FACULTAD DE DERECHO

DERECHO A LA INTIMIDAD EN LA ERA DIGITAL

Protección de datos y privacidad

Autor: Jaime de la Vega Carretero
2024-2025, 5ºE-3 Analytics
Derecho Civil
Tutor: Blanca Gómez Bengoechea

Madrid
Marzo 2025

RESUMEN

Este trabajo analiza los desafíos legales y éticos que enfrenta la protección de la intimidad en un mundo digital cada vez más avanzado. Se examinan las leyes actuales tanto en España como en Europa, y se reflexiona sobre su efectividad para enfrentar los riesgos que se derivan del uso de internet y de las redes sociales. A lo largo del análisis, se destacan las limitaciones de la normativa vigente, en particular en el tratamiento de *cookies* y datos personales. Se propone mejorar la educación digital, ante el desconocimiento por parte de los cibernautas de los riesgos asociados a una mala gestión de la privacidad de sus datos. Además, se subraya la necesidad de actualizar las leyes para proteger mejor la intimidad de las personas en un entorno tecnológico en constante cambio.

Palabras clave: Protección de la intimidad, privacidad, *cookies*, internet, privacidad en redes sociales, regulación de datos personales, GDPR.

ABSTRACT

This paper analyzes the legal and ethical challenges in protecting privacy in an increasingly digital world. It examines current laws in Spain and Europe and reflects on their effectiveness in addressing the risks posed by the internet and social media. Throughout the analysis, the limitations of existing regulations are highlighted, especially regarding cookies and personal data processing. The paper suggests improving digital education, as many users are unaware of the risks associated with poor privacy management. It also emphasizes the need to update laws to better protect individuals' privacy in an ever-evolving technological environment.

Key words: Privacy protection, digital privacy, cookies, internet, social media privacy, personal data regulation, GDPR.

ÍNDICE

CAPITULO I. INTRODUCCIÓN

Imaginemos que estamos navegando por Internet. Accedemos a una página que no hemos visitado nunca, y nos aparece una notificación de "uso de *cookies*[1]", con tres opciones: aceptar todas, configurar o rechazar todas[2]. En ese instante, por nuestra mente pasan en menos de un segundo mil preguntas que nos hacen cuestionarnos qué datos de nuestra vida privada estaremos compartiendo exactamente y qué uso tiene para la plataforma la recepción de dichos datos. Lo fácil, y por lo que la mayoría de los ciudadanos optamos, es por aceptar todas esas *cookies*, entre otras razones, porque por lo general esa opción va acompañada de un color que resalta más sobre el resto de las opciones y es el camino más rápido de acceso a la totalidad de la página web. Detrás de esta simple acción, se comparte una gran cantidad de información privada con los proveedores de servicios sin ser muchos de los usuarios conscientes de los riesgos que esto conlleva. Este es uno de los muchos problemas que surgen en la actualidad, conforme avanzan las nuevas tecnologías.

El objetivo de este trabajo es analizar los problemas legales relacionados con la protección de la intimidad en un mundo cada vez más digital. En concreto, se busca ver si las leyes actuales, tanto en España como en Europa, son suficientes para enfrentar los desafíos que presentan Internet y las redes sociales en cuanto a la gestión de nuestros datos personales. También se analizarán las limitaciones de estas leyes y la necesidad de mejorar la protección de la privacidad de una manera más efectiva.

A través de este análisis, se pretende identificar los riesgos que existen en el mundo digital y reflexionar sobre cómo mejorar las leyes actuales para proteger mejor nuestra intimidad. En particular, en el apartado de conclusiones se destaca la necesidad de promover más educación digital, considerando que gran parte de la población no conoce los riesgos de una mala gestión de su privacidad. Además, se hablará sobre la importancia de actualizar

[1] Según la Real Academia de la Lengua Española (RAE), *cookie* es una palabra inglesa que significa *pequeño archivo de datos que queda instalado en el disco duro de un ordenador cuando este accede a una página web.*

[2] A modo de ejemplo, cuando visitamos la página web del Real Madrid aparece el siguiente mensaje: "*Real Madrid usa cookies propias y de terceros para garantizar la funcionalidad de la web (cookies necesarias y de funcionalidad), para fines analíticos (cookies de rendimiento o analíticas) y para mostrarle publicidad relacionada con sus preferencias a partir de sus hábitos de navegación (cookies dirigidas o de publicidad). Puede aceptar todas las cookies, seleccionar aquellas que desee en "Configurar" o rechazarlas todas."*

las leyes para que sigan siendo efectivas frente a los rápidos avances tecnológicos, asegurando que los derechos de las personas se respeten completamente.

Para comprender el origen de este problema, es necesario que nos remontemos unos centenares de años atrás, concretamente al Siglo XVIII en Inglaterra, donde tuvo lugar la Revolución Industrial. Este fenómeno, que posteriormente se propagará a los países de la Europa Continental, conforma un conjunto de transformaciones económicas, políticas, sociales, etc. unidas bajo un común denominador: la mecanización de la industria. Así, a lo largo de la historia surgen tres fenómenos evolutivos: la primera revolución industrial, marcada por el uso de las máquinas a vapor; la segunda, que introduce la electricidad; y la tercera, impulsada por la informática, la automatización y las telecomunicaciones.

En la actualidad, se dice que se está construyendo una cuarta revolución industrial también conocida por el nombre de digitalización, diferenciada de la tercera por su velocidad, alcance e impacto en los sistemas. Y es que tenemos la posibilidad de utilizar un dispositivo móvil con una potencia sin precedentes en el procesamiento, capacidad de almacenamiento y acceso al conocimiento sin límites (Schwab, 2020). Estas posibilidades se multiplicarán debido a los grandes avances tecnológicos en campos como el Big Data, la Inteligencia Artificial (en adelante, IA), el Cloud Computing o el Internet de las Cosas.

Estas tecnologías han transformado nuestra vida cotidiana, aportando mejoras significativas en múltiples áreas. Por ejemplo, el Big Data permite predecir terremotos y accidentes, mientras que la Inteligencia Artificial (IA) ayuda a diagnosticar enfermedades previamente indetectables o a optimizar la logística en catástrofes humanitarias. No obstante, el uso de estas tecnologías implica el tratamiento masivo de datos personales, lo que intensifica las preocupaciones sobre su impacto en la privacidad.

Sin embargo, esta revolución no solo comprende aspectos positivos, sino que también ha tenido consecuencias perjudiciales: desde influir en el voto ciudadano hasta introducir *malware*[3] para obtener y revelar contenido confidencial con ánimo de lucro. Los riesgos son significativos.

[3] En palabras de González Herrera (2023), un *malware* es un programa o código diseñado para infectar, dañar o acceder a sistemas informáticos.

En la era digital, las nuevas formas de flujo de datos permiten monitorear constantemente a las personas, tanto al consumir productos, servicios o contenidos, como al comunicarse e interactuar entre ellos. Esto ha generado diversas preocupaciones que suelen enmarcarse en los paradigmas relacionados con la privacidad y la protección de datos.

Debido a los riesgos asociados al avance de estas nuevas tecnologías, que tienen que ver principalmente con la seguridad y la protección de nuestros datos personales y nuestra privacidad, surgen normativas nacionales, como la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), y europeas como el Reglamento Europeo de Protección de Datos (en adelante, GDPR, por sus siglas en inglés, Global Data Protection Regulation) que lo que pretenden precisamente es frenar estas amenazas y que serán objeto de análisis en este trabajo.

En este contexto, el derecho a la intimidad emerge como un pilar fundamental, no solo para garantizar la dignidad individual, sino también para equilibrar las tensiones entre el desarrollo tecnológico y la protección de los derechos humanos.

CAPITULO II. MARCO CONCEPTUAL DEL DERECHO A LA INTIMIDAD

Previo a analizar la normativa vigente que garantiza la protección del derecho a la intimidad es necesario conocer qué es lo que se entiende por "intimidad" no sólo en nuestro país, sino también en el contexto estadounidense y europeo, del que como veremos, emana gran parte de la jurisprudencia sobre esta cuestión. Por ello, en este capítulo analizaremos el concepto, origen y modalidades del derecho a la intimidad.

3.1. Conceptualización

La Constitución Española, como norma suprema, reconoce en su artículo 18.1 el derecho a la intimidad personal y familiar. Asimismo, la Ley Orgánica 1/1982, de 5 de mayo, regula la protección civil de este derecho, junto con el derecho al honor y a la propia imagen. A este respecto destacamos la falta de una definición constitucional de la intimidad, pues, aunque se garantice el derecho a la intimidad personal y familiar en la Constitución Española, ésta no ofrece una definición del concepto ni lo diferencia de otros términos del mismo campo semántico, como "vida privada", "ámbito íntimo" o "privacidad" (Maestre, 2019). La jurisprudencia constitucional (STC 202/1999 de 8 de noviembre, STC 254/1993 de 18 de agosto, STC 119/2001 de 24 de mayo…) habla asimismo de vida privada sin llegar a diferenciar cual es el ámbito propio de cada derecho.

En tanto que surgen nuevos ámbitos de protección, relacionados con el avance de las tecnologías, existe un amplio debate doctrinal acerca de la distinción entre intimidad y privacidad. Respecto a la definición dada por la Real Academia Española, la privacidad es el "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*" mientras que la intimidad es comprendida como la "*zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*". A este respecto, el Tribunal Constitucional en la Sentencia 156/2001 de 2 de julio determinó que, si bien el derecho a

la intimidad se trata de un derecho fundamental autónomo, es frecuente que un mismo supuesto de hecho incida en más de uno de los derechos reconocidos en el art. 18 CE[4] .

Para comprender el concepto de derecho a la intimidad es necesario previamente entender la delimitación existente entre el espacio público y el espacio privado, explicada de manera muy clara a través de la "teoría de las esferas" (*Sphärentheorie*), desarrollada en la doctrina y jurisprudencia alemanas, concretamente por el jurista alemán Heinrich Hubmann (1967). Esta teoría ha sido adoptada y desarrollada también por la doctrina española, lo que subraya su importancia en la conceptualización del derecho a la intimidad (Roca, 2022).

La teoría de las esferas clasifica el ámbito de la intimidad en tres niveles, y según nos encontremos en un nivel u otro, mereceremos una menor o mayor protección. La *intimsphäre* (esfera íntima), representa lo más personal y secreto del individuo, como sus opiniones, decisiones y acciones privadas. Entrarían dentro de esta esfera, las conversaciones confidenciales con un terapeuta o los diarios personales. Este núcleo corresponde al círculo más cercano y protegido frente a terceros y fue definido por Pérez Luño como esfera de lo secreto. La *privatsphäre* (esfera privada), incluye la vida privada y familiar del individuo que también requiere protección frente a injerencias externas, aunque en un ámbito algo más amplio. Por ejemplo, las interacciones familiares en el hogar, como las decisiones sobre la educación de los hijos o la celebración de un evento privado. Por último, la *individualsphäre* (o esfera individual), que corresponde a los aspectos de la personalidad que están más expuestos, como el honor y la imagen personal, que reflejan al individuo antes de entrar en la esfera pública. Ejemplos de esta última esfera serían la forma en que una persona se presenta en redes sociales o en actos públicos, ya que, aunque visible, aún necesita cierto grado de protección frente al abuso o la difamación. Así, la esfera de mayor protección jurídica será la íntima y la de menos la individual (Roca, 2022).

Actualmente el Tribunal Constitucional Federal Alemán sigue desarrollando esta teoría para delimitar qué es lo que queda dentro de la esfera privada y qué queda dentro de la

[4] FJ 3º: "*El carácter autónomo de los derechos del art. 18.1 CE supone que ninguno de ellos tiene respecto de los demás la consideración de derecho genérico que pueda subsumirse en los otros derechos fundamentales que prevé este precepto constitucional."*

esfera pública. A pesar de ello, la doctrina alemana ha reconocido que "*no existe plena unanimidad en la doctrina sobre la concreta clasificación y tipología de tales esferas*", pero hay una posición generalizada de cuáles son las dos principales esferas: la esfera íntima (*Intimsphäre*) y la esfera privada (*Privatsphäre*) (Roca, 2022).

Así, en derecho alemán se utiliza el término derecho a la intimidad para referirse al *Privatsphäre*, haciéndose uso también de la acepción, "derecho a la vida privada".

En esta línea, resulta importante clarificar que, en la tradición estadounidense-anglosajona, para hacer referencia al "derecho a la intimidad" se hace uso de la acepción "*right to privacy*" o "derecho a la privacidad" (Roca, 2022).

