legal para la protección de datos personales. Sin embargo, la rápida evolución de las tecnologías digitales y las prácticas de las redes sociales presentan desafíos continuos para la eficacia de estas regulaciones.

La relevancia de este tema radica no solo en la necesidad de proteger los derechos individuales a la privacidad y la seguridad de los datos personales, sino también en el equilibrio entre estos derechos y otros intereses sociales, como la libertad de expresión y la innovación tecnológica. La búsqueda de soluciones adecuadas a los desafíos de la regulación de protección de datos en las redes sociales es crucial para fomentar un entorno digital que respete los derechos fundamentales y promueva un uso responsable de la tecnología.

2. OBJETIVOS

El objetivo general de este Trabajo de Fin de Grado consiste en realizar un análisis profundo sobre los desafíos a los que se enfrenta la legislación de protección de datos en relación con las redes sociales actualmente, tratando de encontrar soluciones y propuestas que permitan una mejor adecuación a los avances tecnológicos. Este trabajo tiene como objeto mostrar detalladamente el marco legal en España, incluyendo la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, para poder

[5] Debatin, B., Lovejoy, J.P., Horn, A.K., & Hughes, B.N., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", *Journal of Computer-Mediated Communication*, vol. 15, n. 1, 2009, p. 86.

así identificar el modo en el que se aplican dichas regulaciones y cuáles son sus principales limitaciones.

Se realizará un análisis sobre cómo han ido evolucionando las redes sociales y cómo han ido afectando cada vez más a la privacidad y a la protección de datos de los usuarios, identificando así los riesgos que conlleva que haya información personal en este tipo de plataformas. A través de este análisis podremos esclarecer los desafíos que surgen del marco normativo actual, y destacar los conflictos que surgen de las redes sociales y los requisitos de protección de datos.

A continuación, y tras este análisis crítico, se intentará realizar propuestas o incorporar ideas de otras legislaciones internacionales que pudieran reforzar nuestra legislación y la protección de datos personales. Al abordar estos objetivos, el trabajo se posiciona como una contribución valiosa al campo del derecho de la protección de datos, apuntando hacia la evolución necesaria de las normativas para responder adecuadamente a las dinámicas digitales contemporáneas.

3. METODOLOGÍA

Este TFG adopta un enfoque metodológico cualitativo y descriptivo, centrado en el análisis jurídico y normativo de la protección de datos en el contexto de las redes sociales. La metodología elegida permite abordar en profundidad las complejidades legales y los desafíos prácticos asociados con la regulación de la privacidad y los datos personales en un entorno digital en constante evolución.

Para el desarrollo de este trabajo, se han utilizado principalmente fuentes secundarias que incluyen legislación vigente, jurisprudencia relevante, doctrina académica, y estudios previos en el ámbito del derecho y la tecnología. Se han revisado y analizado textos legales tanto a nivel nacional como europeo, con especial atención a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y el Reglamento General de Protección de Datos (RGPD) de la UE. La jurisprudencia de los tribunales nacionales y del Tribunal de Justicia de la Unión Europea ha sido fundamental para entender la aplicación y los límites de las normativas en casos concretos. Las

opiniones de expertos y los comentarios académicos han proporcionado perspectivas críticas y profundidad al análisis.

El análisis se ha llevado a cabo mediante una revisión detallada de las fuentes mencionadas, buscando identificar y sintetizar los principales problemas y soluciones propuestas en la literatura y la práctica jurídica. Se ha hecho especial énfasis en el contraste entre la teoría legal y la práctica, evaluando cómo las disposiciones legales son aplicadas por los tribunales y afectan a la realidad social y empresarial. Además, se ha utilizado un enfoque comparativo en algunos puntos del análisis, examinando cómo diferentes jurisdicciones dentro y fuera de Europa abordan problemas similares, lo que permite una comprensión más rica y una perspectiva más amplia sobre los desafíos de la protección de datos en redes sociales.

Finalmente, el estudio incluye una evaluación crítica de las medidas actuales y propuestas de protección de datos en redes sociales. Esta evaluación considera la eficacia de las soluciones existentes y sugiere áreas donde se requieren enfoques innovadores para abordar las lagunas y deficiencias identificadas durante el análisis.

II. DERECHO LA PROTECCIÓN DE DATOS

1. ARTÍCULO 18 DE LA CONSTITUCIÓN ESPAÑOLA

El derecho a la intimidad personal y familiar se encuentra regulado en el artículo 18 de la Constitución Española (CE) de 1978 siguiendo la ruta marcada en la Declaración Universal de Derechos Humanos. Pese a que haya una satisfacción general por parte de la doctrina en relación con la regulación de este derecho fundamental, esto no ha sido impedimento para que se hayan generado controversias y dificultades sobre el conjunto de normas que regula este derecho, por lo que el papel del tribunal constitucional ha sido fundamental.

El artículo 18 de la Constitución Española dicta:

1. “Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento de su titular o resolución judicial, salvo caso de flagrante delito.
3. Se garantiza el secreto a las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”

Este artículo presenta una serie de particularidades como es la ausencia de una definición constitucional del derecho a la intimidad. En el artículo 18 podemos apreciar una garantía al derecho de la intimidad, no obstante, ni perfila ni define el concepto de intimidad. Según señala Fayos Gardó “*La cuestión no es baladí, pues no solo es clave en la garantía y protección de estos derechos, sino también en la relación con otros derechos fundamentales (libertad de expresión y el derecho a la información), con el propio desarrollo legislativo y con sus manifestaciones normativas en otros ámbitos de la vida jurídica, política y social*”[6].

La segunda peculiaridad que cabe destacar tiene relación con la naturaleza del derecho. La Constitución de 1978 no ayuda a distinguir si estamos ante un solo derecho individual (derecho a la intimidad) con distintas manifestaciones (derecho al honor, a la intimidad personal y familiar, y a la propia imagen); o si nos encontramos ante dos, o incluso tres derechos diferentes[7]. Martínez de Pisón coincide con O’Callaghan Muñoz[8] en que el artículo 18 CE regula tres derechos distintos; el derecho al honor, a la intimidad personal y familiar, y a la propia imagen. Y los tres constituyen los derechos de la personalidad.

Es importante destacar que el artículo 18 de la Constitución Española se sitúa en una sección prioritaria dedicada a los derechos fundamentales y las libertades públicas, concretamente en el Título II, Sección 1ª: “*De los derechos fundamentales y de las*

[6] Martínez de Pisón, J., “El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional”, *Anuario de filosofía del derecho*, n. 32, 2016, p. 414.
[7] *Ibid.*, p. 415.
[8] O’Callaghan Muñoz, X., *Libertad de expresión y sus límites: honor, intimidad e imagen*, Edersa, Madrid, 1991, p. 32.

libertades públicas". Esto subraya la importancia suprema de estos derechos en el ordenamiento jurídico español, asegurando una protección reforzada por parte de los tribunales. Esta ubicación refleja el compromiso del sistema legal con la preservación y el respeto de estos derechos esenciales, diferenciándolos en grado de protección frente a otros tipos de derechos.

2. DERECHO AL PRIVACY EN LA JURISPRUDENCIA CONSTITUCIONAL

El Tribunal Constitucional ha realizado una gran labor en la definición de este derecho fundamental y en la elaboración de un sistema coherente a través de una regulación que respete su contenido esencial según establece el artículo 56 CE[9].

Según señala Martínez Pisón "*los tres aspectos de los llamados derechos de la personalidad suelen aparecer diferenciados en las resoluciones del Tribunal Constitucional; que, en todo caso, puede existir una mayor ligazón entre el derecho a la intimidad personal y familiar y el derecho a la propia imagen; y que el derecho al honor encuentra su razón de ser, sobre todo, como límite de la libertad de expresión y el derecho a comunicar y a recibir información del art. 20 de la Constitución*"[10].

La jurisprudencia del Tribunal Constitucional en los primeros años de la década de 1980 establece los siguientes criterios como punto de partida para la delimitación del artículo 18 CE, manifestados durante numerosas sentencias:

- "Los derechos del artículo 18 CE son derechos personalísimos, derechos de la personalidad, derechos ligados a la persona.
- Están vinculados a la dignidad humana, lo que les conecta con el art. 10 CE y el conjunto de tratados internacionales sobre derechos y libertades fundamentales.
- Implican un espacio, un ámbito propio y reservado.
- Pretenden proteger ese ámbito íntimo de injerencias de terceros.

[9] Constitución Española de 1978 (BOE 311, 29 de diciembre de 1978)
[10] Martínez de Pisón, J. M., "La configuración constitucional del derecho a la intimidad", *Revista de Filosofía del Derecho y derechos humanos*, vol. 2, n. 3, 1994, pp. 316-318.

- El derecho a la intimidad no es un derecho absoluto, sino que su contenido debe responder a estimaciones y criterios arraigados en la cultura de la comunidad.
- En los casos de colisión del derecho a la intimidad con otros derechos fundamentales, es fundamental realizar una ponderación que valore los hechos relevantes y equilibre los bienes jurídicos en conflicto"[11].

Estos criterios generales se pueden apreciar en numerosas sentencias en los años 80s del siglo XX como por ejemplo en la STC 231/1988, de 2 de diciembre que dicta que "*los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18 de la CE aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la dignidad de la persona, que reconoce el art. 10 de la CE, y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana. Se muestran así estos derechos como personalísimos y ligados a la misma existencia del individuo*"[12].

