Universitat Autònoma de Barcelona

Dipòsit digital de documents de la UAB

This is the **published version** of the bachelor thesis:

Estrada De la Parte, Ana Lin; Martinez Quirante, Roser, dir. El ciberderecho como disciplina jurídica. 2023. (Pla d'Estudis d'Administració i Direcció d'Empreses Dret)

This version is available at https://ddd.uab.cat/record/287191

under the terms of the BY-NC-ND license

Universitat Autònoma de Barcelona

Facultat de Dret

TÍTULO: El ciberderecho como disciplina jurídica

AUTORA: Ana Lin Estrada de la Parte.

GRADO: ADE + Derecho.

TUTORA: Roser Martínez Quirante.

FECHA DE ENTREGA: 8 de mayo de 2023.

ÍNDICE

ABSTRACT **1**

1. INTRODUCCIÓN: LA TRANSFORMACIÓN TECNOLÓGICA Y LA IMPORTANCIA DE LOS DATOS **2**

2. EL CIBERDERECHO Y SUS BASES ESTRUCTURALES **4**

2.1 ¿QUÉ ES EL CIBERESPACIO? 4
2.2 ORIGEN Y NECESIDAD DE DESARROLLAR LOS DERECHOS DIGITALES 5
2.3 MODELOS DE REGULACIÓN DEL CIBERESPACIO 7
2.4 PRINCIPIOS GENERALES DEL CIBERDERECHO 9

3. EL CONTENIDO DEL CIBERDERECHO **17**

4. LA PROTECCIÓN DE LOS DATOS EN EL CIBERESPACIO **24**

4.1 LA PERSONALIDAD VIRTUAL DEL USUARIO DE INTERNET 24
4.2 EL *BIG DAT*A Y LOS DATOS PERSONALES 25
4.3 REGLAMENTO (UE) 2016/679: DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 26
4.4 LA LOPD. COMENTARIO SOBRE LOS DERECHOS DIGITALES EN ESPAÑA 31
4.5 EL DERECHO AL OLVIDO DIGITAL 32

5. CIBERCRIMEN **37**

5.1 TIPOS DE CIBERCRÍMENES 39
5.1.1 Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos *40*
5.1.2 Delitos asociados a la informática *41*
5.1.3 Delitos de contenido *41*
5.1.4 Delitos relativos a las infracciones contra la propiedad intelectual y derechos conexos *42*
5.2 DISCUSIÓN ENTRE EL *HARD* Y EL *SOFT LAW* 43

6. CONCLUSIONES **44**

7. REFERENCIAS Y BIBLIOGRAFÍA **45**

7.1 NORMATIVA 45
7.2 JURISPRUDENCIA 47
7.3 ARTÍCULOS, OBRAS Y TEXTOS JURÍDICOS 48
7.4 PÁGINAS WEB Y OTROS DOCUMENTOS 53

ABSTRACT

Hoy en día, es indudable la globalización que existe y lleva existiendo desde hace unas décadas en nuestra sociedad. Por ello, era imperativo encontrar una manera para poder mantener dicha conectividad dentro de los parámetros del Estado de derecho. Como sociedad, nos hemos apoyado en el avance de la tecnología y hemos encontrado un espacio para relacionarnos aun estando a grandes distancias que habría sido impensable en otra época: Internet. Este espacio permite la omnicanalidad en la que estamos inmersos—esto es el acceso a éste desde los diferentes dispositivos inteligentes a través de los cuales operamos.

Asimismo, la existencia de una comunidad virtual que es capaz de contener una ingente cantidad de información y datos debe tener algún tipo de supervisión, puesto que cabe la posibilidad de que tengan lugar varios escenarios que deben poder resolverse en base a unos parámetros fijos. Para ello, hemos reconocido una regulación específica a la que hemos denominado ciberderecho o derecho digital.

El presente proyecto tiene como objeto el estudio del derecho digital, así como las amenazas que pueden surgir y los mecanismos para prevenir peligros y riesgos.

Palabras clave: connectividad, Internet, datos, ciberderecho, derecho digital.

Nowadays, there is no doubt that globalization exists and has existed since some decades ago in our society. That is why it was imperative to find a way to be able to keep this connectivity inside the parameters of the State of Law. As a society, we have relied on the technology advances and have found a space to keep in touch despite the distance that would have been impossible to achieve in another period of time: the Internet. This space allows us to operate through the multiplicity of smart devices that are at our disposal.

However, the existence of a virtual community that is able to contain a huge amount of information and data must have some kind of supervision, given that there is a high probability that some situations happen and they should be able to be solved on the basis of established parameters. Thus exists what we have identified as cyberlaw or digital law.

The present project has as an object of study the digital law, as well as the possible threats that can emerge and the mechanisms to prevent them.

Keywords: connectivity, Internet, data, cyberlaw, digital law.

1. Introducción: la transformación tecnológica y la importancia de los datos

Resulta incontestable que ya hace una década que el Internet y los dispositivos inteligentes se han normalizado en nuestra sociedad, cada vez más digitalizada, y forman parte de nuestro día a día. Cabe recordar que, antes de esta revolución tecnológica, disponíamos de varios dispositivos para realizar llamadas telefónicas, ver la televisión, grabar vídeos o escuchar música[1]. Ahora, todo eso es posible a través de un solo dispositivo gracias a Internet.

Lo que se denomina «tecnocultura» es predominante e irrefutable[2]. Es lógico, pues, que con el uso constante de los dispositivos inteligentes se llegue a procesar un gran volumen de datos—los cuales, en ocasiones, son sensibles[3]—sobre todo, teniendo en cuenta que la economía, hoy en día, está cada vez más basada en los datos. En este sentido, se ha llegado a señalar en *The Economist* que «*el recurso más valioso del mundo ya no es el petróleo, sino los datos*» y «*si los gobiernos no quieren una economía de datos dominada por unos pocos gigantes, deberán actuar pronto*» por lo que «*el derecho administrativo está llamado a actuar para prevenir estas amenazas monopolistas a la seguridad y la privacidad*»[4].

Ciertamente, la información personal ha devenido en objeto de competencia para las empresas, las cuales la contemplan como «materia prima para los modelos de negocios digitales»[5]. El hecho de que los datos que se recogen en la Red lleguen a ser tan determinantes hace que se planteen cuestiones como las siguientes: ¿se informa a los usuarios de manera efectiva sobre el uso de estos datos? ¿Qué se hace con esa información una vez ya ha sido analizada? ¿Se ve vulnerado el derecho a la intimidad de las personas u otros derechos paralelos? En este sentido, se hace necesario conciliar la preservación de los derechos fundamentales con los avances que

---

[1] Mueller, M. N. (2010). *Networks and States. The Global Politics of Internet Governance*. The MIT Press.