La aplicación de la teoría de las esferas en España tiene su origen en el más alto órgano jurídico. En sus primeras sentencias, el Tribunal Constitucional se refería a esas *Sphärens* para definir qué supuestos entrarían dentro de la esfera constitucionalmente protegida y cuáles no[5]. Este último caso se daría respecto de aquellos supuestos que se subsumirían dentro de la esfera pública, no protegida jurídicamente.

A este respecto, la STS 44/1989 de 20 de febrero, definió que "*la esfera privada (...) incluye aquel sector de circunstancias que, sin ser secretas, ni de carácter íntimo, merecen, sin embargo, el respeto de todos, por ser necesarias para garantizar el normal desenvolvimiento y la tranquilidad de los titulares particulares, sin que, en modo alguno, y fuera de los casos permitidos por la ley o las mismas circunstancias, se admitan intromisiones extrañas. El derecho que cada uno tiene a que se respete su esfera privada garantiza la inviolabilidad de su vida particular, y merece también protección la personalidad frente a publicación indebida de hechos particulares o familiares, aunque no sean secretos, prescindiendo de si son ciertos o inciertos*".

5 Por ejemplo, STC 231/1988, de 2 de diciembre: "el derecho a la intimidad personal y familiar se extiende, *no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen",* FJ 4*; "Las escenas se difundieron en los programas informativos de Televisión Española, lo que conduce a plantearse si esas imágenes no constituirán, así, escenas que pertenecen al conocimiento público, fuera por tanto de la esfera de la intimidad",* FJ 9.

De acuerdo con la doctrina, distinguimos, al igual que la jurisprudencia, una esfera denominada "intimidad" y otra conocida como "vida privada". Por un lado, la intimidad se refiere, en lo personal y familiar, a la voluntad de no dar a conocer o difundir públicamente información sobre los pensamientos, ideologías, creencias, sentimientos, emociones, sensaciones, proyectos vitales, relaciones personales… Por otro, la vida privada refiere a aquellos aspectos de la vida de un individuo que se pueden asociar a su vida social (en concreto, la esfera comercial, laboral, económica y profesional) [6]. Por ello, según Gutiérrez-David (2014), la vida privada participa de la intimidad, pero no se identifica con ella. A este respecto, existen autores que defienden que la intimidad está relacionada con el "principio de libre desarrollo de la personalidad", implicando un ámbito propio y reservado frente a la acción y conocimiento de los demás (Martínez de Aguirre, 2024).

2.2. Origen del derecho a la Intimidad

Delimitado el concepto de derecho a la intimidad, procedemos al análisis de su origen para concluir en qué momento y en qué contexto fue reconocido este derecho como tal.

2.2.1. Origen en EE.UU.

El origen del concepto jurídico del derecho a la privacidad se remonta al año 1873 en Estados Unidos, cuando el juez Thomas McIntyre Cooley introdujo el concepto en su obra *"The Elements of Torts"*. En este texto, Cooley describió la privacidad como *"the right to be let alone*[7]*",* que en español se traduce como "el derecho a estar solo" o "el derecho a que se respete la soledad", sentando así las bases de esta noción jurídica.

[6] Afirmación apoyada en la STC 12/2012, de 30 de enero: "*El Tribunal Europeo de Derechos Humanos ha señalado que sería muy restrictivo limitar la noción de vida privada protegida por el art. 8.1 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales a un «círculo íntimo» en el que el individuo puede conducir su vida personal a su manera y excluir plenamente el mundo exterior no incluido en este círculo. No puede desconocerse que también en otros ámbitos, y en particular en el relacionado con el trabajo o la profesión, se desarrollan relaciones interpersonales, vínculos o actuaciones que pueden constituir manifestación de la vida privada."*

[7] El concepto del derecho a no ser molestado, durante esa época, no solo se entendía en términos de una protección negativa, sino que también incluía un componente positivo: la prohibición de difundir fotografías de una persona sin su autorización, considerando que la fotografía representaba un avance mecánico que invadía la privacidad individual. Estos principios fueron reconocidos judicialmente, como explica Elvira López Díaz, quien señala que, tres años después de la publicación de un conocido artículo,

El derecho a la privacidad está implícito en la Constitución de los Estados Unidos y fue inicialmente reconocido por la "*Supreme Court of the United States*". Aunque ni en la Constitución de 1787 ni en sus enmiendas se menciona explícitamente el concepto de "*right to privacy"*, este derecho ha sido desarrollado a través de la jurisprudencia y se deriva de otros derechos ya establecidos. Por ejemplo, la Primera Enmienda protege el derecho de asociación, mientras que la Cuarta Enmienda salvaguarda frente a registros personales y domiciliarios. Asimismo, la Decimocuarta Enmienda abarca aspectos relacionados con la privacidad de la información, conocida como *information privacy* (Roca, 2022).

Entre las primeras teorías sobre el derecho a la privacidad destaca la obra de Warren y Brandeis, publicada en 1890 bajo el título "The Right to Privacy". Este trabajo se considera un punto de partida fundamental para el desarrollo del concepto de privacidad en los Estados Unidos, y plantea la privacidad como una respuesta necesaria frente a los avances tecnológicos de la época. Con esta obra, ambos autores pretendían establecer límites jurídicos que pudieran impedir intromisiones de la prensa en la vida privada de las personas (Roca, 2022).

Durante los cincuenta años posteriores a la publicación de la obra de Warren y Brandeis, se debatieron numerosos casos relacionados con la invasión de la vida privada a través de medios como la prensa, la fotografía, la radio y la televisión. A raíz de estas discusiones, el derecho a la privacidad evolucionó hasta convertirse en un derecho autónomo, aunque su protección se encontraba integrada en la tutela de otros derechos. Además, de este derecho surgieron otros derechos derivados, como el derecho al honor, a la propia imagen, la inviolabilidad del domicilio y las comunicaciones, así como la protección de los datos personales (Roca, 2022).

---

un tribunal empleó por primera vez la idea propuesta por los abogados Warren y Brandeis. Este caso, conocido como *Marks v. Joffa* y resuelto por el Tribunal de Nueva York, involucró a un actor y estudiante de leyes que vio su retrato publicado sin consentimiento en un periódico vinculado a un concurso de popularidad, al que él se oponía. La sentencia falló a favor del demandante, declarando su derecho a que su imagen no fuese utilizada sin su consentimiento, fundamentado en que ninguna institución o medio de comunicación podía usar el nombre o la fotografía de una persona sin su aprobación previa. *Cfr*. López Díaz, E., *El derecho al honor y el derecho a la intimidad*, Ed. Dykinson, Madrid, 1996, p. 175.

En Estados Unidos, el derecho a la privacidad se desarrolla principalmente dentro del derecho común o "*Common Law*", cómo hemos mencionado, sin un reconocimiento explícito en la Constitución. Según este marco, cualquier persona que invada deliberadamente, ya sea de forma física o mediante otros medios, el aislamiento o los asuntos privados de otra, puede ser considerada responsable por invasión de la intimidad conforme a las leyes de responsabilidad civil (*Torts Law)*.

Este principio, aplicado originalmente a espacios privados, se extiende también a los archivos informáticos almacenados en lugares privados. De manera similar, la jurisprudencia aplicada a las escuchas telefónicas y la interceptación del correo personal respalda esta interpretación amplia. Por tanto, en el contexto de Internet, cualquier intrusión ofensiva puede implicar la obligación de compensar a la víctima por la vulneración de su intimidad (Porras, 2016). Esta interpretación se enmarca principalmente en jurisprudencia de EEUU, donde la protección de la privacidad se ha ampliado a diversos ámbitos de la vida personal.

Tras consolidarse en la jurisprudencia estadounidense, el derecho a la privacidad fue posteriormente reconocido en el ámbito internacional con la Declaración Universal de los Derechos Humanos (DUDH) de 1948, que buscó proteger el espacio íntimo de las personas frente a la intromisión de terceros y garantizar el derecho de cada individuo a decidir quién puede o no participar en su vida privada (Soler, 2019).

2.2.2. Origen en Europa

El camino que se siguió en Europa fue distinto al de EE. UU, existiendo en un inicio únicamente formulaciones filosóficas y doctrinales sobre el derecho a la intimidad. Es decir, no aparece en textos constitucionales hasta pasada la Segunda Guerra Mundial (Porras, 2016). Como ya vimos en el capítulo II apartado 1, la teoría alemana de las esferas supone un primer acercamiento a este derecho. La intimidad, el espacio personal, y la vida privada se presentan como el límite entre lo público y lo privado, entre aquello que resulta confidencial y lo que puede mostrarse (Soler, 2019).

Inicialmente, este derecho, que surge como preocupación por la protección de la esfera privada en reacción a las constates intromisiones de la prensa en el ámbito personal y

familiar, fue conceptualizado como parte de los derechos de la personalidad. Así se dio cabida a su reconocimiento en el Convenio Europeo de los Derechos Humanos, concretamente en su artículo 8, que reza, *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"* (Soler, 2019).

En materia constitucional, el primer texto europeo que incluyó de forma expresa el derecho a la intimidad fue la Constitución Portuguesa de 1976, en su artículo 26.1. Posteriormente, la Constitución Española de 1978 lo recogió en su artículo 18, consolidándolo como un derecho fundamental (Porras, 2016).

En Alemania, el reconocimiento del derecho a la intimidad se basa en la ya comentada "teoría de las esferas" (*Sphärentheorie*) y en la jurisprudencia del Tribunal Constitucional Federal. Como hemos comentado previamente, esta teoría establece que el derecho a la privacidad no solo se refiere al espacio físico, sino también a las esferas personales y familiares, y más recientemente a los datos personales. La interpretación alemana ha influido en gran medida en el desarrollo de la legislación de privacidad en toda Europa, especialmente en lo que respecta a la protección de los datos personales (BVerfG, 1999).

Por otro lado, en Francia, la protección del derecho a la intimidad se abordó principalmente a través de la doctrina y la jurisprudencia antes de que se integrara de manera formal en la legislación. La ley de 1970 sobre el derecho de imagen y la Ley de Protección de la Privacidad de 1978 se centraron en proteger a los individuos de intromisiones ilegítimas en su vida privada (Tachon, 2021). Esta preocupación por la privacidad también se extendió a la protección de los datos personales, lo que llevó a la creación de la Comisión Nacional de Informática y Libertades para garantizar el cumplimiento de los derechos fundamentales en el contexto digital.

Con respecto al derecho a la protección de datos, existía a finales del S.XX una clara disparidad entre las distintas legislaciones europeas que abogaban por su protección, por lo que se vio necesario crear una legislación que armonizara las leyes nacionales sobre protección de datos. Esta regulación armonizada se fundó con la Directiva 95/46/CE, 1995 O.J. (L281) 31 sobre protección de datos que establece un sistema aplicable a cualquier tipo de base de datos que contiene información personal. De ella destacamos su artículo 6, según el cual los datos recabados con unos fines determinados no deben

utilizarse para otros fines (Manny, 2003). La Directiva fue la base de la legislación de protección de datos en Europa hasta la entrada en vigor del Reglamento General de Protección de Datos (GDPR) en 2018.

2.2.3. Origen en España

Antes de ser reconocido como un derecho fundamental en la Constitución Española de 1978, el derecho a la intimidad en España estuvo sujeto a diversas formulaciones doctrinales y legislativas en el ámbito de la protección de los derechos personales. La idea de la protección de la intimidad se fue desarrollando en España, principalmente, a través de la legislación sobre el derecho al honor, la propia imagen y la dignidad, que fueron reconocidos a lo largo del siglo XX (Porras, 2016).

La Ley 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, fue un avance importante en el reconocimiento de este derecho, ya que estableció de forma clara que la invasión de la vida privada era una intromisión ilegítima. Sin embargo, el derecho a la intimidad ya había sido recogido de manera previa en la Constitución Española (CE) de 1978, aunque sin entrar en el detalle que se lograría con la Ley de 1982 (Porras, 2016). Este reconocimiento en la Constitución surge por la necesidad de adaptar los derechos fundamentales a los avances tecnológicos y sociales, lo que resultó decisivo para la incorporación de una regulación que abordará los riesgos de la sociedad actual y tecnológica.

En concreto el artículo 18 CE recoge el derecho a la intimidad en su primer punto, mientras que en el 18.4[8] se hace una mención a la informática y el uso de tecnologías para garantizar la protección de la intimidad personal y familiar. Este precepto responde a la creciente preocupación por los avances tecnológicos y la capacidad de la informática para incidir en la privacidad de los ciudadanos (Pérez Luño, 1981).