En el artículo 18.4 CE, se reconoce explícitamente la dimensión de la libertad informática, entendiéndose esta como la prerrogativa de los ciudadanos a garantizar la confidencialidad de sus datos personales frente al tratamiento automatizado. Dicha preocupación se cristaliza en el artículo 18.4 de la Constitución Española, el cual establece una limitación normativa sobre el empleo de tecnologías de la información, con el fin de preservar el honor y la intimidad personal y familiar, así como asegurar la plena vigencia de los derechos individuales. Conforme a este precepto constitucional, se promulgó la Ley Orgánica 5/1992, de 29 de octubre (ya derogada), que regulaba el tratamiento automatizado de los datos de carácter personal, incorporando salvaguardas específicas para prevenir infracciones a la privacidad derivadas del procesamiento de información. Este marco legal se fundamenta en el principio de "implantar mecanismos cautelares", tal como se explicita en su Exposición de Motivos[13].

[11] Martínez de Pisón, J. *Op. cit*., p. 418.
[12] Sentencia del Tribunal Constitucional 231/1988, de 2 de diciembre, FJ 2.
[13] Martínez de Pisón, J. *Op. cit*., p. 421.

En una interpretación jurisprudencial reforzadora de esta normativa, la Sentencia del Tribunal Constitucional (STC) 254/1993, de 20 de julio, delimita el uso de la informática en el respeto al honor y la intimidad personal, articulando que la protección de la intimidad no solo posee una dimensión negativa (de no intervención), sino que se extiende a un aspecto positivo materializado en el derecho de control sobre los datos personales. En este contexto, la "libertad informática" se configura como el derecho de los individuos a supervisar el uso de sus datos personales almacenados en sistemas informáticos[14].

El Tribunal Constitucional reitera el carácter personalísimo de estos derechos contenidos en el artículo 18 CE, vinculando estos a la esfera individual de sus titulares y como una derivación de la idea de la dignidad contenida en el artículo 10.1 CE.

Durante las últimas dos décadas, el Tribunal Constitucional se ha dedicado a consolidar la doctrina en relación con el derecho fundamental del artículo 18 CE, el derecho a la intimidad personal y familiar. A través de numerosas sentencias ha ido perfilando y afinando la construcción jurídica de este derecho y solventando las lagunas legislativas que resultaban de dicho artículo.

Según señala Martínez de Pisón[15], algunas de las causas que justifican la tendencia constitucional a detallar y perfilar el derecho a la intimidad:

1. Crecimiento de los recursos de amparo abogando por una protección a los derechos del artículo 18 CE. Esto se debe a que, con el aumento de las nuevas tecnologías, redes sociales… cada vez es mayor el número de ciudadanos preocupados por su privacidad.
2. Difícil relación entre el derecho a la intimidad, el derecho a la imagen y al honor y los derechos contenidos en el artículo 20 CE, el derecho a la libertad de expresión y el derecho a la información.
3. Nuevos bienes o intereses ligados a la personalidad que merecen protección como por ejemplo los datos personales que se encuentran en ficheros informáticos y que han dado lugar a la libertad informática.

[14] Martínez de Pisón, J. *Op. cit*., p. 421.
[15] Martínez de Pisón, J. *Op. cit*., p. 423.

4. Por último, cada vez es más frecuente recurrir a mecanismos de ponderación de bienes para resolver los casos relativos a la intimidad y a la propia imagen.

Finalmente, la Constitución Española en su artículo 20.4 complementa las disposiciones sobre la intimidad, estableciendo que las libertades expresadas tienen como frontera el respeto hacia los derechos articulados en el mismo Título, las normas que los desarrollan y, en particular, la consideración hacia el honor, la intimidad personal, la propia imagen y la protección de menores. Ante la revolución tecnológica que estamos viviendo, y todos los problemas que surgen en relación con los datos personales y el derecho a la intimidad personal y familiar, se pone de manifiesto la necesidad de delimitar hasta dónde llega la libertad informática y la libertad de expresión.

3. REGULACIÓN ACTUAL DEL DERECHO A LA PROTECCIÓN DE DATOS

El derecho a la protección de datos es un derecho que está íntimamente relacionado con el derecho a la privacidad y se puede considerar como un derecho implícito en determinados textos de referencia como puede ser la Declaración Universal de los Derechos Humanos (artículo 12), pero se trata de un derecho que no dispone de un instrumento legal internacional común que aborde específicamente su protección[16]. El derecho a la protección de datos se trata de un derecho autónomo que atribuye a su titular "*un poder de disposición sobre sus propios datos personales*"[17], lo que implica un poder que abarca desde el derecho del afectado de consentir que se recojan y utilicen sus datos personales, hasta el derecho a ser informado sobre el destino de estos y a acceder, rectificar y cancelar dichos datos[18].

3.1.Sistema de protección de datos en el ámbito comunitario

[16] Bygrave, L.A., "Privacy and Data Protection in an International Perspective", *Scandinavian studies in law*, n. 56, 2010, p. 181.
[17] Piñar Mañas, J.L., *Seguridad, transparencia y protección de datos*, Fundaciones Alternativas, 2009, p.5.
[18] Minero Alejandre, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario Jurídico y Económico Escurialense,* n. 50, 2017, p. 20.

En este apartado nos centraremos en el análisis de la legislación de la Unión Europea (UE). Esta legislación destaca por sus avances significativos en la armonización de normativas destinadas a proteger los derechos de los individuos y facilitar la libre circulación de datos en el contexto del mercado único[19].

A nivel europeo, el derecho a la protección de datos es reconocido como un derecho fundamental en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE, en adelante) y en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea. Las Directrices de Privacidad de la Organización para la Cooperación y Desarrollo Económico (OCDE) de 1980 y el Convenio no 108 que adoptó el Consejo de Europa de 1981 sobre la protección de datos personales marcaron los primeros pasos internacionales hacia la regulación de la protección de datos, y crearon el primer y único instrumento internacional vinculante sobre protección de datos[20]. Estas directrices terminaron culminando en la Directiva 95/46/CE de 1995 que buscaba equilibrar la protección de la privacidad individual con la libre circulación de datos personales dentro de la UE, con objeto de armonizar la protección de los derechos individuales con el tratamiento de datos personales[21].

No obstante, según avanzó el tiempo y evolucionó Internet, se fueron identificando deficiencias en la Directiva 95/46/CE de 1995 que fue incapaz de adaptarse a la exponencial evolución de Internet y de crear una legislación uniforme. La incapacidad de crear una legislación uniforme fue consecuencia de numerosos preceptos que suscitaban dudas, especialmente en el ámbito territorial donde era necesaria la trasposición de la normativa en cada uno de los Estados miembro[22]. Este problema es identificado en la consideración 9 del Reglamento 2016/679 de Protección de Datos que dicta que "*aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión Europea se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas*

[19] Durán Arroyo, A., "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito", *Revista Jurídica de la Universidad Autónoma de Madrid*, n. 37, 2018, p.418.
[20] Gil González E., *Big data, privacidad y protección de datos*, Boletín Oficial del Estado, Madrid, 2016, p. 49.
[21] *Ibid*. p. 49.
[22] Durán Arroyo, A. *Op. cit*., p. 419.

físicas en particular del derecho a la protección de los datos de carácter personal. Hay diferencias en los niveles de protección debido a las diferencias en la ejecución y aplicación de la Directiva".

Estos problemas propiciaron una reforma legislativa y en 2012 la Comisión Europea propuso una modernización de la legislación que reflejara los principios originales de la Directiva 95/46/CE pero que también se adaptara a los nuevos retos de la realidad tecnológica de nuestra sociedad. Además, otro de los objetivos principales era crear un marco legal único para todos los Estados miembro de la Unión Europea que partiera de las mismas fuentes jurídicas que la Directiva, así como de sus bases y pronunciamientos del TJUE[23]. Esta reforma incorporó cambios de gran relevancia cómo un enfoque más estricto en la transparencia y consentimiento y reconoció nuevos derechos de privacidad como por ejemplo el derecho al olvido y la portabilidad de datos[24]. Asimismo, trata de fortalecer las obligaciones de transparencia e integrar el principio de privacidad por defecto y desde el diseño. De gran importancia es que la propuesta sigue apoyándose en el consentimiento informado como el principal mecanismo para la protección de los datos y la privacidad de los ciudadanos de la Unión Europea; en realidad, se subraya aún más el valor del consentimiento[25].

Como resultado, aparece el Reglamento 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 (RGPD en adelante) que reemplazó y derogó la Directiva 95/46/UE y estableció un marco legal unificado para toda la Unión Europea (UE, en adelante). El RGPD entra en vigor el 25 de mayo de 2018 y tiene como objeto mejorar la regulación para eliminar la fragmentación legal en la UE, y proporcionar una mayor seguridad jurídica tanto para los individuos como para los responsables del tratamiento de datos[26].

3.2.Protección de datos en España

[23] *Ibid*. p. 419.
[24] Gil González, E. *Op. cit. p. 54.*
[25] López Aguilar, J. F., "Por fin una ley europea de protección de datos (I)", Huffington Post, 24 de octubre de 2013 (disponible en https://www.huffingtonpost.es/juan-fernando-lopez-aguilar/ley-europea-de-proteccion-de-datos_b_4148971.html; última consulta 13/03/2024).
[26] Durán Arroyo, A. *Op. cit*. p. 419.