[2] Aranda, F. J. (2021) *Derecho y nuevas tecnologías: la influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español*. Dykinson, S.L.

[3] Leo-Castla, J.I. (2019, octubre 4). Compliance y gestión del riesgo normativo en el contexto del Reglamento europeo de protección de datos. *La Ley.* Sección Ciberderecho, núm.32. Recuperado el 8 de diciembre de 2022 de https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAEAC1NwW7CMAz9GnJBmtqxipMvXY8IIah2dxMrjRRiSJxC_37ewPKT_eT3_O6V8jrSU8CyC563N0oYTVkTp_UKY65kBKcCzWZvW8WnQSsV48AWvvZ_JCw04gSN4ewo96tuwoLxTAXatutMmflxxCV4lMCpx_x6G5yDYWy0dtptZxbKRQXwEzwlITMHPx8U8tIXwmznE3oCDa9X1fAHltvzfemriLonSZd_bmzUOaDQN0ZK7p37C14AdqryAAAAWKE

[4] Martínez-Quirante, R., y Rodríguez-Álvarez, J., (2019). *Towards a new AI race. The challenge of lethal autonomous weapons systems (LAWS) for the United Nations* (p.110). Thomson-Reuters Aranzadi.

[5] El tratamiento de esta información, puede servir para mejorar los productos o servicios y la publicidad de las empresas. Esto puede ser determinante para aumentar los beneficios. Barrón Arniches, P. (2019): La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales), *Cuadernos europeos de Deusto*, 61 (pp. 33-34).

se realizan en el ámbito del flujo de la información a través de canales digitales. Un aspecto no excluye el otro y se debe procurar que ambos coexistan y que este equilibrio se respete ahora más que nunca, ya que nunca hemos estado tan expuestos a las amenazas que pueden llegar a surgir.

En todo caso, los autores advierten que «*el análisis, la vigilancia y la acumulación masiva y pormenorizada de datos a través de sistemas inteligentes están conduciendo a cambios en la gobernanza y daños en el núcleo de la sociedad civil. Nos referimos a lo que McQuillan denomina la implantación de estados de excepción algorítmicos*»[6].

[6] Martínez Quirante, R. y Rodríguez Álvarez, J. (2018). *Inteligencia artificial y armas autónomas letales* (p.108). Trea.

2. El ciberderecho y sus bases estructurales

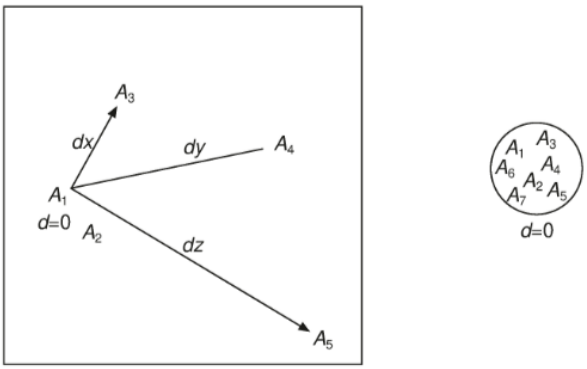
2.1 ¿Qué es el ciberespacio?

Moisés Barrio Andrés, especialista en derecho digital, define el ciberespacio como «*el espacio global en el entorno de la Sociedad de la Información que consiste en el conjunto interdependiente de infraestructuras de TIC, y que incluye a Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados propios del Internet de las Cosas (IoT)*»[7]. Con esta definición, se desprende que, a pesar de ser un espacio virtual, se requieren medios físicos como ordenadores o dispositivos inteligentes que permitan conectar el ciberespacio con el mundo físico, aunque los actos que se desempeñen en dicho mundo virtual no sean actos físicos como tal. Asimismo, mientras que para las relaciones en el espacio físico se requiere una cercanía entre emisor y receptor, en el ciberespacio la comunicación puede tener lugar independientemente de la distancia a la que se sitúen emisor y receptor[8].

Gráfico 1

Contracción de la distancia en el ciberespacio y expansión de la capacidad comunicativa: a_1 necesita d = 0 para comunicarse con a_2, a_3, a_4, etc.

ESPACIO FÍSICO **CIBERESPACIO**



De *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio* (p. 148), por F. Miró Llinares, 2012, Marcial Pons Ediciones Jurídicas y Sociales. Copyright 2012 por Fernando Miro Llinares.

Como se muestra en el gráfico, la distancia no supone un obstáculo en el ciberespacio, por lo que encontramos una contracción de espacio y de tiempo, puesto que pueden tener lugar eventos de forma mucho más rápida en el mundo virtual que en el real[9].

---

[7] Barrio Andrés, M. (2018). *Ciberderecho: Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*. Tirant lo Blanch.

[8] Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons Ediciones Jurídicas y Sociales. Recuperado el 28 de abril de https://elibro.net/es/ereader/uab/58741?page=26

[9] Wellman, B. (2001), Computer networks as social net- works, en *Science*. 293 (p. 2034).

Es comprensible que con la transformación digital que hemos presenciado—y seguimos presenciando—se haya creado un espacio en el que el conjunto de interacciones sociales se concentren. Esto implica que las antiguas formas de control y abordajes que realice la ley sobre el mundo digital resulten obsoletas, nulas e ineficaces[10].

Una vez entendido este concepto, podemos proceder a analizar las siguientes cuestiones.

2.2 Origen y necesidad de desarrollar los derechos digitales

La digitalización aún sigue avanzando e influyendo cada vez más aspectos de nuestro día a día. De hecho, la Comisión Europea, en febrero de 2020, observó que «*la comunicación digital, la interacción en redes sociales, el comercio electrónico y las empresas digitales se están consolidando y transforman nuestro mundo*». Esto, pues, es señal de que se requiere una regulación respecto a la transformación digital que proteja a los individuos y respete sus valores[11]. Con la pandemia de la COVID-19, este proceso se ha acelerado pero también ha establecido retos fundamentales en el ámbito de la digitalización[12].

Uno de los principales objetivos de la tecnologización que estamos viviendo es asegurar que los derechos de los ciudadanos se respeten en el entorno digital de la misma manera que se preservan fuera de él. El concepto de los «derechos digitales», pues, abarca tanto los derechos fundamentales como los ordinarios. Teniendo en cuenta cómo está construido el mundo digital, cabe plantearse cómo proteger de la manera más óptima dichos derechos, puesto que es evidente la falta de entereza de la regulación jurídica que acompaña a la nueva realidad digital. Ésta se manifiesta en la vigilancia de nuestros movimientos o comportamientos en el ciberespacio en tiempo real, la consolidación de monopolios que perjudican la competencia en el mercado digital e incluso la aparición de ciberdelitos que afecten a los ciudadanos.