La inclusión de este apartado en la CE responde a la preocupación por las posibles amenazas que el desarrollo tecnológico podría representar para la privacidad y las

[8] Artículo 18.4 CE: "*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.*"

libertades individuales y a los riesgos asociados al uso masivo de datos personales. Como bien apuntaba Rallo (2017), "*la meritoria —por expresa y vanguardista— referencia a la informática en el texto constitucional de 1978 constituyó un innegable aldabonazo para otorgar trascendencia constitucional a la necesaria protección del individuo frente a los riesgos que sobre él —y, particularmente, sobre el disfrute de algunos de sus derechos fundamentales— cernían los avances tecnológicos ligados a la incipiente y primaria computarización*".

Asimismo, Pérez Luño, en su publicación *Informática y libertad. Comentario al artículo 18.4 de la Constitución Española (1981)*, destaca que este precepto constitucional aborda la relación entre la informática y los derechos fundamentales, resaltando la necesidad de una regulación legal que limite el uso de la tecnología para proteger la intimidad y otros derechos de los ciudadanos.

Aunque el artículo 18.4 CE se centra en la protección del honor y la intimidad personal y familiar, su alcance es más amplio, ya que busca garantizar el pleno ejercicio de los derechos de los ciudadanos en el contexto de una sociedad informatizada. Pérez Luño sugiere que este enfoque puede considerarse fragmentario e individualista, dado que no aborda de manera completa las cuestiones de índole personal y social que surgen en la intersección entre intimidad e informática (1981).

Además, el citado jurista menciona que tanto el artículo 18.4 como el artículo 105.b)[9] de la Constitución remiten a una ley orgánica para delimitar su alcance y desarrollo, lo que implica la necesidad de una legislación específica que establezca las garantías y límites en el uso de la informática para proteger los derechos fundamentales de los ciudadanos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales, Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, principalmente).

[9] Artículo 105 CE: "*La ley regulará: b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas."*

2.3. Modalidades del derecho a la intimidad

La teoría de las esferas (*Spharentheorie*) de Heinrich Hubmann, ya expuesta en el epígrafe 2.1, proporciona un marco conceptual para entender las modalidades del derecho a la intimidad que son reconocidas por la doctrina (Roca, 2022). Según esta teoría, la esfera íntima corresponde al núcleo más reservado del individuo (el ámbito de lo secreto) donde se sitúan aspectos muy personales como la vida sexual y las decisiones privadas más trascendentales (lo que cierta doctrina denomina intimidad decisional, ligada a la autonomía personal) (Beca, 2011). La esfera privada constituye el segundo círculo, más amplio, que abarca la vida personal familiar y doméstica que el individuo mantiene reservada del escrutinio público. Por su parte, la esfera individual o social cubre los aspectos de la persona que se expresan en sociedad (como la imagen y el honor) y representa la zona límite con la vida pública, con un nivel de protección menor en materia de intimidad (salvo frente a intromisiones graves, como la difusión de información falsa y lesiva) (Roca, 2022).

De esta forma, las categorías de Hubmann permiten ubicar cada manifestación específica de la intimidad (sexual, familiar, decisional, etc.) en la esfera correspondiente de la vida personal, clarificando su grado de tutela según la naturaleza del ámbito involucrado. En línea con este enfoque, autores como Talciani (2000) han subrayado que el derecho a la intimidad se proyecta en distintos ámbitos personales, familiares y decisionales, cuyo contenido queda delimitado, precisamente, por ese círculo de reserva frente a injerencias del exterior.

Otra de las manifestaciones de derecho a la intimidad más importantes es el derecho a la privacidad de la información (*information privacy*), ya mencionado en el Capítulo II Apartado 2.1. A este respecto, uno de los casos más relevantes según resalta Roca (2022) es el caso Whalen v. Roe (1977), en el que el Estado de Nueva York elaboró una ley que obligaba a los médicos a informar al Departamento de Estado de Nueva York sobre datos del paciente y del propio sanitario, en todos aquellos casos en los que se otorgase una receta médica. Principalmente, tenían el deber de informar sobre nombre y apellidos del médico, nombre, apellidos y edad del paciente, y fármaco recetado y dosis. Con ello pretendían reducir la prescripción excesiva y combatir el mercado ilegal. El recurso fue interpuesto por Roe (paciente) y desestimado por la corte, pues concluyó que la

recopilación y almacenamiento de la información no representaba una violación de la privacidad, pues el riesgo de una divulgación accidental de la privacidad fuera insuficiente para justificar una invasión de la privacidad, y además existía un interés del Estado en controlar la prescripción excesiva de medicamentos.

De este caso se reconoció la importancia de proteger el interés en evitar la divulgación de datos personales, interés que, aunque forma parte del concepto de privacidad protegido constitucionalmente en Estados Unidos, no fue suficiente para que la Corte declarara una vulneración del derecho en este caso concreto. Lo relevante del caso es que la Corte Suprema mencionó, por primera vez, el derecho a la privacidad de la información en sus sentencias, a pesar de que este derecho aún no estaba formalmente reconocido como tal. Esto se debe a que, en ese momento, no existía un marco legal o constitucional claro que protegiera explícitamente el derecho a la privacidad de la información, lo que generaba una jurisprudencia confusa e inconsistente en este ámbito (Roca, 2022).

La privacidad de la información es, por tanto, el control que tenemos sobre la información sobre nosotros mismos (Fried, 1968 citado en Roca, 2022), la facultad del individuo de decidir cuándo y dentro de qué límites procede revelar situaciones referentes a la vida de uno mismo. También se le conoce como derecho a la autodeterminación de la información o derecho a la protección de datos personales, acuñada por primera vez como tal por el Tribunal Constitucional Federal Alemán en su Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo. Se trata de un derecho que surge para dar respaldo a la posibilidad de un tratamiento masivo de datos.

En palabras de Murillo de la Cueva (2013), "*a partir de los datos obtenidos cabe extraer, relacionando unos con otros, ulteriores perfiles personales utilizables para los más diversos fines, lícitos o ilícitos, tanto por los poderes público como por agentes privados*". Para proteger la utilización que se haga de esa gran cantidad de datos personales informatizados surge la necesidad de crear mecanismos de protección que serán objeto de estudio a continuación. "*Tampoco el Estado se vislumbra como única posible solución a las problemáticas que plantea la sociedad digital, pero de modo parecido al Derecho, es actor necesario, es parte de la solución […] pero con carácter internacional o globalizado, de lo contrario decae en su eficacia*" (Rebollo, 2020).

El derecho a la autodeterminación de la información es un nuevo derecho que no está previsto expresamente en nuestro ordenamiento jurídico. Sin embargo, ha sido extraído de nuestra Constitución (Art. 18.4, ya mencionado en el Capítulo II Apartado 2.3.), y subsumible dentro del supuesto que el artículo 10.2 CE, que plantea: "*Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las materias ratificados por España.*"

En concreto, el TC, en sus Sentencias 290/2000 y 292/2000[10] de 30 de noviembre, ha utilizado el Convenio nº108 del Consejo de Europa, de 28 de enero de 1981, sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, para llegar a la afirmación del derecho fundamental a la protección de datos personales.

10 STC 292/2000 de 30 de noviembre, en su FJ 7º, establece que*, "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".*

CAPITULO III. MARCO NORMATIVO DEL DERECHO A LA INTIMIDAD

Este capítulo comprenderá el análisis normativo del derecho a la privacidad, haciendo especial énfasis en la legislación aplicable a las cookies (como el GDPR, y el deber de información y consentimiento del usuario). Esto nos servirá para, posteriormente, desarrollar las implicaciones prácticas del uso de cookies en internet y en las redes sociales, por ejemplo, en la publicidad digital. De este modo, la regulación de cookies introducida en el Capítulo III se retoma en el Capítulo IV como base para su análisis práctico, lo que permite diferenciar claramente entre el marco legal y su aplicación práctica.

3.1. Protección de datos en Europa

En la sociedad actual resulta fundamental proteger a las personas de cualquier uso indebido o manipulación no autorizada de sus datos personales, especialmente cuando estos son gestionados mediante sistemas informáticos. La tecnología actual ha creado nuevas amenazas para la libertad y la dignidad de los ciudadanos, que ya no dependen del control físico sobre ellos, sino de su información personal. Por eso, el derecho a la protección de datos se ha vuelto tan importante, ya que busca garantizar la privacidad y la seguridad frente al poder creciente de la tecnología.

El Convenio 108 del Consejo de Europa, firmado el 28 de enero de 1981 y ratificado por España en 1984, buscó unificar las leyes europeas para proteger los datos personales tratados mediante sistemas informatizados. Este acuerdo, conocido como el Convenio de Estrasburgo, marcó un avance importante al garantizar normas comunes sobre el uso de datos en Europa y al fortalecer la protección de los derechos de las personas frente al uso de la informática. Además, en España, este convenio se integró en el ordenamiento jurídico, sirviendo como referencia para interpretar los derechos relacionados con la privacidad y la tecnología.

Por otro lado, analizaremos también en este capítulo el GDPR, como norma más reciente en materia de privacidad de datos, emanada de una gran cantidad de directivas y

regulaciones europeas. En la figura 1 se pueden observar las normativas previas de las cuales surge el GDPR, destacándose entre ellas la Directiva 95/46/EC sobre la protección de datos, la Directiva 2002/58/EC sobre privacidad electrónica, y el "Cookie Amendment" de 2009 (Directiva 2009/136/EC), que introdujeron normas clave para garantizar la protección de datos personales.

Figura 1: Timeline of relevant EU privacy legislation (Kretschmer, Pennekamp, y Wehrle, 2021).

Sin embargo, no entraremos a profundizar en cada una de estas normativas previas, ya que el GDPR (Reglamento (UE) 2016/679) es la principal regulación en materia de protección de datos en la actualidad y recoge en su texto gran parte de los principios y directrices previas. Dado que el GDPR es una regulación que abarca ampliamente la protección de datos personales en la UE, no es necesario profundizar en las normativas anteriores, especialmente porque extendernos en ellas alargaría innecesariamente el análisis de este capítulo.

3.1.1. Convenio 108 del Consejo de Europa

El objetivo de este apartado es analizar el Convenio 108 (formalmente, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal), resaltando su contenido esencial, importancia histórica y principios básicos, así como examinar su evolución mediante la versión modernizada (el conocido *Convenio 108+*) y su Protocolo Adicional, incorporando las novedades más recientes en esta materia. Se busca así contextualizar este instrumento dentro del marco general de la protección de datos en Europa y confirmar su relevancia actual.

Con la aparición de la Sociedad de la Información, el acceso a todo tipo de bienes y servicios conlleva la entrega de datos personales, sin ser los ciudadanos en la mayoría de los casos conscientes de ello. Esta situación se complica más aún cuando dichos datos son recogidos por empresas situadas en países que no forman parte de la UE y que, por tanto, ofrecen un nivel normativo de protección distinto. Así surgió la necesidad de crear mecanismos que permitiesen y protegiesen el movimiento internacional de datos con terceros países.

Como bien se expresó al comienzo de este capítulo, el principal objetivo del Convenio es garantizar el respeto de cada persona, sin importar su nacionalidad. En concreto, el respeto del *derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal* (art. 1). El Convenio define la protección de datos cómo cualquier información relativa a una persona física identificada o identificable.

Su importancia es de tal calibre que se trata del primer instrumento normativo jurídicamente vinculante a nivel europeo y el único de aplicación internacional en materia de protección de datos personales. Esto incluye no sólo a países no europeos que han suscrito dicho tratado, sino también a aquellos que, sin ser partes contratantes, son observadores (Tomás, 2019). Todos los Estados miembros del Consejo de Europa han ratificado el Convenio 108, y el instrumento está abierto a la adhesión de países no europeos, lo que ha llevado a que naciones de otros continentes (por ejemplo, Uruguay, Argentina, Marruecos, entre otras) se sumen al tratado (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), s.f.).

En cuanto a su contenido, el Convenio 108 recoge una serie de principios básicos de protección de datos que los Estados parte se comprometen a respetar mediante su legislación interna. Entre estos principios encontramos la calidad y proporcionalidad de los datos (los datos personales deben ser exactos, pertinentes y no excesivos en relación con las finalidades legítimas del tratamiento), la definición de categorías de datos que requieren protección reforzada (por ejemplo, datos sensibles como los relativos al origen étnico, salud, religión, etc.), la obligación de adoptar medidas de seguridad de los datos para prevenir accesos no autorizados o usos indebidos, así como garantías y derechos para

las personas afectadas, incluyendo el derecho de acceso a sus datos, rectificación o eliminación de información que no sea exacta (Martínez, 2021) (Cuadrada, 2007).