En el ámbito nacional, el derecho a la protección de datos fue desarrollado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (LOPD), y su Reglamento de desarrollo 1720/2007, de 21 de diciembre (Reglamento General de Protección de Datos). Por otro lado, también existían otras normas sectoriales que legislaban el derecho a la protección de datos como por ejemplo la Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la Información y de Comercio Electrónico o la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

No obstante, la legislación ha experimentado reformas debido a las modificaciones en las normas dentro de la UE. El Reglamento 2016/679, de aplicación directa en todos los estados miembros de la UE, establece un marco uniforme para la protección de datos. Este marco permite que las legislaciones nacionales especifiquen o complementen sus disposiciones para asegurar la coherencia y comprensión del texto a sus destinatarios, tal como se expresa en el Considerando octavo del Reglamento[27]: "*En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento*". En este contexto, España adoptó la Ley Orgánica 3/2018, de 5 de diciembre, sobre la Protección de Datos Personales y garantía de los derechos digitales, manteniendo la importancia de las normas sectoriales anteriormente mencionadas.

Adicionalmente, la Circular 1/2019 de la Agencia Española de Protección de Datos (AEPD en adelante), aborda el tratamiento de datos personales relativos a opiniones políticas y el envío de propaganda electoral, siguiendo el artículo 58 bis de la Ley Orgánica del Régimen Electoral General.

La normativa española sobre protección de datos, específicamente la Ley Orgánica 3/2018, se aplica de manera amplia. Esta cobertura incluye tanto el procesamiento total como parcial de datos personales, y también se extiende al procesamiento manual de datos personales que están destinados a ser almacenados en ficheros[28].

[27] Considerando octavo del Reglamento 2016/679, de 27 de abril de 2016, de Protección de Datos.
[28] Artículo 2.1. de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Sin embargo, existen ciertas excepciones[29] a esta aplicación. No se incluyen dentro de este ámbito los tratamientos de datos que ya están excluidos por el Reglamento General de Protección de Datos de la UE, así como los datos de personas fallecidas y los tratamientos sujetos a normas sobre protección de información clasificada. Además, cualquier tratamiento de datos que no esté directamente cubierto por el Reglamento de la UE debido a que se relaciona con actividades fuera del ámbito de aplicación del Derecho de la Unión Europea, se regirá por la legislación específica española o, en su defecto, por lo estipulado en el propio reglamento y la ley nacional. Esto se aplica, por ejemplo, a los tratamientos de datos realizados bajo la legislación electoral, en instituciones penitenciarias, o en registros civiles y mercantiles[30].

Por último, el tratamiento de datos realizado por los órganos judiciales en el curso de sus funciones, así como aquel que se realiza en la gestión de la Oficina Judicial, seguirá lo establecido tanto en el Reglamento de la UE como en la ley nacional, sin perjudicar las disposiciones aplicables de la Ley Orgánica del Poder Judicial[31].

III. REDES SOCIALES

1. CONCEPTO DE REDES SOCIALES

Las redes sociales pueden ser definidas como plataformas online que posibilitan a los usuarios crear perfiles públicos, intercambiar información, co-crear contenido y participar activamente en movimientos y debates sociales de manera descentralizada[32]. Estas plataformas proporcionan un espacio para que los individuos establezcan comunicación en Internet, creando perfiles personales y tejiendo redes basadas en interés comunes, facilitando así la conexión e interacción entre los usuarios[33].

---

[29] Artículo 2.2. de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[30] Artículo 2.3. de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[31] Artículo 2.4. de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[32] INTECO (Instituto Nacional de Tecnologías de la comunicación, "Redes Sociales, Menores de Edad y privacidad en la Red", *Observatorio de Seguridad de la Información*, 2007, p. 3.
[33] Ortiz López, P., "Redes sociales", Rallo Lombarte, A. (coord.) & Martínez Martínez R. (coord.), *Derechos y Redes sociales*, Civitas: Thomson Reuters, Pamplona, 2010, p. 24.

Los usuarios se sumergen en estas plataformas digitales con objeto de comunicarse, establecer relaciones sociales y compartir contenido. Estas comunicaciones pueden variar en relación con su alcance: desde comunicaciones directas con amigos hasta información disponible para amigos de amigos y, en algunos casos para el público general en Internet. No obstante, el acceso a los perfiles de otros usuarios en las redes sociales suele depender de la configuración de privacidad que cada uno aplique, así, por defecto, los perfiles en numerosas ocasiones suelen estar configurados como "abiertos" y todos los usuarios pueden ver toda la información contenida en ese perfil, lo que incluye fotos, vídeos y otros datos personales[34].

A modo de ejemplo, si introducimos en motores de búsqueda el nombre y apellidos de una persona que está registrada en una red social como por ejemplo LinkedIn, nos va a aparecer la pantalla de inicio del perfil de dicha persona, con sus datos personales que pueden varias desde fotos, fecha de nacimiento, aficiones… además de darnos la opción de registrarnos en la red social y de añadirle como amigo. El acceso a las redes sociales se ha amplificado de manera exponencial con la evolución de las nuevas tecnologías como las redes wifi o el 4G, que permiten a los usuarios estar 24 horas al día conectados a través de sus dispositivos móviles[35].

Por último, conviene destacar la emergente función comercial de las redes sociales. Actualmente, la gran mayoría de empresas utilizan estas plataformas para promocionar sus productos a un amplio público digital, realizar ofertas de empleo y evaluar la recepción de nuevos productos, lo que destaca la influencia de las redes sociales en el ámbito comercial contemporáneo[36].

2. CONCEPTO DE DATOS PERSONALES EN RELACIÓN CON LAS REDES SOCIALES

El concepto de datos personales es definido en distintas normativas y leyes:

[34] Beltrán Castellanos, J.M. "Aproximación al régimen jurídico de las redes sociales", *Cuaderno electrónico de estudios jurídicos*, n. 2, 2014, p. 63.
[35] *Ibid.* p. 64.
[36] *Ibid.* p. 64.

El actual convenio n.º 108+ de 2018 que actualiza la anterior versión de 1981, define los datos personales en su artículo 2 cómo "*cualquier información con respecto a un individuo identificado o identificable*", al que denomina cómo "*titular de datos o interesado*".

El concepto de "dato personal" también es definido en el artículo 4 del Reglamento 2016/679 del Parlamento Europeo y del Consejo como "*toda información sobre una persona física identificada o identificable*". De esta forma, podemos observar que existen dos tipos de datos personales, que son "*toda información sobre una persona física identificada*" y "*toda información sobre una persona física identificable*".

Así, el RGPD ha recogido lo siguiente "*se considerará persona física identificable toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha personal*".

Según Andoni Polo Roca hablamos de un dato relativo a una persona física identificada cuando el dato indica directamente a esa persona sin necesidad de acudir a un conjunto de medios para poder averiguar su identidad (DNI o pasaporte). Por otro lado, hablamos de un dato relativo a una persona física identificable cuando el dato no indica la identidad de esa persona, ni aporta suficiente información acerca de la misma, pero sí aporta información suficiente para poder averiguar su identidad. De esta forma, a través de los medios adecuados dicho dato permite la identificación exacta del individuo o persona física[37].

La Agencia de Protección de Datos[38] para determinar la naturaleza de un dato como personal, se guía por las indicaciones establecidas en las recomendaciones del Comité de

[37] Polo Roca, A. "Datos, datos, datos: El dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos", *Estudios de Deusto: revista de Derecho Público*, vol. 69, n. 1, 2021, p.217.

[38] Informe 425/2006 de la Agencia Española de Protección de Datos (disponible en https://vlex.es/vid/724113085; última consulta 01/04/2024)

Ministros del Consejo de Europa. Estas directrices señalan que un individuo se considera identificable cuando su identificación no requiera ni plazos ni esfuerzos desproporcionados.

Adicionalmente, el Grupo de Trabajo del Artículo 29 (G29), en la actualidad Comité Europeo de Protección de Datos (CEPD) como consecuencia de que el RGPD creara dicho organismo europeo independiente para sustituir al GT 29, detalló los elementos clave que definen un dato personal de la siguiente manera:

1º- "cualquier información": hace referencia a cualquier tipo de información, cualquiera que sea su naturaleza, forma o contenido. Esto incluye discusiones sobre datos biométricos y las implicar legales de usar muestras biológicas de individuos.
2º- "relativo": relacionado con aspectos tales como el contenido, propósito o efecto, incluyendo información que pueda influir significativamente en cómo se percibe o se trata a una persona.
3º- "identificada o identificable": se centra en la capacidad de identificar a una persona utilizando medios razonables.
4º- "persona física": Aplica exclusivamente a ser humanos vivos. No obstante, se consideran aquellas situaciones particulares de personas fallecidas, nonatos y las entidades jurídicas.

3. DESAFÍOS JURÍDICOS PLANTEADOS POR LOS ELEMENTOS DE LAS REDES SOCIALES

Las redes sociales tienen una serie de elementos básicos o caracteres comunes independientemente de la función de la red social o de su ámbito. Una de estas características comunes es la capacidad de conectar personas de manera eficiente, sencilla y en teoría, segura. Todas las redes sociales promueven la interacción de sus usuarios, facilitando el intercambio de fotos, vídeos e información variada, además de fomentar nuevas conexiones[39].

[39] Beltrán Castellanos, J.M. *Op. Cit.* p. 65.

Uno de los aspectos que cabe destacar de las redes sociales es su capacidad para eliminar barreras geográficas temporales, permitiendo la comunicación desde cualquier lugar y en cualquier momento, siempre y cuando se disponga de acceso a Internet.