Para poder comprender por qué se necesita clarificar las fronteras de los derechos digitales en nuestro ordenamiento jurídico y en los regímenes internacionales, hay que comentar los que se prevén actualmente en las normativas. En España, cabe destacar que nuestra Constitución fue

---

[10] Penney, J.W (2009). Understanding the New Virtualist Paradigm. *Journal of Internet Law*. Recuperado el 18 de diciembre de 2022 de https://ssrn.com/abstract=1355392.

[11] Comisión Europea (2020, 19 de febrero), *Shaping Europe's Digital Future.* COM. 67 (p. 2). Recuperado el 20 de diciembre de https://eufordigital.eu/wp-content/uploads/2020/04/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[12] Faraj, S.; Renno, W.; Bhardwaj, A. (2021). Unto the Breach: What the COVID-19 Pandemic Exposes about Digitalization. *Journal of Information and Organization*, 31(1), artículo 100337. Recuperado el 20 de diciembre de 2022 de https://doi.org/10.1016/j.infoandorg.2021.100337

pionera en contemplar en su artículo 18.4 garantías respecto a este ámbito: «*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*.»

Barrio comenta que esta referencia constitucional viene influenciada por el libro de Orwell *1984*, pues evidencia «*el temor de que el uso generalizado de la informática pudiera desembocar en un descontrol de tales conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*»[13]. En base a este precepto, el ciudadano puede oponerse a las instituciones traten sus datos personales con objetivos diferentes a los que justificaban la obtención de ellos.

Como podemos observar, cierto es que este artículo asentó la base de la necesidad de protección frente a los avances tecnológicos vinculados a la informática por aquel entonces y a las nuevas tecnologías en los tiempos actuales. Sin embargo, la existencia de un derecho fundamental a la protección de datos no es suficiente y cabe plantearse la necesidad de instaurar un nuevo marco jurídico que vele por los derechos de los ciudadanos en esta nueva era digital.

Por otro lado, en el caso de EE.UU, por ejemplo, el marco legal respecto a la cuestión objeto de estudio es más complejo. Hay que partir del hecho que en EE.UU no existe legislación nacional (federal) que regule el Internet o la recaptación, el almacenamiento y el uso de datos personales *online*. Por este motivo, los juzgados tienen dificultades para resolver estas cuestiones, las cuales se presentan con frecuencia.

En EE.UU, entonces, el marco legal está compuesto de 1) preceptos constitucionales; 2) un conjunto de leyes y reglamentos federales y estatales adoptados a lo largo del tiempo y en respuesta a diferentes situaciones y problemas; 3) pautas y principios desarrollados por agencias gubernamentales y grupos de la industria que no tienen fuerza de ley pero forman parte de marcos autorreguladores que se consideran como «*best practices*», es decir, buenas prácticas[14].

En cuanto a las previsiones constitucionales, cabe comentar que la Constitución de EE.UU, a pesar de ser del siglo XVIII, engloba varios de las cuestiones presentadas con el uso del Internet.

[13] Barrio Andrés, M. (2021). Génesis y desarrollo de los derechos digitales. *Revista de las Cortes Generales*, p.197-233. Recuperado el 24 de diciembre de 2022 de: https://doi.org/10.33426/rcg/2021/110/1572

[14] Las buenas prácticas son los métodos y procesos demostrados de una empresa.

La primera enmienda protege la libertad de expresión, de prensa y de reunión[15], mientras que la cuarta protege de un registro y allanamiento poco razonable[16]. Su aplicación al acceso y uso del Internet resulta, evidentemente, un ejercicio de interpretación complejo.

Respecto a las leyes federales, es de especial interés comentar que algunas se aplican específicamente a actividades que tratan información personal—como telemarketing y e-mail comercial—[17], mientras que otras protegen determinadas categorías de información—como finanzas o salud[18]. Las tres leyes federales más relevantes respecto a los desarrollos de Internet son la Ley de privacidad de comunicaciones electrónicas (1986), la Ley de comunicaciones almacenadas (1986) y la Ley de decencia en las comunicaciones (1996)[19].

EE.UU abarca numerosos principios y normativas respecto a la privacidad. No obstante, tal y como se ha mencionado con anterioridad, no es un marco jurídico unificado y está más bien disperso.

En definitiva, si se observa el marco legal del que disponemos actualmente, se puede llegar a la conclusión de que es hora de una renovación jurídica que pueda ser capaz de resolver los retos que se presentan en la actualidad para poder, así, proteger y preservar los derechos de los ciudadanos.

2.3 Modelos de regulación del ciberespacio

Es innegable la problemática que surge con el ciberderecho: la globalidad de Internet. No obstante, ello no impide que el derecho y el Estado tengan presencia en la regulación de la Red. Esto implica que esa primera idea que puede surgir de la existencia de un ciberespacio libertario, sin influencia de derecho y Estado de ningún tipo, resulta una hipótesis que claramente no se cumple en la realidad.

---

[15] «*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*.» Constitución de EE.UU, primera enmienda [en línea]. Recuperado el 26 de diciembre de 2022 de: https://www.archives.gov/founding-docs/constitution

[16] «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause […] particularly describing the place to be searched, and the persons or things to be seized*.» Constitución de EE.UU, cuarta enmienda. Recuperado el 26 de diciembre de 2022 de: https://www.archives.gov/founding-docs/constitution

[17] Por ejemplo, la *Privacy Act of 1974*. Recuperado el 26 de diciembre de 2022 de: https://www.justice.gov/opcl/privacy-act-1974

[18] Por ejemplo, la *Gramm-Leach-Bliley Act,* también conocida como la *Financial Services Modernization Act of 1999*. Recuperado el 26 de diciembre de 2022 de https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

[19] Stewart, D. (2018). Recent Developments in U.S. Cyberlaw. *Agenda internacional*, 25(36), p.113.

Por ese motivo, uno de los modelos de regulación defiende la extensión de la soberanía territorial de los Estados al ciberespacio: la territorialización del ciberespacio. Este se manifiesta mediante la legislación fiscal, de propiedad intelectual o de protección de datos, puesto que la aplicación de las normativas de los diferentes ordenamientos jurídicos será posible siempre que se pueda conocer la localización geográfica de los usuarios y páginas web, los cuales están establecidos en determinados lugares físicos que pertenecen al territorio de un Estado.