El Convenio prevé igualmente excepciones y restricciones justificadas (por ejemplo, por motivos de seguridad del Estado) siempre que sean proporcionales, e incluye mecanismos de recurso y sanción en caso de vulneración de sus disposiciones.

Por razones de extensión, no se desarrollan en detalle cada uno de estos principios en este apartado. Cabe señalar, no obstante, que dichos principios sentaron las bases de la legislación europea posterior y anticiparon muchos de los conceptos luego recogidos en instrumentos como la Directiva 95/46/CE y el Reglamento General de Protección de Datos (RGPD).

Con el fin de reforzar y actualizar el Convenio 108, el Consejo de Europa adoptó en 2001 un Protocolo Adicional relativo al control y a los flujos transfronterizos de datos. Este Protocolo adicional introdujo dos mejoras sustanciales a la estructura del Convenio: por un lado, exigió la creación de una autoridad de protección de datos independiente en cada Estado parte, encargada de velar por el cumplimiento de los principios del Convenio; y por otro, estableció condiciones para las transferencias internacionales de datos hacia países que no sean parte del Convenio. A partir de la creación de este protocolo, los datos personales solo pueden transferirse a un destinatario en un Estado no adherido al Convenio si ese Estado ofrece un nivel de protección adecuado (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), s.f.).

Las disposiciones del Protocolo adelantaron el concepto de "*nivel adecuado de protección*" que luego sería central en el derecho de la UE. Si bien todos los países del Consejo de Europa han suscrito el Convenio 108, no todos ratificaron inmediatamente el Protocolo Adicional; aun así, con el tiempo este estándar de autoridades de control independientes y protección en transferencias internacionales se convirtió en una práctica común en Europa y otras regiones.

Tras más de tres décadas de vigencia, las rápidas transformaciones tecnológicas hicieron necesaria una modernización del Convenio 108 para mantener su efectividad. En 2018, los Estados parte acordaron un Protocolo de modificación del Convenio (Protocolo

Adicional nº 223 del Consejo de Europa, conocido informalmente como Convenio 108+), destinado a actualizar sus disposiciones a las nuevas realidades de la era digital, para proteger al ciudadano al tiempo que proporciona un marco adecuado y con todas las garantías para el intercambio y flujos internacionales de datos (Martínez, 2021).

La versión modernizada se firmó el 10 de octubre de 2018 en Estrasburgo, contando con la adhesión tanto de países europeos como de terceros Estados (por ejemplo, Uruguay) y entró en vigor el 1 de octubre de 2023, tras alcanzar el número mínimo de ratificaciones requerido (38 Estados) (Martínez, 2021).

Entre las principales novedades del Convenio 108+ destacan las siguientes: se clarifican las bases legales que legitiman el tratamiento de datos (por ejemplo, consentimiento del interesado, interés legítimo, etc.); se amplía el catálogo de datos sensibles, incluyendo datos genéticos y biométricos; se establece la obligación de notificar a las autoridades de control las brechas de seguridad que comprometan datos personales; se fortalecen los derechos de los individuos, garantizando el derecho de acceso a los datos y el derecho de supresión de los mismos; introducción de requisitos más estrictos en materia de principios generales (por ejemplo, refuerzo de los principios de proporcionalidad, minimización de datos y licitud del tratamiento) (RedIPD, 2022)… Por tanto, existen una amplia gama de novedades que debido a su gran extensión no incidiremos en todas ellas.

3.1.2. Reglamento General de Protección de Datos (GDPR)

Como consecuencia, entre otras razones, de la popularidad de las redes sociales y de la digitalización de las gestiones online, el uso de las TIC ha seguido creciendo en los últimos años. Como mencionábamos al comienzo de esta tesis, los usuarios comparten información sensible por internet, sin ser conscientes de los riesgos que esto puede suponer.

Para prevenir esta afectación a la seguridad del usuario, es necesario que el mismo conozca en que consiste la privacidad de datos, cómo protegerla y ofrecerles herramientas para que puedan ejercer este derecho (Daudén-Esmel, Castellá-Roca & Viejo, 2022). Una de las claves para ello es el Reglamento (UE) del Parlamento Europeo y del Consejo de

27 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 (en adelante, GDPR).

Según el informe "Online Tracking: A 1-million-site Measurement and Analysis" publicado en 2016 por Englehardt y Narayanan, se reveló que alrededor del 70% de los sitios web más populares a nivel global emplean algún tipo de rastreo de usuarios. Este tipo de prácticas, que han generado preocupaciones sobre la privacidad, está ahora regulado por el GDPR, que impone restricciones claras sobre el uso de datos personales y su recopilación (Kretschmer, Pennekamp, y Wehrle, 2021).

Este Reglamento es de aplicación cuando (1) la empresa trata datos personales y tiene su sede en la UE, independientemente de donde se traten de hecho los datos o (2) la empresa tiene su sede fuera de la UE, pero trata datos personales relativos a ofertas de bienes o servicios a ciudadanos de la UE, o supervisa el comportamiento de datos en la UE.

Para proceder al tratamiento de datos personales, es necesario que se cumpla alguna de las siguientes condiciones (art. 6 GDPR):

- el interesado ha dado su **consentimiento**
- los datos personales son necesarios para respetar una **obligación contractual** con el interesado
- los datos personales son necesarios para cumplir una **obligación legal**
- los datos personales son necesarios para proteger los **intereses vitales** del interesado
- los datos personales se tratan para una **misión de interés público**
- se actúa en **interés legítimo** de la empresa, siempre que en el tratamiento de los datos del interesado no se vean gravemente afectados los derechos y libertades fundamentales de este; si los derechos de esa persona prevalecen sobre los intereses de la empresa, no se pueden tratar sus datos personales.

El GDPR impone normas estrictas sobre cómo se deben tratar los datos personales, basándose en el consentimiento. El propósito de estas regulaciones es asegurar que la persona afectada comprenda claramente lo que está aprobando. Por ello, el

consentimiento debe ser otorgado de forma libre, específica, informada e inequívoca, y debe presentarse mediante una solicitud redactada en un lenguaje claro y accesible (art. 7 GDPR). Este consentimiento debe manifestarse a través de un acto afirmativo, como marcar una casilla en línea o firmar un formulario.

Una vez que una persona da su consentimiento para el tratamiento de sus datos personales, estos solo podrán ser utilizados para los fines establecidos en el consentimiento. Además, se le debe ofrecer la posibilidad de retirar dicho consentimiento u oponerse al procesamiento de datos basado en intereses legítimos en cualquier momento. A modo de ejemplo, en la sección o pestaña dedicada precisamente a cookies, de la página web oficial del Real Madrid aparece lo siguiente: *"La presente política tiene por objeto informarle sobre las cookies que se utilizan en este Sitio Web. Usted puede aceptar todas las cookies, rechazar las no necesarias o aceptar sólo algunas de ellas a través de nuestro panel de configuración. También tiene la opción de eliminar las cookies mediante la selección de la correspondiente opción en su navegador*". No obstante, en la práctica esto realmente podría provocar un incorrecto funcionamiento de ciertos servicios e incluso el no acceso a la página web.

A diferencia de directivas anteriores, el GDPR introduce sanciones vinculantes para aquellos proveedores de servicios que incumplan las disposiciones del mismo. En particular, aquellos que no respeten sus normas pueden enfrentarse a multas de hasta el 4% de su facturación anual o 20 millones de euros, según lo establecido en su artículo 83.5 y 83.6. Sin embargo, conforme al art. 84.1, cada Estado Miembro de la UE tiene la libertad de establecer multas adicionales para infracciones no contempladas expresamente en el GDPR, siempre que estas sean efectivas, proporcionadas y disuasorias (Kretschmer, Pennekamp, y Wehrle, 2021).

3.2. Protección de datos en España

A lo largo de este apartado revisaremos la normativa española en materia de protección de datos personales, haciendo especial énfasis en la Ley de Servicios de la Sociedad de la Información (LSSI) por su relación directa con las *cookies*. Se presentarán las principales

leyes que han configurado el marco nacional de protección de datos y se explicará por qué, de cara al desarrollo del Capítulo IV, resulta necesario centrarse en la LSSI.

En España, como ya hemos adelantado, el derecho a la protección de datos tiene rango constitucional desde 1978 (art. 18.4 CE) y su desarrollo normativo proviene de varias leyes orgánicas. El desarrollo legislativo de la protección de datos comenzó con la Ley Orgánica 5/1992, de 29 de octubre de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Esta ley tenía por objeto limitar el uso de la informática para garantizar el honor y la intimidad de las personas, estableciendo las bases de la protección de datos y contemplando la creación de un registro de ficheros y de la propia Agencia Española de Protección de Datos (s.f.).

Sin embargo, la LORTAD fue posteriormente derogada y sustituida por la Ley Orgánica 12/1999, de protección de datos personales y garantía de los derechos digitales (LOPD), que transpone al ordenamiento español la Directiva Europea 95/46/CE. La LOPD supuso el "segundo hito" en la evolución de este derecho fundamental en España y actualizó el alcance de la LORTAD para adaptarse a la realidad digital emergente, ampliando la protección a todo tipo de tratamiento de datos (no solo automatizados), y detallando los derechos de los ciudadanos o derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Este régimen permaneció vigente hasta la aprobación de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), que adaptó el derecho español al GDPR y que incorpora un innovador catálogo de derechos digitales (como la desconexión digital, testamento digital, acceso universal a Internet, entre otros), siendo considerada por la doctrina como un "hito jurídico" (Dopazo, 2019).

A pesar de la existencia de numerosas leyes en materia de protección de datos, para evitar una amplia redacción, pondremos el foco en la legislación vigente más pertinente para internet, en especial la LSSI, por su conexión directa con el uso de cookies y otras tecnologías de seguimiento en la web.

3.2.1. Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (en adelante, LSSI)

Además de la normativa de protección de datos personales, en España existe un marco legal específico que regula ciertos aspectos de la actividad online, entre ellos el uso de *cookies*. La ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), transpone la Directiva Europea sobre Comercio Electrónico y establece las obligaciones de los prestadores de servicios en Internet. En el contexto de la protección de datos, la LSSI tiene una importancia particular porque establece el deber de información y obtención del consentimiento de los usuarios antes de instalar cookies u otras tecnologías similares en sus dispositivos.

La principal regulación relativa al uso de *cookies* se encuentra en la LSSI, concretamente en el artículo 22.2, que reza:

"2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario."

Según Riutort (2021), resulta necesario distinguir dos conceptos relevantes en el mundo de la publicidad: el editor o entidad prestadora de servicios titular de una página web que ofrece el espacio publicitario y, por otro lado, el de anunciante, que paga por utilizar ese espacio con el objetivo de publicitar sus servicios o productos.

Del citado precepto, se desprenden dos pilares fundamentales en el uso de *cookies*: la obligación de informar que tiene el editor respecto del usuario, y el consentimiento libre, específico e informado de este último.

En lo que refiere al deber de información, se trata de una obligación legal de tracto sucesivo, lo que implica que los usuarios deben tener acceso permanente, incluyendo cualquier modificación o actualización realizada por el responsable de la *cookie.* Una vez que se le haya proporcionado una información clara y completa al usuario sobre el uso de cookies, será, solo entonces, cuando el mismo estará en condiciones de prestar dicho consentimiento (Riutort, 2021).

En sus inicios (2002), la ley exigía informar a los usuarios sobre las cookies y ofrecerles la posibilidad de rechazarlas, pero tras la reforma introducida por el real Decreto-Ley 13/2012, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista, se endureció la regulación, pasando a requerir una aceptación previa por parte del usuario.

Desde 2012, por tanto, es obligatorio obtener el consentimiento del usuario antes de instalar cookies, una vez que este haya sido informado. Esta exigencia alineó la normativa española con las exigencias europeas en materia de privacidad. Posteriormente, la entrada en aplicación del GDRP en 2018 supuso elevar aún más el nivel de exigencia en cuánto a la validez del consentimiento.

La Agencia Española de Protección de Datos (2020) explica que, la LSSI, aunque es una norma sectorial distinta del GDPR, remite a la normativa de protección de datos para definir las condiciones del consentimiento. En consecuencia, hoy día el consentimiento para el uso de cookies en España debe cumplir con los criterios del GDPR: debe ser una manifestación de voluntad libre, específica, informada e inequívoca del usuario.