El tercer aspecto que destacar sobre las redes sociales es lo que se denomina en muchas ocasiones como la difusión viral, ya que los contactos se comunican con toda su red de contactos y estos hacen lo mismo, pudiéndose expandir el fenómeno red social de forma casi ilimitada por toda la plataforma. En muchas ocasiones, esto lleva a que las redes sociales sean comparadas con un virus ya que su finalidad principal consiste en expandirse en la red, ampliando al máximo número posible su número de usuarios[40].

Actualmente las redes sociales desempeñan un papel fundamental en la comunicación y en el intercambio de información. No obstante, esta irrupción en nuestra sociedad es acompañada de retos significativos en relación con la protección de datos. La naturaleza intrínseca de estas plataformas cuyo objeto es promover la compartición abierta de información personal, en muchas ocasiones entra en conflicto con los principios generales de protección de datos lo cual lleva a vulneraciones específicas que pueden socavar la privacidad y seguridad de los usuarios[41].

Los principales problemas que podemos identificar son[42]:

En primer lugar, uno de los principales desafíos actuales en las redes sociales es la paradoja de la exposición y la protección de datos[43]. Existe un problema derivado de la falta de concienciación por parte de los usuarios de la información que hacen pública en la red. Los usuarios al configurar sus perfiles en las redes sociales inadvertidamente ponen en riesgo su privacidad al exponer datos que en ningún caso expondrían en su vida "offline". Tales datos íntimos frecuentes en las redes sociales pueden variar desde aquellos que tienen relación con la ideología política, a los que tienen que ver con la orientación sexual de los usuarios, datos sobre su situación económica…[44] Todo esto

[40] *Ibid.* p. 65.
[41] Perelló, E. M., "Impacto de las redes sociales en el derecho a la protección de datos personales", *Anuario Facultad de Derecho, Universidad de Alcalá*, 2009, n. 2, 2019, p.122.
[42] Ortiz López, P. *Op. cit.* pp. 33-36.
[43] Perelló, E. M., *Op. cit.* p.122.
[44] Ortiz López, P. *Op. cit.* pp. 33-36.

ocurre ya que frecuentemente se opta por perfiles públicos con el objetivo de maximizar la visibilidad del perfil en la red social y crear más conexiones con otros usuarios. No obstante, muchas veces las preferencias que se establecen por defecto en las plataformas son las menos protectoras para la privacidad y son escogidas por los usuarios sin que tengan plena conciencia de las repercusiones que puede llegar a tener en su identidad digital.

En segundo lugar, encontramos el problema del tratamiento de datos de los menores en las redes sociales. Se considera que los menores de edad no han alcanzado el grado de madurez suficiente y por ello requieren una protección especial en las redes sociales, además de que su consentimiento es insuficiente y deber ser completado con el consentimiento de sus padres o tutores[45]. El tema de la protección especial de los menores en las redes sociales será tratado más adelante con mayor detalle por su complejidad. No obstante, la estrategia predominante de restringir el acceso a los menores o controlar el contenido accesible para ellos no aborda el problema de fondo. Como soluciones más efectivas que la simple prohibición, surgen las ideas de la educación y concienciación. El autor Piñar Mañas, J.L.[46] resalta la importancia de educar a los menores sobre los riesgos y cómo navegar de forma segura en el espacio digital, y critica la aplicación de medidas restrictivas para menores como solución del problema.

En tercer lugar, podemos destacar que los datos publicados pueden ser indebidamente utilizados por terceros: a través de las redes sociales las personas dan a conocer sus horarios, donde suele estacionar su vehículo, la marca y el modelo de su vehículo, el colegio de sus hijos menores de edad… Además, también se puede dar el supuesto de que se publique información falsa lo que puede llegar a crear situaciones jurídicas perseguibles como la vulneración del derecho al honor. También, suelen ser frecuentes en las redes sociales los casos de suplantación de identidad[47].

Otro de los problemas frecuentes en las redes sociales se da en los casos en los que se involucra en las redes sociales a personas que no son usuarios activos, por ejemplo, a

[45] *Ibid.* pp. 33-36.
[46]Piñar Mañas, J. L., "Protección de datos personales y fundaciones", *Anuario de derecho de fundaciones*, n. 1, 2009, p. 122.
[47] Beltrán Castellanos, J.M. *Op. Cit.* p. 66.

través de la publicación de una foto o de datos personales sin su consentimiento. Estos supuestos en muchas ocasiones afectan al derecho al honor, intimidad y la propia imagen, y además generan un gran conflicto entre el derecho a la libertad de expresión y la privacidad[48].

Por último, es importante mencionar que cancelar la suscripción en una red social no garantiza la eliminación definitiva de todos los datos personales, especialmente en el caso de aquellos datos personales que hayan sido compartidos o guardados por otros usuarios de la plataforma. Además, la plataforma intentará persuadir al usuario que tiene por objeto cancelar su suscripción para que reconsidere su decisión de abandonar la plataforma. Es frecuente que lancen preguntas que hagan dudar al usuario sobre la decisión de abandonar y en las que le recuerden la cantidad de conexiones que perderá. Además, el usuario debe exponer el motivo de su baja y completar un formulario. Antes de que se inactive la cuenta, el usuario suele ser informado de que dispone de un plazo para recuperar la cuenta (1-3 meses en general), y de la posibilidad de recuperarla en cualquier momento[49]. No obstante, conviene subrayar la dificultad de asegurar el olvido digital del contenido de datos personales en una red social una vez compartido. No se puede garantizar que un tercero no haya copiado o utilizado datos antes de que estos hayan sido eliminados[50]. Esta falsa ilusión de control que tienen los usuarios supone una amenaza para el derecho de protección de datos ya que los usuarios tienen la percepción de tener un falso control en relación con sus datos personales en las redes. Las plataformas, pese a ofrecer opciones de cancelación, tienen una naturaleza interconectada que hace que la eliminación efectiva de la información sea prácticamente imposible. En un caso contra Facebook, se realizó la recomendación de eliminar los datos de los usuarios que hubieran desactivado sus cuentas pasado un periodo razonable y, en todo caso, que se informara sobre ello a los usuarios[51].

[48] Ortiz López, P. *Op. cit.* pp. 33-36.
[49] Beltrán Castellanos, J.M. *Op. Cit.* p. 67.
[50] Perelló, E. M., *Op. cit.* p.123.
[51] Denham, E. (2009). Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques. Oficina del Comisionado de Privacidad de Canadá (disponible en https://publications.gc.ca/collections/collection_2010/privcom/IP54-31-2009-fra.pdf; última consulta 20/03/2024)

4. PRINCIPIOS DE PROTECCIÓN DE DATOS EN RELACIÓN CON LAS REDES SOCIALES

El Reglamento General de Protección de Datos señala un conjunto de principios que los responsables y encargados del tratamiento, en este caso, los proveedores de servicios de redes sociales (SRS, en adelante), deben tener en cuenta a la hora de tratar datos personales. Los proveedores de SRS encajarían dentro de la definición del artículo 4 apartado 7 del RGPD de responsable del tratamiento, ya que se encargan de recabar, almacenar, y procesar los datos personales de los usuarios. Estas responsabilidades implican asegurar que todas las operaciones con datos personales se hagan respetando las leyes de protección de datos, para lo que deben garantizar la seguridad y privacidad de la información de los usuarios[52]. Los principios son[53]:

i. Principio de licitud, transparencia y lealtad: el RGPD en su artículo 5 apartado a, recoge este principio estableciendo la obligación para los responsables del tratamiento de datos de que el trato se realice de manera lícita, leal y transparente en relación con el interesado.

ii. Principio de finalidad: recogido en el artículo 5 apartado b, este principio implica que los datos sean tratados con un objetivo determinado, explícito y legítimo, y además establece la prohibición de que esos datos recogidos con finalidades determinadas sean tratados posteriormente de una manera incompatible con aquellos fines.

iii. Principio de minimización de datos: recogido en el apartado c, este principio aboga por la implementación de unas medidas técnicas y de gestión que aseguren que únicamente se procesan los datos estrictamente necesarios para los objetivos específicos de su tratamiento, minimizando así la cantidad de datos tratados y limitando su tiempo de conservación y accesibilidad.

[52] Perelló, E. M., *Op. cit.* p.118.
[53] Agencia Española de Protección de Datos (disponible en https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/principios; última consulta 21/03/2024)

iv. Principio de “exactitud”: recogido en el apartado d, obliga a los responsables a eliminar o modificar aquellos datos que sean inexactos, y a mantener actualizados los datos.

v. Principio de limitación del plazo de conservación: recogido en el apartado e, refleja la idea de reducción de datos al requerir que la retención de estos se limite al tiempo necesario para cumplir con los objetivos del tratamiento. Al concluir estos objetivos, los datos deben ser eliminados, restringidos o, en su caso, anonimizados, eliminando cualquier posibilidad de identificar a los sujetos implicados.

vi. Principio de seguridad: recogido en el apartado f, obliga a los responsables del tratamiento de datos a realizar un análisis de riesgos para identificar y aplicar las medidas técnicas y de gestión necesarias para proteger la integridad, disponibilidad y confidencialidad de los datos personales.

vii. Principio de responsabilidad activa o demostrada: exige a los responsables del tratamiento mantener una diligencia constante para proteger y asegurar los derechos y libertades de las personas cuyos datos se procesan, evaluando los riesgos que dicho tratamiento pueda representar para estos derechos y libertades, de tal manera que el encargado pueda garantizar y demostrar el cumplimiento de las normativas del RGPD y la LOPDGD.