No obstante, hay algunos expertos del sector que afirman que el diseño de la Red obliga a los gobiernos a promulgar legislaciones poco restrictivas. Esto se podría ver reflejado en el caso del comercio electrónico, en el cual las empresas tienen una tendencia a establecerse en Estados que cuentan con ordenamientos jurídicos que les resultan más convenientes y favorables, así como con menos obstáculos a nivel regulatorio. En este mismo sentido, también se ha observado que regulaciones demasiado restrictivas pueden conllevar a una economía digital mucho menos competitiva e innovadora.

El segundo modelo se fundamenta en la idea de que la regulación del ciberespacio debe reposar en los convenios internacionales creados entre Estados. Sin embargo, debido a que los Estados se siguen mostrando reacios a someterse a normas jurídicas creadas en otros, este modelo no tiene demasiados logros atribuidos; aun así, se puede encontrar en materias como el cibercrimen[20] o la transferencia internacional de datos[21].

El tercer modelo defiende la creación de nuevos organismos internacionales que se hagan cargo de la regulación del ciberespacio, ya que se entiende la regulación del ciberespacio como una responsabilidad global; por ello, se busca la cooperación y coordinación entre diferentes países y organismos internacionales. El modelo busca evitar la fragmentación y el conflicto en la regulación del ciberespacio, así como promover un enfoque armonizado y global. Ya existen algunas organizaciones que están funcionando con éxito: la *Internet Corporation for Assigned Names and Numbers* (ICANN), el *World Wide Web Consortium* (W3C) o la *Internet Society* (ISOC).

[20] Convenio sobre la Ciberdelincuencia del Consejo de Europa, hecho en Budapest el 23 de noviembre de 2001. Ratificado por España el 20 de mayo de 2010. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[21] Convenio 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. Ratificado por España el 27 de enero de 1984. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

La ICANN[22] se creó en 1998 como una organización supuestamente sin ánimo de lucro amparada por el derecho de EE.UU para supervisar, principalmente, los nombres de dominio y de las direcciones de IP de Internet.

El *World Wide Web Consortium*[23], por su parte, se creó como un consorcio de empresas y entidades miembros que coordina la fijación de estándares técnicos de la web.

Finalmente, la ISOC[24] es una asociación internacional no gubernamental y sin ánimo de lucro para la promoción del uso de Internet.

El cuarto modelo plantea la posibilidad de regular directamente la arquitectura del ciberespacio, es decir poder generar efectos regulatorios aprovechando el código de la Red. De esta manera, el ciberespacio se regiría no solo en virtud de las normas jurídicas, sino también por su estructura. Así, mientras se regula la arquitectura, también se regula la Red, haciéndola más o menos abierta—ahora mismo, el ciberespacio es abierto debido a la falta de centralización de la Red.
Este modelo resulta un tanto controvertido, dado que la regulación de la arquitectura del ciberespacio no es muy práctica en el sentido de que se acabarían generando colisiones con otros ordenamientos normativos.

Cabe decir que la Unión Europea emplea los cuatro modelos de regulación explicados. Sin embargo, hay que tener en cuenta que el hecho de que estos modelos coexistan no quiere decir que la UE sea un regulador neutral ni se asegure un ciberespacio libre. Aquí hay que tener en consideración también que Internet fue originado en los Estados Unidos, por lo que la mayoría de su regulación—así como los problemas que pueden llegar a surgir—recaen sobre su ordenamiento jurídico. Por ello, las soluciones que se deben plantear, irremediablemente tienen que incluir una especial atención al derecho norteamericano.

2.4 Principios generales del ciberderecho

Es necesario entender qué se entiende por «principios generales». Debemos comprenderlos como las bases que cimientan el ciberderecho, esenciales debido a la ausencia de un marco legal global coherente que aborde adecuadamente los nuevos desafíos que plantea la Red.

[22] ICANN. Recuperado el 5 de febrero de 2023 de https://www.icann.org/es/system/files/files/getting-to-know-icann-quicklook-30apr20-es.pdf
[23] World Wide Web Consortium. Recuperado el 5 de febrero de 2023 de https://www.w3.org/
[24] ISOC. Recuperado el 5 de febrero de 2023 de https://www.internetsociety.org/es/about-internet-society/

A pesar de que hay algunos principios que son de común acuerdo, no se ha establecido una lista que los recoja todos de manera internacional. Por ello, comentaremos algunos de los más asentados en el ciberespacio.

1. *Principio de libertad de expresión en el ciberespacio*

   La libertad de expresión es una de las máximas directrices en el ciberespacio y, probablemente, el principio más discutido en la Red. ¿Quién no ha debatido sobre el *tweet* de alguna figura pública opinando sobre un tema controvertido? Como podemos imaginar, el ciberespacio tiene un gran impacto en la libertad de expresión, puesto que éste permite a las personas comunicar y compartir sus ideas a nivel global, independientemente de su ubicación geográfica. Además, la viralidad de las redes sociales y otras plataformas en línea permite que los mensajes se propaguen y alcancen una audiencia mucho más amplia que en otros medios de comunicación tradicionales.

   La libertad de expresión en el ciberespacio se fundamenta en el derecho a la libertad de pensamiento y de opinión, el cual cabe recordar que está reconocido en varios tratados internacionales de derechos humanos, como la Declaración Universal de DDHH, la Convención Americana sobre DDHH, la Carta Africana de DDHH y la Convención Europea de Derechos Humanos (CEDH).

   La libertad de expresión en el ciberespacio también se basa en la idea de que el acceso a la información y la capacidad de compartir ideas y opiniones libremente en línea son fundamentales para el desarrollo democrático y la promoción de los derechos humanos en todo el mundo[25]. Sin embargo, ¿hasta qué punto se extiende esta libertad de expresión? Actualmente, el debate gira entorno a los límites que se establecen; la libertad de expresión en el ciberespacio no es absoluta, puesto que puede estar sometida a restricciones como la protección de los derechos de otros, la seguridad nacional, el orden público y la moralidad pública. Por este motivo, hay que encontrar un equilibrio adecuado entre la protección de los derechos y la libertad de expresión en línea.

   a. *El derecho al acceso al Internet*. Con el principio de libertad de expresión ha surgido el planteamiento del derecho a acceder a Internet de manera libre, abierta y sin restricciones injustificadas[26]. Este derecho ya está reconocido por la ONU, ya que se caracteriza como un elemento fundamental para poder poner en

[25] MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for internet freedom* (p. 135). Basic Books.
[26] Wu, T. (2011). *The master switch: The rise and fall of information empires* (p. 311). Vintage Books.

práctica otros derechos como la libertad de expresión, la educación, la información, la participación ciudadana y la innovación.