Tras la adopción del GDPR y la LOPDGDD, se ha aclarado que ninguna forma de consentimiento implícito o por omisión es válida para las cookies (AEPD, 2020), lo cual descarta prácticas antes toleradas (como asumir el consentimiento por el mero hecho de

seguir navegando). Asimismo, se exige ofrecer al usuario mecanismos claros y efectivos para aceptar o rechazar las cookies, y se establece que solo podrán utilizarse sin consentimiento aquellas cookies exceptuadas (por ejemplo, las que sean necesarias para prestar un servicio expresamente solicitado) (AEPD, 2020).

En virtud de este deber de transparencia, el Grupo de Trabajo del artículo 29 sobre protección de datos, creado por la Directiva 95/46/CE para proporcionar directrices sobre la interpretación de las normas de protección de datos (actualmente denominado Comité Europeo de Protección de Datos), recomienda el sistema de información por capas, que permite que el usuario acceda directamente a los aspectos más relevantes del aviso, según su interés, sin necesidad de revisar todo el contenido. De esta forma se evitaría la sobrecarga informativa (Riutort, 2021).

CAPÍTULO IV. DERECHOS RELACIONADOS CON LAS TECNOLOGÍAS

El marco normativo español en materia de protección de datos ha evolucionado en línea con las regulaciones europeas, adaptándose a los desafíos que plantea la digitalización. Normativas como la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) han establecido requisitos clave, como la obligación de informar y obtener el consentimiento del usuario en el uso de cookies y otros mecanismos de rastreo.

En los siguientes apartados, analizaremos el impacto de las principales regulaciones en materia de privacidad de datos en internet y redes sociales, así como los desafíos de regular tecnologías como Internet y *cookies*.

4.1. Internet

Entre todos los avances tecnológicos que han aparecido a lo largo del tiempo, Internet es el más importante. La RAE lo define como una *"red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación"*, lo que significa que Internet conecta diferentes redes, razón por la que también se le conoce como la "red de redes" o la "Autopista de la Información".

Al tratarse de una red global, no está regulada por un único marco legal, sino que existen miles de normativas locales que se aplican de forma independiente en cada país (Porras, 2016). Esta fragmentación genera problemas jurídicos, ya que cada Estado intenta regular Internet según sus propios intereses mientras la tecnología sigue evolucionando sin fronteras claras.

El crecimiento de Internet ha impulsado la creación de nuevas leyes, instituciones y jurisprudencia con el fin de proteger a los usuarios. Sin embargo, el principal problema es que, si no se logra frenar a tiempo la invasión de la privacidad, ¿cómo se podrá

controlar en el futuro, cuando la tecnología sea aún más avanzada y omnipresente? A pesar de los intentos de regulación, Internet sigue siendo un espacio difícil de controlar, ya que su naturaleza es dinámica y no se limita a un territorio concreto (Porras, 2016).

Un ejemplo de la importancia de la privacidad en Internet lo encontramos cuando un usuario se conecta a su red wifi o *router*[11]. En teoría, acceder a una red privada debería proporcionar cierto nivel de protección. No obstante, la realidad es que terceros pueden interceptar la conexión y manipular, eliminar o apropiarse de información personal con distintos fines, incluidos los económicos. En este contexto, surge la figura del *hacker*, una persona que explora, modifica o accede a sistemas tecnológicos, redes, programas informáticos o *softwares*[12].

La preocupación por la privacidad en la red se intensificó en 2004 con la llegada de Gmail, cuando Google comenzó a analizar el contenido de los correos electrónicos para mostrar publicidad personalizada. Como respuesta a esta invasión de privacidad, surgieron alternativas como DuckDuckGo, un buscador que no rastrea la información de sus usuarios (Porras, 2016).

Esta problemática también se manifiesta en la gestión de *cookies* en la navegación web. Actualmente, al acceder a una página, es común encontrarse con pop-ups que informan al usuario del uso que hacen los proveedores de servicio sobre los datos que recaban mientras navegamos por sus páginas y que ofrecen tres opciones: aceptar todas las *cookies*, rechazarlas o configurarlas. Aceptarlas, aun siendo la opción que habilita al usuario para acceder al contenido de la web en la mayor brevedad posible, sin embargo, permite a prestadores de servicios (empresas y gobiernos) recopilar datos del usuario, creando perfiles detallados y permitiendo la inferencia de información sensible, como datos de salud, situación económica, localización geográfica precisa o aspectos familiares. La tercera opción, requiere de un esfuerzo adicional por parte del usuario, pues debe revisar cada uno de los usos y decidir si los acepta o rechaza de manera manual, invirtiendo una mayor cantidad de tiempo. Como resultado, en la mayoría de los casos,

[11] Según la RAE, un *router* es un dispositivo que distribuye el flujo de paquetes de información entre redes de la manera más eficaz.
[12] Un *software* es el conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

los usuarios terminan aceptando todas las condiciones sin leerlas a fondo. Esto plantea un riesgo significativo para la intimidad del usuario, por lo que requerirá de un exhaustivo análisis en el subapartado 4.1.2.

En algunos contextos, los gobiernos han tomado medidas para restringir el acceso a Internet en situaciones como conflictos bélicos, estados de emergencia, desastres naturales, órdenes judiciales o problemas de seguridad. Estas restricciones buscan, en teoría, garantizar el orden público y evitar alteraciones en la ciudadanía en momentos críticos (Manny, 2003).

En este sentido, la Resolución del Consejo de Derechos Humanos del 5 de julio de 2012 establece que los derechos que tienen las personas en el mundo físico también deben protegerse en el entorno digital. En particular, se defiende la libertad de expresión en Internet y otras tecnologías, reconociendo además que la red es una herramienta clave para el desarrollo y el ejercicio de los derechos humanos.

4.1.1. Internet como derecho fundamental

Uno de los debates más relevantes en torno a Internet es si su acceso debe considerarse un derecho fundamental. Es decir, ¿debería garantizarse el acceso a Internet como un derecho básico para todos los ciudadanos?

En España, este derecho fue reconocido en 2003, y la Ley 2/2011, de 4 de marzo, de Economía Sostenible, lo reforzó al establecer que todos los ciudadanos debían tener acceso a Internet de banda ancha, fijando un mínimo de 1 Mb/s para las descargas. A nivel internacional, en 2011, las Naciones Unidas[13] reconocieron este derecho, lo que llevó a que más países lo adoptaran, considerándolo una extensión de otros derechos fundamentales, como la libertad de expresión.

Uno de los mejores esfuerzos, según cita Porras (2016), es la declaración del derecho como fundamental emitido en la Sentencia 2009/580 DC de 10 de junio 2009 por el

[13] Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue (16 de mayo de 2011).

Consejo Constitucional de la República Francesa *"Considerando que de conformidad con el artículo 11 de la Declaración de los derechos del hombre y del ciudadano de 1789: «La libre comunicación de pensamientos y opiniones es uno de los derechos más valiosos del hombre: cualquier ciudadano podrá, por consiguiente, hablar, escribir, imprimir libremente, siempre y cuando responda del abuso de esta libertad en los casos determinados por la ley»; que en el estado actual de los medios de comunicación y con respecto al desarrollo generalizado de los servicios de comunicación pública en línea así como a la importancia que tienen estos servicios para la participación en la vida democrática y la expresión de ideas y opiniones, este derecho implica la libertad de acceder a estos servicios."*

Sin embargo, garantizar el acceso universal a Internet sigue siendo un reto. Uno de los principales problemas en este ámbito es la llamada brecha digital (*digital divide*), que se refiere a la desigualdad entre quienes tienen acceso a las Tecnologías de la Información y Comunicación (TIC) y quienes no. Esta diferencia es especialmente notable en países en vías de desarrollo, como en América Latina, donde, a pesar del crecimiento económico experimentado en las últimas décadas, sigue existiendo una importante falta de acceso a las TIC.

Por otro lado, hay países donde el acceso a Internet está generalizado, pero es restringido por razones políticas, religiosas, ideológicas o económicas, lo que supone una vulneración de derechos fundamentales. Un caso muy conocido es el de la República Popular de China, donde el acceso a la Red está limitado con el objetivo de controlar la información que recibe la población y evitar influencias externas que puedan afectar al sistema político o económico del país (Moraga, 2004). Entre los sitios web bloqueados en China se encuentran ChatGPT (cuyo veto favorece a su alternativa local, DeepSeek), Reddit, LinkedIn, YouTube o The New York Times (Vic-Liu, 2024). Un caso aún más extremo es el de Corea del Norte, donde directamente no existe Internet para la población (Moraga, 2004).

Otro de los grandes problemas de Internet es la seguridad en la red. La facilidad de acceso y el anonimato han favorecido la proliferación de actividades ilícitas, como la difusión de pornografía, la prostitución infantil, el narcotráfico, el terrorismo, las estafas y los fraudes. Estos riesgos ponen en peligro la seguridad de los usuarios y han llevado a los gobiernos

a establecer medidas para combatir estas amenazas, aunque muchas veces se enfrentan a la dificultad de regular un espacio tan amplio y descentralizado.

Con todo ello, puede parecer que el acceso a Internet como derecho fundamental no tiene relación directa con la intimidad. Hoy en día, casi todas nuestras actividades pasan por Internet: informarnos, comunicarnos, comprar, trabajar o incluso hacer gestiones con la Administración. Por eso, cuanto más necesario se vuelve el uso de internet, más expuestos estamos también a que se vulneren nuestros datos personales. En este contexto, reconocer el acceso a Internet como un derecho también implica reforzar las garantías para proteger la privacidad de los cibernautas. Es decir, no basta con permitir que todos accedan a Internet, también hay que asegurarse de que ese acceso no implique renunciar a la intimidad.

4.1.2. Cookies

Como veníamos puntualizando al comienzo del capítulo, internet supone uno de los mayores avances tecnológicos del momento, y es que me atrevería a decir que se ha vuelto fundamental en nuestro día a día. Tanto es así que ya hasta las compras se efectúan por internet y buena parte de la publicidad que desarrollan las empresas se realiza de modo digital. A este respecto resulta muy importante la utilización de *cookies*, pues es lo que permite a las empresas llegar a un público acertado a la hora de publicitar sus productos. Por ello, en este subapartado veremos en qué consisten, además de alternativas a su uso.

El término *cookies* de HTTP se refiere a los datos almacenados en el dispositivo de un usuario para facilitar el acceso a páginas web y realizar un seguimiento de su actividad en la red. Se puede resumir en la idea de que prestadores de servicios obtienen datos relacionados con los usuarios, susceptibles de ser utilizados para diversos fines (Riutort, 2021).

Entre las compañías que más se han beneficiado del uso de *cookies* se encuentra Google, a través de su servicio Google Analytics, que permite generar informes sobre el comportamiento de los usuarios y el tráfico en la red (Porras, 2016).

Las *cookies* juegan un papel clave en el mundo de la publicidad digital. Son herramientas esenciales para la prestación de numerosos servicios de la sociedad de la información, ya que facilitan la navegación y permiten ofrecer publicidad personalizada basada en los hábitos de consumo de los usuarios. Se enmarcan en un concepto de publicidad definida en el Dictamen 2/2010, emitido el 22 de junio de 2010 por el Grupo de Trabajo de Protección de Datos del Artículo 29 (GT29), sobre publicidad comportamental en línea como aquella *"basada en la observación continuada del comportamiento de los individuos, que busca estudiar las características de dicho comportamiento a través de sus acciones (visitas repetidas a un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los intereses inferidos de su comportamiento"*.

El GT29 delimita el proceso que siguen las cookies de rastreo de la siguiente manera:

1) Cuando un usuario visita por primera vez una página web que muestra anuncios de una determinada red publicitaria, esta red coloca una cookie de rastreo en su dispositivo (ordenador, móvil...).
2) Esta cookie es única para cada navegador, por lo que si el usuario vuelve a visitar la misma página o accede a otro sitio web que también forma parte de esa red publicitaria, la cookie permite reconocerlo como un visitante recurrente.
3) Con el tiempo, al analizar los sitios que visita y la frecuencia con lo que lo hace, la red publicitaria recopila información sobre sus intereses y comportamiento en línea.
4) Con base en este perfil, la red publicitaria puede mostrar anuncios adaptados a los gustos y hábitos del usuario, aumentando así la efectividad de la publicidad.

Así, el contenido que se muestra en una página web puede ser diferente para cada usuario, incluso si acceden al mismo tiempo.

Originalmente, fueron creadas con la intención de mejorar la experiencia de navegación, pero con el tiempo se han convertido en una herramienta de rastreo masivo que ha generado preocupaciones en materia de privacidad. Si bien no todas las *cookies* tienen fines ilícitos, su uso ha derivado en abusos por parte de algunas empresas.