Un ejemplo sobre la importancia de respetar estos principios y la importante labor de la Agencia Española de Protección de datos se puede apreciar en el caso de Facebook contra la AEPD. Facebook adquirió Whatsapp en 2014. Posteriormente, en agosto de 2016, Whatsapp actualizó sus términos de servicio y políticas de privacidad, implementando cambios significativos como la compartición de información de sus usuarios con Facebook. En este caso, la Agencia Española de Protección de Datos (AEPD, en adelante) impuso sanciones de 300.000 euros tanto a WhatsApp como a Facebook por infracciones graves de la Ley Orgánica de Protección de Datos. WhatsApp fue sancionada por transferir datos a Facebook sin obtener un consentimiento válido de los usuarios, mientras que Facebook fue sancionada por procesar esos datos para sus propios fines sin consentimiento (vulneración del principio de finalidad). La controversia surgió después

de que WhatsApp actualizara sus términos de servicio y política de privacidad en 2016 para permitir compartir información del usuario con Facebook. La AEPD concluyó que el consentimiento requerido para la transferencia y tratamiento de datos no se obtuvo de manera libre, específica e informada, violando así los requisitos legales (violación del principio de licitud, transparencia y lealtad). La resolución destacó la falta de claridad y precisión en la información proporcionada a los usuarios sobre el uso y finalidad de sus datos, determinando que el consentimiento obtenido no era válido[54].

IV. PRINCIPALES DESAFÍOS DE LA PROTECCIÓN DE DATOS EN LAS REDES SOCIALES

1. CONSENTIMIENTO EN LAS REDES SOCIALES

El consentimiento en las redes sociales se configura como un requisito imprescindible en el tratamiento de datos, ya que, de no existir el consentimiento por parte del titular de los datos, se podría dar la difusión de determinada información cuyo titular no está a favor de que se conozca[55]. En el momento del registro en una red social, el futuro usuario proporciona una serie de datos personales con el objetivo de crear y completar su perfil. Durante este proceso, los proveedores de Servicios de Redes Sociales (SRS) necesitan del consentimiento del propietario de la información. Sin embargo, y como ya ha sido mencionado anteriormente, en el caso de los menores de edad (menores de 14 años[56]) también será necesario el consentimiento de los padres o tutores legales[57].

Dentro del contexto legal, el concepto de consentimiento para el tratamiento de datos se encuentra regulado por el artículo 4 apartado 11 del RGPD 2016/679 del Parlamento Europeo y del Consejo que establece que el consentimiento del interesado es "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el*

[54] Agencia Española de Protección de Datos (disponible en https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar; última consulta 21/03/2024)
[55] Arenas Ramiro, M., "El consentimiento en las redes sociales "on line"", Rallo Lombarte, A. (coord.) & Martínez Martínez R. (coord.), *Derechos y Redes sociales*, Civitas: Thomson Reuters, Pamplona, 2010, pp. 118.
[56] Artículo 7.2. de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[57] Beltrán Castellanos, J.M. *Op. Cit.* p. 79.

tratamiento de datos personales que le conciernen". Por tanto, esta normativa se aplica a los datos proporcionados tanto en las redes sociales como en otros contextos. Además, según el RGPD 2016/679 los datos que se facilitan en las redes sociales son "personales" atendiendo a la definición proporcionada de "dato personal" del artículo 4 apartado 1 del RGPD.

El RGPD establece que el consentimiento debe ser una expresión de voluntad que sea libre, clara, específica e informada. De esta definición se deprenden varios criterios para el consentimiento[58]:

i. Libre: implica que se otorga sin coerción, intimidación o error, a menudo en la de que la información se comparte en un entorno privado.
ii. Informado: Lo cual obliga a los proveedores de SRS a presentar de manera accesible y fácilmente comprensible las condiciones de uso y privacidad de las plataformas. Esto es especialmente importante en las redes sociales ya que gran parte de los usuarios son menores de edad. Sin embargo, y uno de los mayores problemas en las redes sociales, es que rara vez los usuarios leen los términos de servicio, especialmente si estos son extensos y complejos.
iii. Específico: el consentimiento se debe dar para un propósito claro, aunque la información compartida pueda utilizarse más allá de ese propósito inicial.
iv. Inequívoco: asegura que no haya dudas sobre la voluntad del individuo, lo cual se complica con el consentimiento tácito, especialmente en situaciones como ser etiquetado en fotos sin conocimiento previo.
v. Previo: otorgado antes de convertirse en usuario activo de la plataforma.
vi. Revocable: esto hace referencia a que, en teoría, se debería de poder retirar el consentimiento y eliminar toda la información personal publicada, aunque en la práctica, controlar la información una vez compartida en internet puede ser muy difícil.

2. DERECHO AL OLVIDO

[58] *Ibid.* p. 80.

En la actualidad, el derecho al olvido ha emergido como una extensión necesaria de la protección de datos y de la privacidad, tratando de adaptarse a todos los desafíos que presenta Internet. Este derecho es definido como la capacidad de los individuos para solicitar la eliminación personal o irrelevante en plataformas digitales, incluidos los motores de búsqueda y redes sociales[59].

El derecho al olvido encuentra su origen en épocas anteriores a la era digital, apareciendo por primera vez a finales del siglo XIX en Estados Unidos, donde se comenzó a reconocer y proteger este derecho, culminando en el caso Melvin v. Reid en 1931, donde se afirmó el derecho de las personas de olvidar su pasado y ser perdonados. Contrariamente, en el caso Time Inc. V. Hill de 1967 se estableció la figura de "persona pública involuntaria"[60], limitando el derecho al olvido y en favor de la libertad de expresión. Años más tarde, la jurisprudencia francesa también abordó este derecho, especialmente en los casos de los años 60 a los años 80, defendiendo las segundas oportunidades y reconociendo el "*droit a l'oublie*" (derecho al olvido). Estos casos, junto con la Ley francesa de 1978 sobre el tratamiento de información personal, establecieron las bases previas a la digitalización para el derecho al olvido, destacando la importancia de encontrar un equilibrio ente la privacidad de los individuos que se vuelven figuras públicas involuntariamente y el interés público[61].

El auge digital ha resaltado diferencias significativas entre Europa y Estados Unidos en relación con el manejo de la información personal en Internet. Mientras en Europa se considera que el interés público con el paso del tiempo desaparece por lo que la información no debe estar siempre accesible, mientras que en Estados Unidos se considera que no desaparece. En el año 2014 se produce un punto de inflexión con la sentencia del Caso Costeja, dictada por el TJUE[62]. El litigio se basaba en conocer si Google estaba obligada a borrar de su plataforma y de Internet los datos personales de una noticia, y los datos pertenecían al pasado de la vida privada de un ciudadano. Esta

[59] Corral Talciani, H., "El derecho al olvido en Internet*"*, *Revista Jurídica Digital UANDES*, vol. 1, n. 1, 2017, p. 43.
[60] Corte Suprema de EE. UU., caso *Time Inc. v. Hill* de 9 de enero de 1967.
[61] Moreno Boadilla, A., "Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital". *Estudios constitucionales: Revista del Centro de Estudios Constitucionales*, vol.18, n. 2, 2020, p. 126.
[62] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), asunto C-131/12, de 13 de mayo de 2014.

sentencia marcó un precedente al consolidar el derecho al olvido en Europa, alejándose de la postura estadounidense. Con el fallo se estableció que buscadores como Google son responsables del tratamiento de datos y que pueden ser requeridos para eliminar información personal obsoleta o irrelevante de sus resultados de búsqueda, aunque la información personal permanezca en su fuente[63].

La actualización del marco legal europeo sobre protección de datos personales condujo a la adopción del Reglamento General de Protección de Datos (RGPD) en 2018, reemplazando la Directiva 95/46 por su inadecuación ante los retos digitales emergentes. El RGPD, aplicable a entidades que gestionan datos en redes sociales, excluye usos puramente personales y refuerza el derecho al olvido como un derecho individual y una responsabilidad de los encargados de tratamiento de datos[64]. Este derecho se reconoce en el considerando 39 del RGPD, que establece que "*para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos*".

El concepto de derecho al olvido, que es mencionado como sinónimo del derecho de supresión en el RGPD, amplía su protección más allá del derecho de supresión en el considerando 66 del RGDP que manifiesta que "*a fin de reforzar el "derecho al olvido" en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales*".

Las condiciones bajo las cuáles los responsables del tratamiento de datos deben eliminar todos los enlaces, copias o réplicas de datos personales son desarrolladas por el artículo 17 RGPD. Estas condiciones incluyen supuestos cómo; la irrelevancia de los datos para

[63] Moreno Boadilla, A. *Op. cit.* p. 129.
[64] *Ibid.* p. 133.

los fines originales, la retirada del consentimiento del interesado, y la oposición al tratamiento de datos para mercadotecnia, entre otras. El RGPD instaura una responsabilidad proactiva para las entidades digitales, exigiendo que la protección de datos se integre desde el diseño y por defecto, para prevenir violaciones de privacidad. En palabras de Juan Carlos Bayo "*se exige una responsabilidad proactiva, en lugar de la responsabilidad reactiva (enfoque basado en riesgos), debiéndose actuar con carácter preventivo, tener la diligencia debida para evitar tratamientos o incumplimientos no deseados en la protección de los intereses de los ciudadanos en el ámbito de su privacidad"* [65].

El RGPD busca mitigar las prácticas que puedan afectar a los derechos de privacidad de los usuarios, con la AEPD imponiendo sanciones a las infracciones que vulneren estos derechos. En esencia, el RGPD codifica el derecho al olvido en el contexto digital, buscando un equilibrio ente la protección de la privacidad personal y los derechos de acceso a la información y libertad de expresión[66].