2. *Principio de la neutralidad de la red*

Tal y como hemos señalado, Internet es un espacio abierto y libre en el cual cualquier usuario puede navegar y acceder al flujo de información existente. El principio de la neutralidad del ciberespacio establece el ciberespacio como tecnológicamente neutral respecto de la tecnología que se utiliza actualmente o que se pueda inventar en un futuro. Según este principio, todos los datos que circulan por Internet se deben tratar de igual forma, sin que los proveedores de servicios de Internet (ISPs) o cualquier otro actor con capacidad de influir en el flujo de información en línea puedan realizar discriminaciones.

Algunos expertos en el área han comentado las consecuencias que se generan con la falta de neutralidad en la Red. Por ejemplo, Susan Crawford expone que esta ausencia de neutralidad, en el caso de EE.UU, ha originado un mercado de telecomunicaciones oligopólico y perjudicial para los consumidores, dado que «*los proveedores de servicios de Internet pueden bloquear o ralentizar el tráfico de ciertos sitios o servicios, o dar prioridad a su propio contenido y servicios, lo que les da una ventaja injusta sobre la competencia*»[27]. Cabe tener en cuenta que, si los proveedores de servicios de Internet pueden bloquear o ralentizar ciertos tipos de tráfico, también pueden minar la capacidad de los innovadores para desarrollar nuevos productos y servicios[28].

El principio de neutralidad tecnológica, pues, tiene como objetivo evitar que el uso de la tecnología se realice de forma interesada por los fabricantes, la industria o los proveedores de servicios del ciberespacio con una finalidad excluyente. Resulta un principio clave de la arquitectura descentralizada de Internet, dado que, sin la neutralidad de la red, las empresas de telecomunicaciones pueden controlar el flujo de información en línea y limitar la capacidad de los usuarios para comunicarse libremente[29], así como también restringir la libertad de expresión y la capacidad de los ciudadanos para participar en el debate público[30].

---

[27] Crawford, S. (2013). Captive audience: *The telecom industry and monopoly power in the new gilded age* (pp. 113-114). Yale University Press.
[28] Van Schewick, B. (2012). *Internet architecture and innovation* (p. 100). MIT Press.
[29] Reed, D. (2009). *The end of end-to-end: Preserving the architecture of the internet in the broadband era* (p. 13). The Association for Computing Machinery.
[30] McChesney, R. (2013). Digital disconnect: *How capitalism is turning the internet against democracy* (p. 181). The New Press.

La norma de referencia en Europa es el Reglamento (UE) 2015/2120, por el que se establecen medidas en relación con el acceso a una internet abierta[31]. Este Reglamento establece el principio de que todo el tráfico de Internet debe ser tratado de forma igualitaria, sin discriminación alguna por parte de los proveedores de servicios de Internet (ISP). Así lo declara en su considerando 8, en el cual se establece que «*al prestar servicios de acceso a internet, los proveedores de dichos servicios deben dar un trato equitativo a todo el tráfico, sin discriminaciones, restricciones o interferencias, con independencia de quienes sean el remitente o el receptor y cualesquiera que sean el contenido, aplicación, el servicio o el equipo terminal. De conformidad con los principios generales del Derecho de la Unión y según jurisprudencia reiterada, no debe darse un trato diferente a situaciones comparables ni un trato similar a situaciones diferentes, a menos que tal trato este objetivamente justificado*.»

A pesar de que se crea que debe haber una neutralidad absoluta en la Red, lo cierto es que esto no puede cumplirse al ciento por ciento. Ello es debido a que una neutralidad perfecta—sin herramientas de control—acabaría resultando contraproducente para los usuarios. Se requiere, pues, una mínima regulación que pueda equilibrar los intereses tanto de los proveedores de los servicios de acceso a internet como de los individuos y que evite que las operaciones de la Red se empleen con fines exclusivamente comerciales que puedan perjudicar a los usuarios.

3. *Principio de la buena fe*

A pesar de que el principio de buena fe se relaciona, de primeras, con el derecho contractual, puede ser aplicado en varias situaciones que se dan en el ciberespacio: contratación electrónica, protección del consumidor y regulación de contenidos[32].

El tradicional principio de la buena fe, pues, se introduce en el ciberderecho mediante el deber de informar al usuario no solo de la tecnología empleada sino también de la obtención de los datos—así como su tratamiento. Dicha información se debe dar de manera clara, transparente y detallada, sin utilizar técnicas fraudulentas o engañosas. Esto es especialmente relevante en los casos de tratamiento de *big data* e inteligencia artificial, puesto que, en estos casos, la mayoría de ocasiones los usuarios no son conscientes de la recopilación de sus datos.

[31] Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015R2120

[32] Pauwels, E. (2011). El principio de buena fe en el derecho de Internet. *Revista de derecho privado*, (20), 63-89.

4. *Principio de privacidad*

El principio de privacidad, al igual que otros principios mencionados, también está contemplado por el Derecho internacional de los derechos humanos (art. 17 PIDCP y art. 8 CEDH). El derecho a la privacidad se entiende como un derecho fundamental de las personas a tener un control sobre su información personal y a mantener la confidencialidad de sus datos; busca proteger la decisión del cibernauta de poner a disposición de terceros su información con las pautas que este elija para, así, salvaguardar la confidencialidad, identidad, intimidad y secrecía de sus comunicaciones.

En la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 8 de abril de 2014[33] (caso *Digital Rights Ireland Ltd.* vs. Ministerio de Comunicaciones e Información de Irlanda y otros), se estableció la nulidad de la Directiva 2006/24/EC del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

A través de la sentencia, el TJUE consideró que la Directiva constituía una injerencia desproporcionada en los derechos fundamentales de los ciudadanos de la UE al imponer una obligación general de conservación de datos de todos los usuarios de servicios de comunicaciones electrónicas, sin tener en cuenta las personas cuya conducta pudiera ser objeto de investigación penal y aquellas que no lo fuesen.

Asimismo, el Tribunal acabó determinando que el conjunto de los datos que se obligaba a conservar por los operadores permitiría la obtención de datos relativos a la esfera privada de las personas (hábitos, lugares de residencia, relaciones sociales), lo que se traducía en una intrusión de la vida privada de los individuos y en una infracción de los derechos fundamentales a la privacidad y a la protección de datos personales, consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Por ello, el TJUE concluyó que, a pesar de que los fines que perseguía la Directiva eran de interés general, el legislador había excedido los límites del principio de proporcionalidad sin que hubiese medidas ni garantías adecuadas en la Directiva que limitasen el acceso de las autoridades competentes a los datos conservados, lo que podía dar lugar a su uso abusivo y al riesgo de violación de la privacidad de las personas.