Inicialmente, los usuarios no eran informados sobre la recopilación de datos a través de *cookies*, lo que generó una gran controversia en torno a la privacidad. Como respuesta a esta situación, y conforme a lo estudiado en el capítulo 3.2.1: deber de información y consentimiento del usuario) el Parlamento y el Consejo Europeo aprobaron la Directiva 2009/136/CE, que estableció la obligación de que los servidores informen de manera clara a los usuarios sobre el uso de *cookies* para que conozcan la finalidad para la que se utilizarán sus datos y soliciten y obtengan el consentimiento de los usuarios.

En el ámbito español, la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico también regula el uso de *cookies*. Esta normativa permite que las empresas almacenen información en los dispositivos de los usuarios, siempre que cuenten con su consentimiento previo y proporcionen información detallada sobre la finalidad de los datos recopilados.

Continuando con el ejemplo de los pop-ups que mencionábamos al comienzo de este capítulo, y a pesar de que se le ofrezca al usuario la posibilidad de retirar su consentimiento[14], lo cierto es que el proceso de aceptación / configuración de cookies de rastreo se debe repetir cada vez que un particular desee acceder a un nuevo sitio web, lo que resulta muy difícil recordar todas las páginas web para las que ha dado su consentimiento y el tipo de consentimiento que otorgó. ¿No sería más sencillo hacer una preconfiguración general de cookies que aplique de igual manera a todas las páginas web?

Cómo respuesta a ese abuso del derecho a la privacidad, existen autores (Daudén-Esmel, Castellá-Roca, & Viejo, 2022) que proponen un nuevo sistema de almacenamiento de datos que *"de forma automática y transparente gestione las preferencias del uso de las cookies y del nivel de privacidad que desea cada usuario. De este modo, se evitará el "Aceptar todo" (...). Se requiere de una alternativa a esta centralización de la gestión del consentimiento en los servidores de proveedores de servicio. Como alternativa, algunos trabajos sugieren descentralizar estos consentimientos mediante su inclusión en*

[14] Se considera que se cumple dicho requisito cuando el sistema de gestión de cookies (panel de configuración, plataformas de gestión del consentimiento, etc.) esté integrado en la propia política de cookies o cuando se incluya en la misma un enlace que lleve directamente al sistema de gestión (Agencia Española de Protección de Datos (2020)).

Contratos Inteligentes, los cuales son ejecutados en una blockchain[15] *(se realiza el "deploy*[16]*" del contrato inteligente)".*

Proponen por tanto un sistema automatizado para gestionar la privacidad y el uso de *cookies* en internet, evitando que los usuarios tengan que aceptar o rechazar manualmente los avisos de *cookies* en cada página web que visitan. Se trata de una plataforma basada en *blockchain* que registra de manera segura las preferencias de privacidad de cada usuario, asegurando que no puedan ser alteradas sin su consentimiento. Se instala una extensión en el navegador que responde automáticamente a las solicitudes de cookies según las preferencias configuradas previamente. Así, los usuarios podrían ver quién tiene acceso a sus datos, modificar sus preferencias y revocar permisos en cualquier momento.

El objetivo principal de esta propuesta consiste en evitar que los usuarios tengan que interactuar constantemente con avisos de cookies, además de asegurar que las preferencias de privacidad se respeten de manera automática y dar transparencia y control sobre quién accede a los datos personales.

Resulta asimismo relevante la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 1 de octubre de 2019, en el asunto C-673/17, en la que se establece que el consentimiento para el uso de cookies no es válido si se otorga mediante una casilla marcada por defecto que el usuario debe desmarcar si no desea aceptar el almacenamiento de datos.

Esto implica que la inacción del usuario no puede interpretarse como un consentimiento válido según la normativa europea de protección de datos. Este criterio refuerza la necesidad de adoptar medidas que garanticen una verdadera elección parte del usuario, asegurando así una protección más efectiva de su privacidad.

[15] IBM define el *blockchain* como, "a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network".
[16] Implementación, despliegue, o puesta en marcha.

CAPÍTULO V. DERECHO A LA PROPIA IMAGEN DE MENORES EN REDES SOCIALES

En el contexto del derecho a la intimidad en la era digital, uno de los fenómenos más relevantes ha sido la aparición de las redes sociales. Lo que comenzó como un medio para conectar con amigos y familiares se ha convertido en una herramienta con múltiples aplicaciones, desde el marketing digital hasta la movilización política.

De acuerdo con el informe de IAB (asociación mundial de comunicación, publicidad y marketing digital) (2020), aproximadamente un 90% de la población en España hace uso de las redes sociales, abarcando un rango de edad que va desde los 16 hasta los 65 años. No obstante, este porcentaje ha experimentado un incremento a raíz de la pandemia. En cuanto a la distribución por género, el uso de estas plataformas es prácticamente equitativo, con un 49% de hombres y un 51% de mujeres. Las redes que lideran el ranking de uso son: WhatsApp (85%) que sigue posicionándose como la red favorita, Facebook (81%) utilizado por un público más mayor, y Youtube (70%) e Instagram (59%) utilizado en gran parte por mujeres y por los más jóvenes (Martín y Medina, 2021).

Debido al constante uso de las redes sociales por parte de la población, resulta necesario analizar a lo largo de este capítulo el derecho que lo protege, la legislación y la afectación a un caso más concreto (menores de edad), junto con casos recientes resueltos por la jurisprudencia.

5.1. Derecho a la propia imagen

El derecho a la propia imagen es un derecho fundamental reconocido en el art. 18.1 CE, junto con, como mencionamos en el Capítulo III, los derechos al honor y a la intimidad. Este derecho otorga a toda persona (incluidos menores) la "*facultad de impedir la obtención, reproducción o publicación de su imagen por terceros sin su consentimiento expreso*".

Al igual que el derecho a la intimidad, no es un derecho absoluto, pues debe coexistir con otros derechos fundamentales (como la libertad de información). Es decir, una persona

tiene el derecho a controlar el uso de su imagen, pero este derecho no siempre es ilimitado pues tiene que equilibrarse con otros derechos fundamentales. No obstante, cuando se quiere limitar o restringir el derecho a la propia imagen, es necesario realizar un análisis que compare qué derecho prevalece en cada caso concreto. Para ello, hay que evaluar si la difusión de una imagen sin el consentimiento de la persona afecta su privacidad y dignidad (de las Hervas, 2018).

En el caso de los menores de edad, la protección de su imagen y privacidad es aún más intensa, dado que son especialmente vulnerables y la divulgación de su imagen puede afectar su desarrollo y futura reputación. De hecho, la doctrina constitucional española exige la máxima cautela en la difusión de información o imágenes de menores, otorgándoles un ámbito de "superprotección", incluso cuando pudiera haber interés público (Toral Lara, 2020)[17].

El marco legal específico para proteger la imagen de los menores incluye la LO 1/1982, de Protección Civil del Derecho al Honor, Intimidad y Propia Imagen, que tipifica como intromisión ilegítima la publicación de la imagen de una persona sin consentimiento (salvo excepciones) y exige consentimiento expreso del titular del derecho para legitimar la difusión. Los menores, aun careciendo de plena capacidad de obrar, son titulares de estos derechos de la personalidad (honor, intimidad, imagen) según reconoce expresamente el artículo 4.1 de la Ley Orgánica 1/1996, de Protección Jurídica del Menor (Toral Lara, 2020).

Esta ley subraya que, incluso con el consentimiento de los padres, la publicación de imágenes de un menor podría constituir una intromisión ilegítima si menoscaba su honor o reputación (Saiz, 2023). Es decir, los representantes legales del menor no pueden consentir válidamente una publicación que perjudique al hijo, ya que siempre debe primar el interés superior del menor.

Por otro lado, desde la perspectiva de protección de datos personales y según la Agencia Española de Protección de Datos (AEPD), la imagen de un menor se considera un dato

[17] STS 1003/2008, de 23 de octubre y STS 1004/2008, de 23 de octubre.

personal: la LO 3/2018 (adaptada al RGPD) fija en 14 años la edad a partir de la cual un menor puede consentir por sí mismo el tratamiento de sus datos en internet. Por debajo de esa edad, se requiere el consentimiento de los padres o tutores para cualquier tratamiento de datos personales del menor, incluida la publicación de fotografías en redes sociales. En todo caso, el consentimiento debe ser expreso e inequívoco por parte del titular del derecho (o sus representantes legales), según exige el art. 2 LO 1/1982 (Toral Lara, 2020).

5.2. Caso de estudio: Publicación de imágenes de menores en redes sociales por sus progenitores

Cuando son los propios padres u otros representantes legales quienes publican fotos de menores en redes sociales, deben respetar estos límites legales. En general, los padres tienen la potestad de decidir sobre la imagen de sus hijos, pero siempre en beneficio de ellos. El art. 156 CC establece que la patria potestad se ejerce conjuntamente por ambos progenitores y, aunque cada uno puede tomar decisiones "conformes al uso social" de forma individual, en caso de decisiones de mayor trascendencia se requiere el consentimiento de ambos. La difusión de la imagen de un hijo en Internet suele considerarse un acto relativo a la patria potestad (no meramente cotidiano), por lo que precisa de la autorización de ambos progenitores si ambos ostentan la patria potestad (Toral Lara, 2020).

Numerosas resoluciones judiciales han sostenido que publicar fotos de un menor sin el consentimiento del otro progenitor constituye una vulneración de su derecho a la imagen[18]. Incluso si uno de los padres tiene la custodia exclusiva, la imagen del menor sigue bajo patria potestad compartida, lo que implica que la oposición de uno de ellos a la publicación debe ser respetada, salvo autorización judicial en caso de no estar ambos de acuerdo (Saiz, 2023). En situaciones de desacuerdo, el progenitor que desee difundir

[18] Sentencia de la Audiencia Provincial de Pontevedra, Sección 1ª, 208/2015, de 4 de junio; Sentencia de la Audiencia Provincial de Barcelona, Sección 18ª, 360/2017, de 25 de abril; Sentencia Audiencia Provincial de Cantabria, Sección 2ª, 24/2020, de 13 de enero; Sentencia del Tribunal Supremo 249/2023, de 14 de febrero.

la foto debe acudir al juez, para que este resuelva quién decide sobre esta cuestión (con un procedimiento de jurisdicción voluntaria, art. 86 de la Ley 15/2015) (Toral Lara, 2020).

Es importante destacar que el consentimiento de los padres no es ilimitado: aunque ambos estuvieran de acuerdo, la publicación de imagenes "sensibles" o que pudieran perjudicar la dignidad, seguridad o privacidad del menor sería ilícita. Los tribunales y la Agencia de Protección de Datos recomiendan a los progenitores máxima prudencia. Una vez que la imagen se sube a redes, se pierde control sobre su difusión y puede ser usada por terceros para fines no deseados, lo que puede dañar gravemente al menor (Saiz, 2023). Por tanto, incluso fotos aparentemente inofensivas pueden entrañar riesgos (posible *bullying*, robo de identidad, uso por pedófilos, etc.) y se aconseja evitar exponer de manera innecesaria a los niños en Internet. En palabras de la jurisprudencia, los padres "no están autorizados a una difusión ilimitada" de la imagen o información del menor, especialmente si puede ocasionarle perjuicio (Toral Lara, 2020). Su trabajo como representantes consiste en salvaguardar la privacidad e imagen del hijo, más que promocionarla.

A este respecto, juega un papel muy importante el Ministerio Fiscal como garante del interés superior del menor, que instará de inmediato las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil (art. 4.2) y solicitará las indemnizaciones que correspondan por los perjuicios causados. El Fiscal podrá solicitar al juez la retirada de imágenes, impedir nuevas publicaciones o adoptar medidas urgentes de protección, incluso contra la voluntad de los padres si considera que la exposición del menor en redes vulnera los derechos fundamentales (Alviarez, 2018).

5.2.1. Cuentas privadas vs. Cuentas públicas en Redes Sociales

Al publicar fotos de menores en redes sociales, el ámbito de difusión (privado o público) es un factor relevante legalmente. No es lo mismo compartir la imagen en un perfil privado, accesible solo a familiares y amigos de confianza, que en una cuenta pública abierta a cualquier usuario. Algunos tribunales han considerado que compartir fotografías

no comprometedoras de un menor en un entorno privado (círculo familiar o amistad cercana) puede encuadrarse dentro de los usos sociales normales de la patria potestad. En esos casos, se ha estimado que no hay una intromisión ilegítima en la imagen del menor siempre que la difusión esté limitada y controlada (pues el riesgo para el menor es mínimo) (Saiz, 2023).