La regulación internacional también ha seguido avanzando en la protección del derecho al olvido, como es evidente en la legislación de Alemania y el Reino Unido, reflejando diversas aproximaciones a la privacidad y protección de datos. Alemania, por ejemplo, ha implementado la Ley de Redes Sociales (NetzDG) en 2017, que exige a las plataformas sociales eliminar contenido ilegal dentro de 24 horas bajo la amenaza de multas de hasta 50 millones de euros. Esta ley pone en evidencia la seriedad con la que Alemania aborda la regulación del contenido en las plataformas digitales proporcionando un modelo de intervención proactiva que podría considerarse en otros contextos[67].

3. DESAFÍOS EN RÉGIMEN ESPECIAL DEL MENOR EN LAS REDES SOCIALES

Las redes forman parte de nuestra vida cotidiana y han generado grandes desafíos en la protección de los datos personales, especialmente en el caso de los menores de edad. Los jóvenes han incrementado su actividad en línea, y esto sumado a su vulnerabilidad

[65]Bajo, J. C., "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el compliance", en López Calvo, José (coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Wolters Kluwer, Madrid, 2018, p. 281.
[66] Moreno Boadilla, A. *Op. cit.* p. 145.
[67] *Ibid.*p.137.

inherente ha planteado grandes desafíos para los legisladores, educadores, padres y para las propias plataformas digitales[68].

EL marco legal de los menores en relación con la protección de los datos personales está regulado por el RGPD y por la LOPDGDD, que establecen un marco de acción para la protección de los menores. El tratamiento de datos de los menores de edad viene delimitado a un rango de edad por el RGPD en su artículo 8 que establece que "*el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó*". Por otro lado, también establece que "*Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años*". De este modo, se prohíbe el tratamiento de datos personales de menores de 16 años sin el consentimiento parental, salvo en aquellos casos donde la legislación de los Estados miembros disponga de una edad inferior, que no podrá ser menor de 13 años. En España, el artículo 7 de la LOPDGDD establece que "*el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años*", por lo que el límite legal para que los menores puedan dar su consentimiento en cuanto al tratamiento de sus datos en redes sociales se sitúa en los 14 años.

La especial protección de los menores en el ámbito de la protección de datos se puede observar en numerosos artículos de la LOPDGDD. El Tribunal Supremo también se ha manifestado a estos efectos, declarando que se debe proteger la intimidad de todas las personas, pero con más razón cuando se trate de la infancia, ya que la población infantil es más desvalida y vulnerable[69]. Entre las normas que refuerzan la protección de los menores encontramos:

El artículo 84 LOPDGDD de protección de los menores en Internet establece que:

[68] Hernández Serrano, M. J., Renés-Arellano, P., Campos Ortuño, R. A., & González-Larrea, B., "Privacidad en redes sociales: análisis de los riesgos de auto-representación digital de adolescentes españoles", *Revista Latina de Comunicación Social*, n. 79, 2021, p. 135.
[69] Sentencia del Tribunal Supremo Sala 1ª 621/2003, de 27 de junio.

1. "*Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información*"
2. "*La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor*".

El artículo 92 LOPDGDD de protección de datos de los menores en Internet establece que:

> "*Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información*".

La LOPDGDD además de establecer estas obligaciones, considera el trato de los datos personales de los menores en su artículo 73 b, como grave e impone sanciones y medidas cautelares ante la vulneración de los derechos de los menores en relación con el tratamiento de sus datos personales.

Entre los principales retos en la protección de los menores en relación con las redes sociales encontramos[70]:

i. Derecho al olvido digital para menores

En relación con el derecho al olvido digital para menores de edad el artículo 12.6. de la LOPDGDD, otorga a los titulares de la patria potestad a ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles.

[70] Hernández Serrano, M. J., Renés-Arellano, P., Campos Ortuño, R. A., & González-Larrea, B. *Op. cit.* p. 136.

Es interesante comentar el caso de Reino Unido, que ha actualizado su normativa a través de la entrada en vigor del reglamento Data Protection Act 2018[71], que según las palabras de Marina Sancho "*han incorporado derechos reconocidos en el Reglamento como el de acceso a los datos, a su traslado y a su borrado, incluyendo el derecho al olvido, así como incorporando prerrogativas nuevas como la facultad de solicitar el borrado automático de todo lo publicado en las redes sociales con una edad menor a los 18 años (bautizado popularmente como el "derecho a la inocencia")*"[72]. Esto muestra una adaptación del derecho al olvido a las realidades de la edad digital, asegurando que los individuos, especialmente los jóvenes, puedan reclamar una segunda oportunidad respecto a la información que podría afectar su vida futura.

ii. Responsabilidad de las plataformas de las redes sociales en relación con la verificación de la edad y el consentimiento parental

El artículo 28.1. de LOPDGDD establece que los responsables y encargados del tratamiento de datos, es decir, los proveedores de los SRS, "*determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento*" y subraya la existencia de un riesgo mayor en relación con la adopción de estas medidas en el artículo 28.2.e., "*Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad*".

Carlos Barriuso Ruiz señala que la responsabilidad de las redes sociales no se limita únicamente a las acciones bienintencionadas o indiferentes de los usuarios, especialmente cuando son menores. Destaca que la omisión en la verificación de edad para fines legales, respecto al consentimiento y la validez de los actos que los menores llevan a cabo en estas plataformas, constituye una "obligación" para los propietarios de las redes sociales[73].

[71] Moreno Boadilla, A. *Op. cit.* p. 137.
[72] Sancho López, M. & Plaza Penadés, J., *La protección de datos en el Reino Unido: evolución del right to privacy y escenarios post-Brexit*, Thomson Reuters Aranzadi, 2019, p. 171.
[73] Barriuso Ruiz, C., "Las redes sociales y la protección de datos hoy", *Anuario de la Facultad de Derecho,* n. 2, 2019, p. 332.

iii. Educación y concienciación digital

Esta creciente preocupación por la seguridad de los menores en Internet y en las redes sociales ha sido reflejada en la jurisprudencia y en las iniciativas de organismos internacional. En España, la AEPD[74] ha publicado numerosas guías y recomendaciones dirigidas a fomentar un uso seguro de Internet y las redes sociales por parte de los menores, así como para concienciar a los responsables de las plataformas sobre su importante papel en la protección de este grupo vulnerable.

Además, el artículo 97 de la LOPDGDD establece la obligación al Gobierno, para que en colaboración con las Comunidades Autónomas (CCAA, en adelante) elabore un "*un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales*".

Como hemos mencionado anteriormente, el autor Piñar Mañas, J.L.[75] resalta la importancia de educar a los menores sobre los riesgos y cómo navegar de forma segura en el espacio digital, y critica la aplicación de medidas restrictivas para menores como solución del problema.

V. TRATAMIENTO ILÍCITO DE DATOS

En el sistema español el derecho a la protección de datos ha sido delimitado por nuestros tribunales según afirma Elena Gil. Los tribunales españoles definen el derecho a la protección de datos como la capacidad de gestionar y controlar los propios datos personales. Este derecho permite a una persona decidir sobre qué información quiere compartir con terceros, ya sean entidades estatales o privadas, y conocer quién tiene

[74] Agencia Española de Protección de Datos (disponible en https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-recomendaciones-orientadas-evitar-el-acceso; última consulta 25/03/2024)
[75] Piñar Mañas, J. L., *Op. cit*. p. 122.

acceso a sus datos y con qué propósito. Además, brinda al individuo la posibilidad de rechazar que otros posean o utilicen sus datos personales. Su carácter como derecho fundamental le confiere una protección especial, como es el hecho de ser un derecho irrenunciable o que puede prevalecer sobre otros derechos no fundamentales[76].

En el sistema español, la Agencia Española de Protección de Datos (AEPD, en adelante) juega un papel fundamental. La AEPD fue fundada en 1983 y se trata de una agencia pública que tiene como misión encomendada que la Ley Orgánica de Protección de da Datos de Carácter Personal en España se aplique de manera efectiva. Opera como una entidad pública autónoma, distanciada de la administración gubernamental en sus operaciones y con una jurisdicción que se extiende a todo el territorio nacional. Igualmente, en España existen agencias dedicadas a la protección de datos en ámbitos autonómicos, y concretamente, en Cataluña y País Vasco.

Entre las obligaciones de la AEPD, encontramos la obligación de salvaguardar derechos fundamentales como el acceso, la rectificación, la limitación, la oposición, la supresión (conocido como "derecho al olvido"), la portabilidad de los datos y la oposición a la toma de decisiones automatizadas. Por otro lado, la AEPD también establece las obligaciones de aquellos que manejan los datos personales, ya sean organizadores, compañías o entidades gubernamentales[77].

La AEPD tiene como propósito principal la supervisión de las entidades responsables del archivo de datos, lo que incluye tanto a empresas privadas y asociaciones como a instituciones públicas, y hacer que cumplan con la vigente legislación de protección de datos. Así, de esta manera asegura el respeto al derecho fundamental de protección de datos personales de los ciudadanos[78]. Por último, cabe añadir que la AEPD ejerce sus funciones de investigación principalmente a instancia de parte y cuando exista una solicitud por parte de un ciudadano. Sin embargo, tiene potestad para iniciar un proceso de investigación. Como es un organismo jurídico independiente, mantiene una relación con el gobierno a través del Ministerio de Justica.

---

[76] Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre de 2000.

[77] Agencia Española de Protección de Datos (disponible en https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos; última consulta 25/03/2024).