5. *Principio de la cooperación jurídica internacional*

[33] Sentencia del Tribunal de Justicia de la Unión Europea, de 8 de abril de 2014, C-293/12. Recuperado de https://curia.europa.eu/juris/document/document.jsf;jsessionid=0A176C3D89F9EFC98B28C32B1C820D44?text=&docid=150642&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=3191586

Teniendo en cuenta la dimensión del ciberespacio, es evidente que la cooperación jurídica internacional es necesaria, dado que la Red traspasa fronteras. Es por ello por lo que los Estados deben colaborar de forma conjunta mediante actuaciones internacionales para poder lidiar con los retos que plantea el ciberespacio.

Los delitos que se producen en esta dimensión digital, normalmente, son cometidos por ciberdelincuentes a través de servidores en un Estado diferente a la persona afectada. Teniendo en cuenta esto, es lógico que se requiera una cooperación judicial coordinada entre Estados, dado que puede haber casos que exijan la investigación en más de una jurisdicción.

> La Resolución del Parlamento Europeo sobre la lucha contra la ciberdelincuencia[34], adoptada el 3 de octubre de 2017, fue un gran paso en la lucha contra el cibercrimen y la protección de los ciudadanos de la UE.
>
> En esta resolución, el Parlamento Europeo solicitó a los Estados miembros y a la Comisión Europea que reforzasen la cooperación judicial internacional y la coordinación en la lucha contra la ciberdelincuencia, especialmente, mediante el intercambio de información y de la colaboración entre autoridades nacionales y europeas: «*Destaca la importancia de una estrecha cooperación con terceros países en la lucha global contra la ciberdelincuencia, en particular, mediante el intercambio de mejores prácticas, las investigaciones conjuntas, la creación de capacidades y la asistencia jurídica mutua.*» (considerando 76, respecto a la cooperación mejorada con terceros países).
>
> Además, el Parlamento Europeo también instó a los Estados miembros a mejorar su capacidad para prevenir, detectar y responder a los ataques cibernéticos, así como a desarrollar y aplicar medidas efectivas para proteger a los ciudadanos de la UE contra el robo de datos, el acoso en línea, el *grooming*, la extorsión y otros tipos de delitos en línea.
>
> La resolución también subrayó la importancia de la formación y educación en materia de seguridad cibernética—tanto para los ciudadanos como para las empresas—e invitó a un mayor esfuerzo en la promoción de la concienciación sobre los riesgos cibernéticos y las mejores prácticas para proteger los datos personales.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, de 23 de noviembre de 2001, es el primer instrumento que propone una cooperación internacional entre Estados para investigar y perseguir penalmente los ciberdelitos.

[34] Resolución del Parlamento Europeo, de 3 de octubre de 2017, sobre la lucha contra la ciberdelincuencia (2017/2068(INI)). Recuperado de https://www.europarl.europa.eu/doceo/document/TA-8-2017-0361_ES.html

6. *Principio de seguridad*

Este principio se fundamenta en la integración de medidas de seguridad desde la fase inicial del diseño de sistemas, aplicaciones y dispositivos que operan en el ciberespacio. De esta manera, la seguridad está presente desde el principio del desarrollo de la tecnología, es decir, no sería un elemento añadido posteriormente.

Hoy en día, lo podemos ver presente especialmente en el Internet de las Cosas (IoT), en la protección de la información personal que se recopila y se comparte a través de los dispositivos IoT.

> El Internet de las cosas (IoT) ha sido definido de muchas maneras. Una de sus definiciones es la siguiente: «*una red mundial de objetos físicos interconectados que utilizan sensores y software para recopilar y compartir datos*»[35].
>
> El término «Internet de las cosas» (*Internet of Things*, en inglés), se refiere a objetos únicos e identificables—cosas—y sus representaciones virtuales en una estructura similar a Internet. Fue propuesto por primera vez en 1998[36].

Conforme haya más dispositivos conectados a Internet, más fundamental resulta asegurar la privacidad de los individuos.

En el mismo sentido, estos dispositivos plantean varios desafíos en la esfera de privacidad de los usuarios; se recopilan enormes cantidades de datos personales, como la información de ubicación, los hábitos de navegación, los patrones de uso o incluso la salud o los hábitos de consumo.

Cabe tener en cuenta que muchos de los dispositivos IoT tienen características de seguimiento y monitoreo que se pueden emplear para recopilar información sin el conocimiento o el consentimiento de los usuarios[37]. Toda esta resulta información sensible, por lo que la recopilación de estos datos se utiliza con fines fraudulentos, la privacidad y la seguridad de los usuarios se pueden ver comprometidas[38]. Es por ello por lo que, para proteger la privacidad en el IoT, se deben implementar medidas de

---

[35] Rifkin, J. (2014). *La sociedad de coste marginal cero*. Paidós.

[36] Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30. Recuperado el 15 de marzo de https://doi.org/10.1016/j.clsr.2009.11.008

[37] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

[38] Abomhara, M. and Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. Artículo presentado en la *International Conference on Privacy and Security in Mobile Systems (PRISMS)* de 2014 (pp. 1-8), Aalborg, Denmark. Recuperado el 18 de marzo de: https://doi.org/10.1109/PRISMS.2014.6970594

seguridad adecuadas, como la encriptación de datos y la autenticación de usuarios[39]. Además, también resulta esencial que los usuarios entiendan para qué se recopilan sus datos y la finalidad de uso de estos para puedan tomar medidas para controlar el acceso a esta información.

Asimismo, las empresas y organizaciones que desarrollan y utilizan dispositivos IoT también deben cumplir con las leyes y regulaciones de privacidad y proporcionar a los usuarios información clara y transparente sobre cómo se trata la información obtenida por sus sistemas.

En el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[40], en su considerando 78, se declara que el responsable del tratamiento de datos debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Esto está desarrollado en los artículos 25, sobre la protección de datos desde el diseño y por defecto,[41] y el artículo 47, sobre las normas corporativas vinculantes[42].

---

[39] Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A Review. En la *International Conference on Computer Science and Electronics Engineering* (ICCSEE) de 2012 (pp. 648-651). Hangzhou, China. Recuperado el 18 de marzo de https://doi.org/10.1109/ICCSEE.2012.373

[40]Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L 119/1-88. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[41] «*[…] 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento […]*».

[42] «*[…] 2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos: a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros; b) las transferencias o conjuntos de transferencias de datos […]; c) su carácter jurídicamente vinculante, tanto a nivel interno como externo; d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes; e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos […]*».