Por ejemplo, la Audiencia Provincial de Barcelona en la sentencia 265/2015, de 22 de abril, permitió a una madre publicar fotos de su hijo siempre que la configuración de privacidad de su cuenta restringiera el acceso a únicamente familiares y amigos, negando la petición del padre de prohibir cualquier publicación bajo esas condiciones. En tal situación, se entiende que la publicación es conforme a los usos sociales ordinarios (Toral Lara, 2020), equiparable a enseñar fotos del álbum familiar, y por tanto un solo progenitor podría autorizarla (siempre que el contenido no vulnere la dignidad del menor).

En cambio, cuando las imágenes se comparten en perfiles públicos (accesibles de forma general en Internet), la difusión es indiscriminada y el riesgo para la privacidad del menor se dispara. Publicar en abierto la foto de un niño equivale a divulgarla mundialmente, lo que suele considerarse una intromisión en su derecho a la propia imagen si no medió el consentimiento de ambos padres y, por supuesto, del propio menor si tiene suficiente madurez. La jurisprudencia mayoritaria en España exige el acuerdo de los dos progenitores para publicaciones de este tipo, dada la potencial gravedad para el menor (Toral Lara, 2020).

Incluso en casos de cuentas privadas, no existe una garantía absoluta: las imágenes pueden ser reenviadas o copiadas por terceros sin autorización. De hecho, en la Sentencia 360/2017 (secc.18), de 25 de abril, la Audiencia Provincial de Barcelona sostuvo que aun cuando el padre publicó fotos del hijo en un entorno restringido a amigos, la falta de consentimiento de la madre hacía ilegítima la publicación[19]. Es decir, no hay un cambio de criterio general por limitar la audiencia: la oposición de un hijo puede tornar ilícita la difusión, aunque sea en ámbito inicialmente privado.

[19] Sentencia de la Audiencia Provincial de Barcelona, Sección 18ª, 360/2017, de 25 de abril.

En síntesis, existe una tendencia a considerar que la publicación de fotos de menores es una decisión que forma parte de la patria potestas, lo que implica que se necesita el consentimiento de ambos padres. Sin embargo, en algunos casos, esta exigencia puede ser menos estricta si la difusión se limita al entorno familiar y no representa un riesgo para el menor. Pero incluso en estos supuestos, se reconoce el riesgo de "filtración" de esas imágenes fuera del círculo privado (Toral Lara, 2020).

Por ello, la recomendación es prudencia máxima: si se van a compartir fotos de niños, que sea con un perfil privado, pocos contactos de confianza, y contenido respetuoso, pues cuanto mayor sea la difusión (por ejemplo, en una cuenta pública o de "*influencer*"), mayor la probabilidad de vulnerar derechos del menor.

5.2.2. Jurisprudencia relevante

A continuación, se identifican y analizan algunos casos jurisprudenciales destacados en España referentes a la publicación de imágenes de menores en redes sociales.

1) Sentencia Audiencia Provincial de Pontevedra 208/2015 (Sección 1ª, 4 de junio de 2015). Se trata de un caso de padres divorciados en el que la Audiencia Provincial declaró que publicar fotos de la hija menor en Facebook formaba parte de la patria potestad, por lo que era necesario el consentimiento de ambos progenitores. Al no contar con el consentimiento del padre, ordenó la retirada de las imágenes y prohibió futuras publicaciones sin acuerdo mutuo, priorizando el interés de la menor.
2) Sentencia Audiencia Provincial de Cantabria 24/2020 (Sección 2ª, 13 de enero de 2020). En ella, la Audiencia Provincial confirmó, una vez más, que sin consentimiento de ambos progenitores no se pueden subir fotos de una hija menor de edad a redes sociales. En este sentido, la Audiencia Provincial ordenó a la madre cesar la publicación de imágenes de su hija en Facebook, enfatizando la protección reforzada de la intimidad de los menores, y, por tanto, estimando la demanda del padre que pretendía proteger la imagen de la niña.
3) Sentencia Audiencia Provincial de Barcelona 360/2017 (Sección 18ª, 25 de abril de 2017). Un padre compartió fotos de su hijo en redes con perfil privado

(únicamente a amigos). A pesar de ello, la Audiencia Provincial consideró la publicación ilegítima por carecer del consentimiento de la madre, ordenando también la eliminación de fotos. Esta sentencia dejó claro que ni siquiera la privacidad configurada limita la exigencia de autorización de ambos padres cuando uno de los dos se opone (Toral Lara, 2020).

4) Sentencia Tribunal Supremo nº249/2023 (Sala 1ª de lo Civil, 14 de febrero de 2023). Se trata de un caso singular en el que el Tribunal Supremo avaló la difusión de imágenes de una niña con el consentimiento de solo uno de sus progenitores, dadas las circunstancias especiales. En este asunto, la madre (personaje público) había proporcionado fotos de su hija a un medio digital y las publicó en redes, mientras el padre (también personaje público) no consentía. El TS desestimó la demanda del padre contra el medio, recordando que para menores no maduros quienes deben consentir son los titulares de la patria potestad, y que "*vale con el de uno solo, conforme al uso social y a las circunstancias*" (Europa Press, 2023). Se consideró probado que la madre había consentido y que la publicación (una entrevista familiar durante el confinamiento, y fotos ya existentes en el perfil público de la madre) no lesionaba el interés de la menor. Esta sentencia del TS matiza que, en algunos contextos muy concretos, el consentimiento de un solo progenitor podría ser suficiente, aunque realmente se trata de una excepción que depende de las circunstancias (por ejemplo, imágenes ya divulgadas por uno de los padres en un ámbito público, ausencia de riesgo apreciable para la niña, etc.). En general, fuera de esta excepción, sigue rigiendo la necesidad de contar con el acuerdo conjunto de los padres para difundir la imagen de hijos menores.

Además de los casos expuestos, la jurisprudencia y la doctrina han avisado de las posibles consecuencias legales a futuro por la exposición excesiva de menores en redes, concepto conocido como *sharenting*. Por ejemplo, se ha planteado que los hijos, al alcanzar la mayoría de edad, podrían demandar a sus propios padres por la vulneración de su derecho a la imagen durante la infancia. De hecho, estarían legitimados para reclamar una indemnización por daños morales e incluso ejercitar acciones penales por un delito contra la intimidad (art. 197.7 CP) en aquellos casos en los que la difusión de sus fotos de niño le causara algún tipo de perjuicio.

Sainz (2023) señala que una vez mayores de edad, los hijos podrían exigir (1) la retirada de las imágenes, a pesar de que las mismas estuvieran en cuentas privadas y (2) la responsabilidad civil correspondiente, teniendo en cuenta la magnitud que tuvo la difusión para valorar los daños. Así unos padres "*influencers*" que explotan la imagen de sus hijos menores en redes (conocidos como "*instamamis*" o "*instapapis*") se arriesgan a futuras reclamaciones de sus hijos por haber comprometido su privacidad (González, 2021).

A modo de resumen, la normativa española reconoce ampliamente el derecho de los menores a su propia imagen y establece límites claros a su difusión en redes sociales. Publicar fotos de niños requiere, por regla general, el consentimiento de ambos progenitores y debe hacerse siempre velando por el interés del menor. La ley y los tribunales protegen de forma reforzada a los menores frente a intromisiones en su imagen: si una publicación en redes vulnera su privacidad o dignidad, puede considerarse ilegítima y dar lugar a acciones de retirada e indemnización.

La diferencia entre un entorno privado y uno público en redes es relevante, pero no exime de responsabilidad; incluso con ajustes de privacidad, se aconseja el mutuo acuerdo de los padres y prudencia extrema. La evolución de la jurisprudencia muestra una tendencia protectora: salvo excepciones predomina la necesidad de autorización conjunta para difundir imágenes de menores. En definitiva, el derecho del menor a no ser expuesto prevalece sobre el deseo de los padres de compartir su imagen, y las autoridades recomiendan limitar la huella digital de los niños hasta que puedan decidir por sí mismos.

CAPITULO VI. CONCLUSIONES.

1. El derecho a la intimidad ha cobrado una gran importancia en la era digital debido al mayor uso que hace la población de las tecnologías y la masiva recopilación de datos personales. Las personas están constantemente compartiendo información en Internet, ya sea de forma activa, como al registrarse en una página web, o de manera pasiva, a través del uso de cookies y otras tecnologías de rastreo. A raíz de esto, surge un reto: asegurarse de que el derecho a la privacidad sea respetado en un entorno donde la información fluye libremente, y las leyes que protegen la intimidad deben adaptarse rápidamente a estos cambios tecnológicos.
2. A pesar de que existan normativas como el Reglamento General de Protección de Datos (GDPR) y la Ley de Servicios de la Sociedad de la Información (LSSI), la realidad es que la protección de la privacidad enfrenta aún importantes dificultades como es el manejo de las *cookies* en la web. A pesar de la variedad de intentos legislativos de garantizar que los usuarios sean correctamente informados sobre el uso de sus datos, la mayoría de las personas tienden a aceptar las cookies sin leer las condiciones, lo que genera grandes perjuicios en materia de privacidad. Además, la regulación aún no cubre completamente las nuevas tecnologías emergentes como el uso de la Inteligencia Artificial para crear perfiles detallados de los usuarios, lo que plantea nuevos desafíos a la protección de la privacidad.
3. La protección de la privacidad y los datos personales supone un constante reto, debido a la falta de conocimiento y control por parte de los usuarios sobre cómo se utilizan sus datos. La aceptación masiva e involuntaria de *cookies* es un claro ejemplo de cómo las normativas actuales no logran frenar completamente la invasión de la privacidad. Para mejorar la efectividad de la protección, se podrían implementar soluciones como un sistema de gestión automatizada de las cookies, basado en la propuesta de Daudén-Esmel, Castellá-Roca y Viejo (2022), comentada en el apartado 4.3.2. Proponen una plataforma basada en *blockchain* que guarda las preferencias de privacidad del usuario de manera segura. Con esta extensión para el navegador, los usuarios no tendrían que aceptar o rechazar manualmente las cookies en cada página, sino que el sistema respondería automáticamente según sus preferencias preconfiguradas. Además, el usuario podría ver quién tiene acceso a sus datos y modificar sus permisos en cualquier momento, asegurando así un control total sobre su privacidad. Este tipo

de soluciones tecnológicas podrían simplificar la gestión de la privacidad para los usuarios y garantizar que sus datos no sean utilizados "de mala manera".

4. El constante avance de las tecnologías requiere que la legislación sobre privacidad se mantenga actualizada para adaptarse a nuevos riesgos. Por ejemplo, los datos generados por dispositivos conectados, como los del Internet de las Cosas (IoT) o la Inteligencia Artificial, no están suficientemente regulados. Las leyes deben evolucionar para abordar estos nuevos desafíos, ofreciendo mayor protección frente a la recopilación masiva de datos que se está produciendo en la actualidad.
5. La privacidad no es solo una cuestión nacional, sino también global. Los datos personales circulan por todo el mundo, y a menudo, las empresas que los recopilan se encuentran fuera de la jurisdicción de los países en los que se generan esos datos. Esto hace necesario una cooperación entre gobiernos internacionales para garantizar que la protección de la intimidad sea efectiva y uniforme en todos los países. Para lograrlo, sería importante crear acuerdos globales que armonicen las legislaciones de privacidad y protejan los derechos de los usuarios sin importar su ubicación.
6. A pesar de los avances normativos, existen brechas que necesitan todavía ser cubiertas. Un ejemplo de ello es la regulación sobre el uso de imágenes de menores en redes sociales. Muchos padres suben fotos de sus hijos a estas plataformas sin tener en cuenta las posibles consecuencias para la privacidad y el futuro digital de los menores. Aunque el marco legal actual reconoce el derecho de los menores a su propia imagen y contempla mecanismos de protección, no existe una regulación clara y específica que limite de manera efectiva esta práctica. Como comentamos en el Capítulo V, el Ministerio Fiscal cumple un papel fundamental como garante del interés superior del menor y puede instar medidas judiciales para proteger sus derechos. Sin embargo, en la práctica estas actuaciones suelen producirse únicamente cuando existe un conflicto entre los padres o una denuncia previa, lo que implica que no hay un control preventivo generalizado. Esto deja a muchos menores expuestos a riesgos digitales sin una tutela efectiva. En mi opinión, esta es una cuestión que refleja una carencia legal importante que debería corregirse a través de una normativa específica que regule el uso de la imagen de los menores en el entorno digital estableciendo límites y mecanismos de protección más eficaces.
7. Dese mi punto de vista, la sociedad actual no tiene suficiente conocimiento sobre las implicaciones de compartir nuestros datos personales en Internet. Muchas personas aceptan cookies y dan acceso a su información sin entender realmente cómo se utiliza

o qué riesgos conlleva. Por ello, propongo mejorar y promover la educación digital, explicando de manera clara los riesgos de una mala gestión de la privacidad. Esto ayudaría a que los usuarios sean más conscientes de la importancia de proteger sus datos y puedan tomar decisiones informadas sobre qué información compartir en Internet y Redes Sociales.