[78] Agencia Española de Protección de Datos (disponible en https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos; última consulta 25/03/2024).

En relación con el tratamiento ilícito de datos, como hemos mencionado en el párrafo anterior, el proceso de investigación puede ser iniciado por la solicitud de un ciudadano. Así, el artículo 77.1. del RGPD concede a cualquier persona el derecho a presentar una reclamación ante una autoridad supervisora si "*considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento*". Esta reclamación en particular puede realizarse en el Estado miembro que sea el lugar de residencia del individuo, lugar de trabajo o en el lugar donde se haya cometido la infracción. Este procedimiento, que requiere menos costes y esfuerzos que las acciones judiciales, es crucial para que los individuos afectados puedan solicitar la protección de sus derechos[79].

En situaciones donde un individuo perciba un manejo inadecuado de sus datos, tiene varias opciones para buscar remedio: puede buscar el amparo administrativo de las autoridades de supervisión o alternativamente, tiene la opción de tomar acciones legales directamente contra la entidad que maneja los datos y, conforme al Reglamento General de Protección de Datos, contra aquellos encargados del procesamiento[80].

1. RECLAMACIONES ANTE LAS AUTORIDADES DE CONTROL Y TUTELA JURISDICCIONAL

Se debe destacar que los cambios realizados en el Reglamento General de Protección de Datos han empoderado significativamente a las autoridades reguladoras del derecho de protección de datos, que han sido denominadas como "guardianas de los derechos relacionados con el tratamiento de datos personales"[81] en todos los Estados miembros de la Unión Europea, otorgándoles una amplia gama de facultades y responsabilidades. Este desarrollo se evidencia de manera notable a partir del caso Schrems[82].

Con la introducción del nuevo Reglamento, se modifican las jurisdicciones en términos de alcance de la autoridad y de los poderes conferidos a las autoridades de control,

[79] De Miguel Asensio, P. A., "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea", *Revista Española de Derecho Internacional,* vol. 69, n. 1, 2017, p.91.
[80] *Ibid.* p.91.
[81] Sentencia del Tribunal de Justicia de la Unión Europea C-518/07 de 9 de marzo de 2010 (Diario Oficial de la Unión Europea, 1 de mayo de 2010), párr. 23.
[82] Sentencia del Tribunal de Justicia de la Unión Europea C-362/14, de 6 de octubre de 2015, *Schrems*, (Diario Oficial de la Unión Europea, 6 de octubre de 2015).

eliminándose la vinculación directa entre las leyes nacionales y las competencias, como consecuencia de la unificación normativa que trae consigo este nuevo marco legal. Esto significa que el rango de acción y competencias ya no está confinado al Estado Miembro de origen[83].

La partida inicial es la definición de una "autoridad de control principal", que corresponde a la del establecimiento principal o del único establecimiento del responsable o encargado del tratamiento de datos. Las "autoridades de control interesadas" incluyen aquellas que se ven implicadas por el tratamiento de datos, ya sea porque el responsable o encargado esté ubicado en su Estado miembro sin ser este su establecimiento principal, porque los datos procesados puedan afectar significativamente a los ciudadanos residentes en ese Estado, o porque se haya recibido una reclamación ante esa autoridad según el artículo 4.22. del RGPD. En el contexto de tratamientos de datos transfronterizos, el artículo 56 de la LGPD establece que se aplica un régimen especial de competencia que favorece a la autoridad de control principal, aunque esta debe operar en cooperación con las autoridades de control interesadas según el procedimiento establecido en el artículo 60[84].

No obstante, el artículo 56.2 del RGPD 2016/679, de 27 de abril de 2016, permite también que una autoridad de un Estado miembro actúe dentro del territorio de otro. Como una excepción al procedimiento de coordinación del artículo 60, se establece que cada autoridad de control tiene competencia para tratar una reclamación que le sea presentada o una posible violación del RGPD, siempre que esta se limite a un establecimiento ubicado en su estado o que afecte significativamente a personas en su estado. Esta situación adquiere particular importancia en lo que respecta a los procesamientos de datos que cruzan fronteras dentro del territorio de la Unión Europea, tal como ocurre en el caso Schrems. De acuerdo con el artículo 4.23 del RGPD 2016/679, de 27 de abril de 2016, existen dos categorías de procesamientos transfronterizos:

Aquellos que se realizan en el contexto de las operaciones de una entidad responsable o encargada dentro de la Unión Europea, cuando esta entidad opera en más de un Estado miembro. O los casos en los que el procesamiento de datos se lleva a cabo dentro del

[83] Sentencia del Tribunal de Justicia de la Unión Europea C-230/14, de 1 de octubre de 2015, *Weltimmo,* párr. 57.
[84] De Miguel Asensio, P. A., *Op. cit.* p. 88.

ámbito de un único establecimiento de un responsable o encargado, pero afecta o podría afectar significativamente a individuos en más de un Estado miembro, como se ve en el caso Schrems[85]. Las decisiones tomadas por las autoridades reguladoras pueden ser apeladas a través de recursos administrativos y, ocasionalmente, revisadas por tribunales de lo contencioso-administrativo.

2. TUTELA JUDICIAL CIVIL CONTRA UN RESPONSABLE O ENCARGADO

El artículo 79 del Reglamento General de Protección de Datos establece el derecho a emprender acciones legales contra aquellos responsables o encargados del procesamiento de datos, destacando el derecho de cualquier individuo a ser compensado por daños y perjuicios como consecuencia de violaciones al mencionado Reglamento (artículo 82 del RGPD 2016/679). Una demanda ante una autoridad de control no permite hacer efectivo el derecho a una indemnización[86]. A diferencia de las reclamaciones ante autoridades reguladoras, que no ofrecen reparación directa por daños, este marco legal brinda la posibilidad de reclamar compensaciones a través de los tribunales civiles (salvo que el responsable o encargado sea una administración pública). No obstante, el Reglamento carece de mecanismos de coordinación entre la tutela civil y la supervisión administrativa a pesar de que la propuesta de Directiva sí lo preveía[87]. La propuesta de Directiva permitía que un tribunal encargado de un caso contra un responsable o encargado pudiera pausar el procedimiento si había otro en curso relacionado con la misma medida, decisión o práctica ante el mecanismo de coherencia (artículo 75.3 de la Propuesta).

Aparte del derecho a recibir indemnización, en los tribunales civiles también se pueden iniciar otros tipos de demandas basadas en la violación de las normas del RPD. Estas acciones judiciales civiles pueden ser una alternativa a presentar una reclamación ante una autoridad de control. Por ejemplo, se podría solicitar que se imponga al responsable una restricción o prohibición sobre el tratamiento de datos.[88]. En el ámbito de casos transfronterizos, este Reglamento incluye una normativa específica sobre competencia judicial internacional en casos civiles, permitiendo a los afectados iniciar un

[85] De Miguel Asensio, P. A., *Op. cit.* p. 88.
[86] *Ibid.* p. 92.
[87] *Ibid.* p. 92.
[88] *Ibid.* p. 92.

procedimiento contra los responsables o encargados del tratamiento en cualquier Estado miembro donde estos tengan una sede, o en el país de residencia habitual del demandante según habilita el artículo 79.2 del RGPD[89]. Esto ha constituido un elemento clave en la evolución del Derecho internacional privado de la UE, que tiene por objeto favorecer a los afectados.

VI. CONCLUSIONES

Esta investigación se ha centrado en analizar y estudiar los distintos desafíos actuales y persistentes a los que se enfrenta la regulación de la protección de datos personales en el ámbito de las redes sociales. En TFG he podido comprobar el complejo panorama de la protección de datos donde la rápida evolución de la tecnología, los cambios en las redes sociales y las expectativas de privacidad de los usuarios pueden llegar a colisionan pese a los esfuerzos de las normativas existentes por proteger este derecho. Tras este análisis he podido extraer las siguientes conclusiones.

i. La legislación actual del derecho de protección de datos, regulada por el RGPD y la LOPDGDD ofrecen un marco sólido tanto a nivel comunitario como a nivel nacional. No obstante, en ocasiones estas normativas encuentras desafíos significativos en relación con su aplicación práctica. Los desafíos derivan de la falta de claridad de determinadas disposiciones, la dificultad para adaptarse a tecnologías nuevas y la variabilidad de aplicación por parte de diferentes autoridades nacionales.

ii. En segundo lugar, me gustaría subrayar la importancia de la educación y concienciación de la sociedad. La concienciación sobre los derechos de protección de datos y las prácticas de privacidad es imprescindible para que los usuarios puedan tomar decisiones informadas y prudentes. Se debe potenciar en nuestra sociedad una cultura que eduque sobre la importancia de los derechos digitales, tanto en el ámbito escolar como en el público general. Tanto los Estados miembro como las redes sociales deben realizar un papel activo en educar a sus usuarios

[89] *Ibid.* p. 96.

sobre cómo gestionar los datos personales y sobre qué herramientas están disponibles para proteger su privacidad.

iii. En un contexto en el que los datos personales trascienden fronteras nacionales, y las redes sociales operan a un nivel global, es necesaria una cooperación internacional robusta y coordinada. Se deben crear marcos legales lo más uniformes posibles y facilitar la incorporación de regulaciones transfronterizas efectivas con objeto de lograr una armonización global mínima en la protección de datos a nivel internacional.

iv. Por otro lado, es importante destacar la labor de las autoridades de control del cumplimiento de la regulación de la protección de datos. Tales autoridades de control como por ejemplo la AEPD, deben disponer de los recursos y poderes suficientes para hacer frente a las infracciones del derecho de protección de datos en las redes sociales. Esto implica endurecer las sanciones con objeto de disuadir a las empresas de comportamientos que vulneren el derecho de protección de datos, así como dotar a las autoridades de más herramientas para investigar y actuar rápidamente contra las violaciones, o contenidos ilícitos.

v. Las empresas que operan plataformas de redes sociales deben adoptar un enfoque de privacidad por diseño y por defecto, asegurando que la protección de datos personales esté integrada en todos los aspectos de sus operaciones. Esto incluye la realización de evaluaciones de impacto sobre la protección de datos, la implementación de medidas técnicas avanzadas para la seguridad de los datos y la transparencia en las prácticas de procesamiento de datos. Para ello, es importante la promoción de la transparencia y el consentimiento informado entre los proveedores de SRS. Los proveedores de SRS deben ser más transparentes en relación con cómo se recopilan, utilizan y comparten los datos personales. Del mismo modo, el consentimiento debe ser una elección real y bien informada, en vez de una simple condición impuesta para que los usuarios puedan acceder al servicio básico de la red social. Estas plataformas deben incluir controles fáciles de usar que les permitan gestionar sus preferencias de privacidad de manera efectiva.