3. El contenido del ciberderecho

Una vez vistos los principios generales del ciberderecho, es necesario realizar un estudio al contenido de este.

Tal y como se ha ido comentando a lo largo de este documento, el ciberderecho no tiene un cuerpo normativo unificado y homogéneo, sino todo lo contrario. Esto es debido a la naturaleza globalizada del ciberespacio y de la variedad regulatoria existente en cada Estado. Hay que tener en cuenta que el aumento de las interacciones económicas y sociales a nivel global ha detonado el surgimiento de múltiples sistemas jurídicos en todo el mundo, lo que puede dar lugar a conflictos normativos básicos. El hecho de que en cada Estado haya pluralidad de ideologías respecto a las mismas materias genera desacuerdos y da paso a lo que Gunther Teubner califica como «globalización policéntrica»[43]. Según Teubner, estos sistemas jurídicos globales no están necesariamente jerárquicamente organizados o coordinados, sino que funcionan de manera policéntrica—esto es, con múltiples centros de poder y autoridad.

A pesar de no existir un cuerpo normativo o una estructura jurídica a la cual recurrir cuando surgen problemas en la Red, hay que reconocer que buena parte de la regulación que tiene por objeto el ciberespacio se ha realizado bajo la supervisión de la Unión Europea—normativa que se analizará a lo largo de este apartado. La creación de una normativa mínima que ponga el enfoque en algunas de las cuestiones que abarca la dimensión digital, pues, evidencia la necesidad de proteger los derechos de los ciudadanos, como la intimidad o la seguridad física, económica y jurídica.

Hoy en día, la incorporación de las nuevas tecnologías en nuestro día a día está tan normalizada que hay aspectos que no paramos a analizar y que nos afectan de manera directa. Con el uso de estas, damos acceso a todos nuestros datos pero sin reflexionar demasiado sobre la finalidad de la recopilación de esta información. Lo que antes utilizaban las empresas para, aparentemente, fines publicitarios, hoy en día lo aprovechan para poder optimizar sus estrategias y, por ende, sus ganancias; las empresas emplean la tecnología y los datos para controlar y predecir nuestro comportamiento, lo que a su vez les permite obtener ganancias a costa de nuestra privacidad y nuestra capacidad para tomar decisiones libres e informadas. Al inicio de este apartado, se ha comentado que ha habido un incremento de las interacciones económicas y sociales a nivel global; en esta misma línea, no solo habría habido un aumento, sino también estaría surgiendo un nuevo sistema económico y social. Esto comportará, a la larga, consecuencias para la

[43] Teubner, G. (2017). *El derecho como sistema autopoiético de la sociedad global*. Olejnik.

democracia y la libertad, puesto que la injerencia de las tecnologías en base a nuestros datos debilita nuestra capacidad para poder tomar decisiones informadas sobre nuestras vidas[44].

Teniendo en consideración los riesgos de las nuevas tecnologías, hay que observar que no solo es necesaria la protección jurídica de determinados derechos, sino que se ven afectados la mayoría de derechos tradicionales gracias a la rapidez con la que la información se propaga en la Red. Por ejemplo, el derecho a la imagen, la dignidad y el honor de las personas o la protección de los consumidores son aspectos que se ven influenciados y que necesitan el establecimiento de un marco jurídico que lo prevea[45]. Asimismo, la creciente difusión de imágenes o informaciones que presenten formas de exhibicionismo, provocación sexual o que fomenten la pornografía entre menores de edad también exige el asentamiento de medidas concretas que velen por los usuarios de Internet y, en especial, protejan a los menores[46].

Respecto a los consumidores, cabe realizar una serie de precisiones. Antes de que viviésemos esta revolución tecnológica, lo habitual era comprar en establecimientos físicos. Sin embargo, actualmente, es cada vez más común realizar las transacciones *on-line* por comodidad, facilidad y ahorro de tiempo para los consumidores. Con la aparición de la pandemia de la COVID-19, este proceso de compra en línea se ha visto aumentado a un ritmo más acelerado y ha obligado a otras empresas a introducir opciones a distancia para poder sostener el negocio. La situación actual, pues, se resume en que el consumo *on-line* es la nueva realidad y, por ello, se deben establecer mecanismos de defensa y protección para los consumidores para asegurar su navegación y posterior transacción comercial por Internet. Se deben implementar garantías que brinden la confianza necesaria a los cibernautas respecto a los contratos electrónicos que formalizan, así como el tratamiento de los datos que revelan durante la transacción.

Así, el Parlamento Europeo detectó que existen regulaciones que no acaban de coincidir entre los distintos Estados, hecho que claramente afecta al marco jurídico de los servicios en el ciberespacio[47].

Para poder lograr unificar una serie de medidas, se impulsó la Directiva 2000/31/CE, de 8 de junio, del Parlamento Europeo y del Consejo, relativa a determinados aspectos jurídicos de los

---

[44] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

[45] Richards, N. M. (2015). *Intellectual privacy: Rethinking civil liberties in the digital age*. Oxford University Press.

[46] En este sentido, se creó, para reforzar la protección penal de los menores, la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

[47] Barrio Andrés, M. (2018): *Ciberderecho: Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*. Tirant lo Blanch.

servicios de la Sociedad de la Información, en particular, el comercio electrónico en el mercado interior[48].

El texto normativo de esta Directiva plantea una regulación de mínimos y promueve la autorregulación normativa, en la medida en que considera que la mejor forma de proteger a los consumidores y usuarios es la aprobación de códigos de conducta que regulen las relaciones entre las empresas, los profesionales y los destinatarios de su actividad; por ello, incita a los Estados miembros a que fomenten este tipo de iniciativas (art. 16 DCE[49]).

Asimismo, la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre, relativa a los derechos de los consumidores, por la que se modifican la Directiva 93/13(CEE del Consejo y la Directiva 85/577/CEE del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo, ha llevado a cabo una revisión de la primera Directiva mencionada (la 2000/31/CE) sobre contratos de consumo en materia de máxima relevancia para el comercio electrónico, dado que se centra en la regulación de los contratos a distancia—con lo que deroga a la Directiva 97/7/CE—e introduce un nuevo enfoque en las obligaciones de los comerciantes en cuanto a proporcionar información a los consumidores respecto a estos contratos, cómo debe facilitarse esa información o el alcance, ejercicio y efectos del derecho de desistimiento. La transposición de esta nueva Directiva en España tuvo lugar mediante la Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.