CAPITULO VII. BIBLIOGRAFÍA.

Agencia Española de Protección de Datos. (2020). *Guía sobre el uso de las cookies*. https://www.aepd.es/guias/guia-cookies.pdf

Agencia Española de Protección de Datos. (s.f.). *Menores y educación*. AEPD. https://www.aepd.es/preguntas-frecuentes/10-menores-y-educacion

Alviarez Figueroa, Ó. E. (2018). *El derecho a la propia imagen del menor en la era de las redes sociales* [Trabajo de fin de grado, Universidad de La Laguna]. RIULL. https://riull.ull.es/xmlui/bitstream/handle/915/10344/El%20derecho%20a%20la%20propia%20imagen%20del%20menor%20en%20la%20era%20de%20las%20redes%20sociales.pdf?sequence=1&isAllowed=y

Beca, J. P. (2011). *Confidencialidad y secreto médico*. Centro de Bioética, Universidad del Desarrollo. https://medicina.udd.cl/centro-bioetica/noticias/2011/04/14/confidencialidad-y-secreto-medico/

BVerfG. (1999). *Sentencia sobre la privacidad de los datos personales*. Tribunal Constitucional Federal de Alemania.

Congreso de los Diputados. (s.f.). *Información sobre las cookies*. https://www.congreso.es/cookies

Cristòfol Daudén-Esmel, J., Castellà-Roca, J., & Viejo, A. (2022). *Sistema para la gestión automática de las políticas de privacidad de los sitios web*. En *Actas de las XVIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2022)*. https://recsi2022.unican.es/wp-content/uploads/2022/11/Cristofol-Dauden-Sistema-para-la-gestion-automatica-de-las-politicas-de.pdf

Cuadrada, E. B. (2007). *La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. IDP. Revista de Internet, Derecho y Política*, (5), 78–92. https://dialnet.unirioja.es/servlet/articulo?codigo=2372618

De las Heras Vives, L. (2018). El derecho a la propia imagen en España. Un análisis desde el derecho constitucional, civil y penal. *Actualidad Jurídica Iberoamericana*, (8), 435–464. https://idibe.org/wp-content/uploads/2018/03/991.DelasHeras.pdf

Dopazo Fraguío, P. (2019). Protección de datos y derechos digitales: arquitectura del nuevo binomio regulatorio. *Derecom*, (26), 17–48. https://dialnet.unirioja.es/descarga/articulo/7064728.pdf

El Derecho. (2021, 15 septiembre). *¿Cuáles son las posibles consecuencias legales para los progenitores por la publicación de fotos de sus hijos menores de edad en redes sociales?* https://elderecho.com/posibles-consecuencias-legales-los-progenitores-la-publicacion-fotos-hijos-menores-edad-redes-sociales

Europa Press. (2023, febrero 15). *El Supremo avala publicar imágenes de hijos menores aunque sea solo con el consentimiento de un progenitor*. https://www.europapress.es/nacional/noticia-supremo-avala-publicar-imagenes-hijos-menores-sea-solo-consentimiento-progenitor-20230215152939.html

Fried, C. (1968) "Privacy", *The Yale Law Journal, núm. 77, pp. 475-493, p. 482.* https://doi.org/10.2307/794941

Gutiérrez-David, M.-E. (2014). *Intimidad y propia imagen: los ecos del common law americano y la evolución de la jurisprudencia constitucional española*. *Derecom*, (18), 85–108. https://revistas.ucm.es/index.php/DERE/article/view/94274

Guzmán Hernández, C. A. (2014). *El derecho a la propia imagen en el entorno digital: Una mirada desde el marco jurídico colombiano*. *Revista CES Derecho, 5*(2), 142–159. https://www.redalyc.org/pdf/788/78824460006.pdf

Herrán Ortíz, A. I. (2003). *El derecho a la protección de datos en la sociedad de la información*. *Cuadernos de Deusto de Derechos Humanos*, (26), 9–11.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2018). *Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* [PDF]. https://inicio.inai.org.mx/nuevo/convenio108.pdf

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Transactions on the Web, 64*(8), 98–106. https://doi.org/10.1145/3466722

Luño, A. E. P. (1981). Informática y libertad: Comentario al artículo 18.4 de la Constitución. Revista de estudios políticos, (24), 31-54.

Manny, C. (2003). La intimidad de la Unión Europea y la seguridad de los Estados Unidos: la tensión entre la ley europea de protección de datos y los esfuerzos por parte de Estados Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros. *Cuadernos de Derecho Público*.

Martín Critikián, D. y Medina Núñez, M. (2021). *Redes sociales y la adicción al like de la generación z. Revista de Comunicación y Salud*, 11, 55-76. https://doi.org/10.35669/rcys.2021.11.e281

Martínez de Aguirre Aldaz, C. (2024). *El derecho a la intimidad, revisitado* Actualidad Jurídica Iberoamericana Nº 20, febrero 2024, ISSN: 2386-4567, pp. 76-105.

Martínez López-Sáez, M., "La ratificación Española del Convenio 108+: Consideraciones jurídicas básicas del nuevo marco paneuropeo de protección de datos", *Revista General de Derecho Europeo 54, 2021.*

Moraga, Á. L. R. (2004). Censura en la red: restricciones a la libertad de expresión en internet. *VV. AA., Prensa y periodismo especializado II, Guadalajara.*

Murillo de la Cueva, P.L. (2009). La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad. El Derecho a la Autodeterminación Informativa (Madrid, Fundación Coloquio Jurídico Europeo). https://www.fcjuridicoeuropeo.org/wp-content/uploads/file/jornada15/1_LUCAS_1.pdf

Porras, A. J. G. (2016). Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica*. La vigilancia masiva. Doctoral dissertation, Universidad de Castilla-La Mancha.*

Rallo Lombarte, A. (2017), "De la <<libertad informática>> a la constitucionalización de nuevos derechos digitales (1978-2018)", *Revista de Derecho Político- UNED*, núm. 100, p. 642.

Rebollo Delgado, L.: "Encuesta sobre la protección de datos personales", *Teoría y Realidad Constitucional (UNED),* núm. 46, 2020.

RedIPD. (2022, noviembre 30). *Se convirtió en ley la aprobación del Convenio 108+*. RedIPD. https://www.redipd.org/noticias/se-convirtio-en-ley-la-aprobacion-del-convenio-108

Riutort, J. F. (2021). La función publicitaria de las cookies: mecanismos de prevención y cautela en el Derecho Español. *THEMIS: Revista de Derecho*, (79), 127-140.

Roca, A. P. (2022). Privacidad, intimidad y protección de datos: una mirada estadounidense y europea. *Derechos y Libertades, (47), 307-338.*

Saiz, M. (s.f.). *Exposición de menores en redes sociales*. Legálitas. Recuperado de https://www.legalitas.com/actualidad/menores-en-redes-sociales:contentReference[oaicite:53]{index=53}:contentReference[oaicite:54]{index=54

Saldaña Díaz, M. N. (2011). *El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego*. *Teoría y Realidad Constitucional*, (28), 279–312. https://dialnet.unirioja.es/servlet/articulo?codigo=3883001

Schwab, K. (2020). La cuarta revolución industrial. *Futuro hoy*, *1*(1), 06-10.

Soler García, I. (2019). *Protección de datos y privacidad: Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos*. *Revista de Derecho UNED (RDUNED)*, (24), 255–281. https://revistas.uned.es/index.php/RDUNED/article/view/27017/21093

Tachon, F. (2021). *La protección de la privacidad en Francia: del derecho de imagen a la privacidad digital*. Ediciones del Derecho.

Talciani, H. C. (2000). Configuración Jurídica del Derecho a la Privacidad I: Origen, Desarrollo y Fundamentos. *Revista chilena de derecho*, 27, 51.

Tomás Mallén, B., "Las Sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108+ del Consejo de Europa", *El Reglamento General de Protección de Datos: un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales,* Tirant Lo Blanch, Valencia, 2019, pp. 59-60.

Toral Lara, E. (2020). *Menores y redes sociales: consentimiento, protección y autonomía*. Derecho Privado y Constitución, 36, 179–21

Torres Díaz, M. C. (2011). Privacidad y tracking cookies. Una aproximación constitucional.

Unión Europea. (s.f.). *Protección de datos (RGPD)*. Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Vélez, J. J. C. (2021). Derecho a la privacidad en la era de la digitalizacion y del blockchain. Práctica de tribunales: revista de derecho procesal civil y mercantil, (149), 3.

Vic-Liu. "Lista de sitios web y aplicaciones bloqueadas en China en 2024". Let´s Chinese, 2024 (disponible en https://letschinese.com/es/lista-de-sitios-web-y-aplicaciones-bloqueados-en-china/ ; última consulta 30/01/2025).

Zarsky, T. Z. (2019). Privacy and manipulation in the digital age. *Theoretical Inquiries in Law, 20(1), 157-188*

Figuras

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. ACM Transactions on the Web (TWEB), 20:5.

Jurisprudencia

Sentencia de la Audiencia Provincial de Pontevedra, Sección 1ª, 208/2015, de 4 de junio. Recuperado de CENDOJ, Roj: SAP PO 208/2015 - ECLI: ES:APPO:2015:208.

Audiencia Provincial de Barcelona, Sección 18ª, 265/2015, de 22 de abril. Recuperado de CENDOJ, Roj: SAP B 4797/2015 - ECLI: ES:APB:2015:4797.

Sentencia de la Audiencia Provincial de Barcelona, Sección 18ª, 360/2017, de 25 de abril. Recuperado de CENDOJ, Roj: SAP B 360/2017 - ECLI: ES:APB:2017:360.

Sentencia Audiencia Provincial de Cantabria, Sección 2ª, 24/2020, de 13 de enero. Recuperado de CENDOJ, Roj: SAP CA 24/2020 - ECLI: ES:APCA:2020:24.

Sentencia del Tribunal Constitucional 170/1987, de 30 de octubre. HJ. 1987:170.

Sentencia del Tribunal Constitucional 231/1988, de 2 de diciembre. HJ. 1988:231.

Sentencia del Tribunal Constitucional 254/1993, de 18 de agosto. HJ. 1993:254.

Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre. HJ. 1999:202.

Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre. FJ 7º. HJ. 2000:292.

Sentencia del Tribunal Constitucional 119/2001, de 24 de mayo. HJ. 2001:119.

Sentencia del Tribunal Constitucional 156/2001, de 26 de julio. FJ 3º. HJ. 2001:156.

Sentencia del Tribunal Supremo 44/1989, de 20 de febrero. VLEX 75826313.

Sentencia del Tribunal Supremo 1003/2008, de 23 de octubre. Roj: STS 5554/2008 - ECLI: ES:TS: 2008:5554.

Sentencia del Tribunal Supremo 1004/2008, de 23 de octubre. Roj: STS 5704/2008 - ECLI: ES:TS: 2008:5704.

Sentencia del Tribunal Supremo 249/2023, de 14 de febrero. Recuperado de CENDOJ, Roj: STS 249/2023 - ECLI: ES:TS:2023:249.

Sentencia del Tribunal de Justicia de la Unión Europea de 1 de octubre de 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände -

Verbraucherzentrale Bundesverband eV contra Planet49 GmbH, C-673/17, ECLI:EU:C:2019:801.

Legislación

Código Civil de España, aprobado por Real Decreto de 24 de julio de 1889, BOE núm. 206, 27 de julio de 1889.

Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, BOE 15 noviembre 1985, No. 282.

Constitución Española, 29 de diciembre de 1978, BOE núm. 311.

Ley Orgánica 1/1982, de 5 de mayo, BOE núm. 115, 14 de mayo de 1982 (Protección civil del derecho al honor, a la intimidad y a la propia imagen).

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, BOE núm. 261, 30 de octubre de 1992.

Ley Orgánica 1/1996, de 15 de enero, BOE núm. 15, 17 de enero de 1996 (Protección Jurídica del Menor).

Ley Orgánica 12/1999, de 13 de diciembre, de protección de datos personales y garantía de los derechos digitales, BOE núm. 298, 14 de diciembre de 1999.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, BOE núm. 166, 12 de julio de 2002.

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 (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), DOUE L 119, 4 de mayo de 2016.