En conclusión, esta investigación ha demostrado que, aunque las redes sociales han tenido un impacto positivo en la forma en la que nos comunicamos, también plantean numerosos riesgos, por lo que deben ser abordados mediante una regulación sólida y uniforme, educación, y un compromiso firme hacia la protección de la privacidad y los datos personales por parte de todos los agentes que intervienen en su tratamiento.

VII. BIBLIOGRAFÍA

1. LEGISLACIÓN

Constitución Española de 1978 (BOE núm. 311 29 de diciembre de 1978).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 6 de diciembre de 2018).

Reglamento 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 (DOUE núm. 119, 4 de mayo de 2016).

Informe 425/2006 de la Agencia Española de Protección de Datos de 1 de enero de 2006 (disponible en https://vlex.es/vid/724113085; última consulta 01/04/2024)

Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (BOE núm. 60, 11 de marzo de 2019)

Declaración Universal de los Derechos Humanos adoptada y proclamada por la Resolución de la Asamblea General 217 A (iii) del 10 de diciembre de 1948.

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 (DOCE núm. 281, 23 de noviembre de 1995) (ya derogada).

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE núm. 262, 31 de octubre de 1992) (ya derogada).

Ley N. ª 78-17, de 6 de enero de 1978, sobre el procesamiento de datos informáticos, los archivos y la libertad, Francia (7 de enero de 1978).

2. JURISPRUDENCIA

Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre de 2000.

Sentencia del Tribunal Constitucional núm. 231/1988, de 2 de diciembre, FJ 2.

Sentencia del Tribunal Constitucional núm. 254/1993, de 20 de julio.

Sentencia del Tribunal Supremo Sala 1ª 621/2003, de 27 de junio.

Sentencia del Tribunal de Justicia de la Unión Europea C-362/14, de 6 de octubre de 2015, *Schrems*, (Diario Oficial de la Unión Europea, 6 de octubre de 2015).

Sentencia del Tribunal de Justicia de la Unión Europea C-230/14, de 1 de octubre de 2015, *Weltimmo.*

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), asunto C-131/12, de 13 de mayo de 2014.

Sentencia del Tribunal de Justicia de la Unión Europea C-518/07 de 9 de marzo de 2010 (Diario Oficial de la Unión Europea, 1 de mayo de 2010).

Corte Suprema de EE. UU., caso *Time Inc. v. Hill* de 9 de enero de 1967.

Court of Appeal of California, Fourth District, Melvin v. Reid, 112 Cal. App. 285, de 28 de febrero de 1931.

3. OBRAS DOCTRINALES

Agencia Española de Protección de Datos (disponible en https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar; última consulta 21/03/2024)

Agencia Española de Protección de Datos (disponible en https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/principios; última consulta 21/03/2024)

Agencia Española de Protección de Datos (disponible en https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-recomendaciones-orientadas-evitar-el-acceso; última consulta 25/03/2024)

Arenas Ramiro, M., "El consentimiento en las redes sociales "on line"", Rallo Lombarte, A. (coord.) & Martínez Martínez R. (coord.), *Derechos y Redes sociales*, Civitas: Thomson Reuters, Pamplona, 2010, pp. 117-144.

Barriuso Ruiz, C., "Las redes sociales y la protección de datos hoy", *Anuario de la Facultad de Derecho,* n. 2, 2019, pp. 301-338.

Bajo, J. C., "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el compliance", en López Calvo, José (coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Wolters Kluwer, Madrid, 2018, pp. 278-288.

Beltrán Castellanos, J.M. "Aproximación al régimen jurídico de las redes sociales", *Cuaderno electrónico de estudios jurídicos*, n. 2, 2014, pp. 61-90.

Boyd, D. M., & Ellison, N. B., "Social network sites: Definition, history, and scholarship", *Journal of Computer-Mediated Communication*, vol. 13, n.1, pp.210-230.

Bygrave, L.A., "Privacy and Data Protection in an International Perspective", *Scandinavian studies in law*, n. 56, 2010, pp. 165-200.

Corral Talciani, H., "El derecho al olvido en Internet*"*, *Revista Jurídica Digital UANDES*, vol. 1, n. 1, 2017, pp. 43-66.

De Miguel Asensio, P. A., "Competencia y derecho aplicable en el Reglamento General de Protección de Datos de la Unión Europea", *Revista Española de Derecho Internacional,* vol. 69, n. 1, 2017, pp.75-108.

Debatin, B., Lovejoy, J.P., Horn, A.K., & Hughes, B.N., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", *Journal of Computer-Mediated Communication*, vol. 15, n. 1, 2009, pp. 83-108.

Denham, E. (2009). Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques. Oficina del Comisionado de Privacidad de Canadá (disponible en https://publications.gc.ca/collections/collection_2010/privcom/IP54-31-2009-fra.pdf; última consulta 20/03/2024)

Durán Arroyo, A., "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito", *Revista Jurídica de la Universidad Autónoma de Madrid*, n. 37, 2018, pp. 415-440.

Fraguela, N., "El número de usuarios de internet en el mundo crece un 1,8% y alcanza los 5.350 millones (2024)", *Marketing for eCommerce*, 31 de enero de 2024 (disponible en https://marketing4ecommerce.net/usuarios-de-internet-mundo/; última consulta 28/03/2024).

Gil González E., *Big data, privacidad y protección de datos*, Boletín Oficial del Estado, Madrid, 2016.

Hernández Serrano, M. J., Renés-Arellano, P., Campos Ortuño, R. A., & González-Larrea, B., "Privacidad en redes sociales: análisis de los riesgos de auto-representación digital de adolescentes españoles", *Revista Latina de Comunicación Social*, n. 79, 2021, pp. 133-154.

López Aguilar, J. F., "Por fin una ley europea de protección de datos (I)", Huffington Post, 24 de octubre de 2013 (disponible en https://www.huffingtonpost.es/juan-fernando-lopez-aguilar/ley-europea-de-proteccion-de-datos_b_4148971.html; última consulta 13/03/2024)

Martínez de Pisón, J. M., "La configuración constitucional del derecho a la intimidad", *Revista de Filosofía del Derecho y derechos humanos*, vol. 2, n. 3, 1994, pp. 313-340.

Martínez de Pisón, J., "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional", *Anuario de filosofía del derecho*, n. 32, 2016, pp. 409-430.

Minero Alejandre, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario Jurídico y Económico Escurialense,* n. 50, 2017, pp. 13-58.

Moreno Boadilla, A., "Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital". *Estudios constitucionales: Revista del Centro de Estudios Constitucionales*, vol.18, n. 2, 2020, pp. 121-150.

O'Callaghan Muñoz, X., *Libertad de expresión y sus límites: honor, intimidad e imagen*, Edersa, Madrid, 1991.

INTECO (Instituto Nacional de Tecnologías de la comunicación, "Redes Sociales, Menores de Edad y privacidad en la Red", *Observatorio de Seguridad de la Información*, 2007.

Ortiz López, P., "Redes sociales", Rallo Lombarte, A. (coord.) & Martínez Martínez R. (coord.), *Derechos y Redes sociales*, Civitas: Thomson Reuters, Pamplona, 2010, pp. 23-36.

Perelló, E. M., "Impacto de las redes sociales en el derecho a la protección de datos personales", *Anuario Facultad de Derecho, Universidad de Alcalá*, 2009, n. 2, 2019, pp. 107-129.

Piñar Mañas, J.L., *Seguridad, transparencia y protección de datos*, Fundaciones Alternativas, 2009.

Piñar Mañas, J. L., "Protección de datos personales y fundaciones", *Anuario de derecho de fundaciones*, n. 1, 2009.

Polo Roca, A. "Datos, datos, datos: El dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos", *Estudios de Deusto: revista de Derecho Público*, vol. 69, n. 1, 2021, Págs. 165-194.

Real Academia Española: *Diccionario de la lengua española*, 23.ª ed. (consultado en https://dle.rae.es/red?m=form#GExglxC; última consulta 28/03/2024).

Sancho López, M. & Plaza Penadés, J., *La protección de datos en el Reino Unido: evolución del right to privacy y escenarios post-Brexit*, Thomson Reuters Aranzadi, 2019.

Warren, S.D. & Brandeis, L.D., "The Right to Privacy", *Harvard Law Review*, vol. 4, n. 5, 1890, pp. 193-220.