Respecto a la necesidad de velar por la seguridad de las transacciones comerciales realizadas en línea, cabe decir que se ha reflexionado también en la Unión Europea; se ha puesto especial enfoque a la firma digital y el cifrado[50]: la primera es una garantía de la identidad de las partes contratantes y el origen de los mensajes, mientras que el segundo supone una protección de los mensajes ante intrusiones indebidas, así como una garantía de confidencialidad.

La Directiva 1999/93/CE, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica, fue pionera en este ámbito. Fue destinada a

[48] Directiva 2000/31/CE, del Parlamento Europeo y el Consejo de 8 de junio del 2000. Directiva relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular el comercio electrónico en el mercado interior. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000L0031&from=ES

[49] «*[…] 2. Los Estados miembros y la Comisión fomentarán la participación de asociaciones u organizaciones que representen a los consumidores en la redacción y aplicación de los códigos de conducta que afecten a sus intereses […]*».

[50] Kuner, C. (2007). *European Data Protection Law: Corporate Compliance and Regulation*. Oxford University Press.

garantizar la libre prestación de servicios de certificación electrónica en la Unión Europea, así como fijar criterios comunes respecto de la eficacia jurídica de las firmas electrónicas.

El 23 de julio de 2014 la sustituyó el Reglamento (UE) nº910/2014 del Parlamento Europeo y del Consejo[51], relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Este Reglamento, en vez de centrarse exclusivamente en la regulación de la firma electrónica basada en un certificado reconocido, abarca también otros mecanismos como los sellos electrónicos en documentos y autenticación de sitios web. A nivel nacional, tenemos contenida la regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica, la cual ha sido modificada en más de una ocasión.

Por otro lado, es necesario realizar una especial apreciación al derecho a la intimidad, el cual es innegable que se ve afectado directamente por las tecnologías de esta nueva era digital. Dejando al margen a las empresas, cualquier institución privada o pública recoge datos sensibles de los ciudadanos que afectan a su intimidad, en mayor o menor medida. La recolección de todos estos datos personales permite, indudablemente, desarrollar un gran poder de control sobre las personas, el cual se ha visto incrementado con la aparición de la inteligencia artificial y las herramientas de análisis del *big data*[52].

Para poder evitar este riesgo, la doctrina y jurisprudencia alemanas decidieron crear una nueva categoría: «el derecho a la autodeterminación informativa» (*Recht auf informationelle Selbstbestimmung*)[53]. En Alemania, la protección de los datos personales resulta un derecho fundamental[54]; por ello, vieron necesario introducir este derecho, el cual está basado en el reconocimiento del derecho que todos los individuos tienen a conocer qué información puede ser accedida por terceras personas, así como el poder de decisión sobre quién puede acceder y qué información quieren que sea conocida[55]. En otras palabras, este derecho vendría a reconocer

[51] Reglamento (UE) nº910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. Diario Oficial de la Unión Europea, L 257/73-142. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=ES

[52] Lohr, S. (2015). *Data-ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else*. HarperBusiness.

[53] Eichenhofer, J., y Gusy, C. (2017). Chapter 6: Courts, privacy and data protection in Germany: Informational self-determination in the digital environment. En *Courts, Privacy and Data Protection in the Digital Environment*. Cheltenham, UK: Edward Elgar Publishing. Recuperado el 20 de abril de 2023 de https://doi.org/10.4337/9781784718718.00013

[54] Schaar, P. (2008). The Fundamental Right to Data Protection. *Common Market Law Review*, 45(4) (pp. 1103-1123).

[55] Papier, H.-J. (2009). The Development of Data Protection in Germany. *International Data Privacy Law*, 1(3), (pp. 150-160).

que cada persona tiene el control y el derecho a tomar decisiones informadas sobre su información personal y cómo se utiliza y comparte.

> La Sentencia del Tribunal Constitucional Federal de Alemania de 1983[56], sobre el censo electoral, fue la primera en reconocer el derecho a la autodeterminación informativa en Alemania.
>
> El Tribunal Constitucional Federal determinó que la recopilación de datos personales para el censo electoral era inconstitucional debido a que violaba el derecho a la autodeterminación informativa de los ciudadanos: «*§ 9(1) of the 1983 Census Act violates the right to informational self-determination guaranteed under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law, given that the provision seeks to combine what is generally incompatible; the provision is therefore unsuitable to the purpose pursued and lacks legal clarity regarding its content so that, from the perspective of citizens, its implications are not fully comprehensible*.»
>
> Además, declaró que el Estado debe velar por la privacidad de los ciudadanos y que cualquier recolección de datos tiene que ser proporcional a la finalidad establecida.
>
> Esta sentencia sentó las bases para el desarrollo siguiente de la protección de datos como un derecho fundamental en Alemania[57] y ha tenido un impacto significativo en la protección de la privacidad en todo el mundo.

El derecho a la autodeterminación informativa también lo tenemos reconocido en nuestra Constitución, en el artículo 18[58]: «*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen; […]; 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial; 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*.». En el mismo sentido, en la sentencia 254/1993, de 20 de julio, el Tribunal Constitucional[59] determinó que «*la llamada libertad informática es un derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)*» (FJ7). Es decir, la libertad informática ya no se fundamentaría en la libertad de negar información sobre los propios hechos privados o datos personales, sino en el derecho a controlar el uso de los datos personales dentro de un programa informático. Esta

---

[56] Sentencia del Tribunal Constitucional Federal alemán del 15 de diciembre de 1983. Recuperado el 22 de abril de 2023 de: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

[57] Sieber, U. (2019). *Datenschutzrecht*. C.H.Beck.

[58] Constitución Española. (1978). Artículo 18. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

[59] Sentencia del Tribunal Constitucional 254/1993, de 20 de julio. Recuperado el 12 de abril de: https://www.boe.es/buscar/doc.php?id=BOE-T-1993-21425

resolución sentó un precedente, situando la libertad informática como derecho fundamental. Desde entonces, ha habido otras sentencias que también han hecho referencia al derecho a la autodeterminación informativa[60].

Por otro lado, en el marco europeo, se promulgó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que sería sustituida por el actual Reglamento General de Protección de Datos[61]. En España, la transposición de esta Directiva se hizo efectiva mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y la Administración independiente creada para tutelar el derecho a la protección de datos—que serían sustituidas posteriormente por la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[62], y la Agencia Española de Protección de Datos (AEPD).

El derecho a la protección de datos está estrechamente relacionado con el anteriormente mencionado derecho a la intimidad del art. 18 CE, puesto que tienen en común el objetivo de brindar protección constitucional efectiva de la esfera personal y familiar de los individuos. La diferencia la hallamos en que el derecho a la protección de datos otorga al individuo la capacidad jurídica de exigir a terceros que lleven o no a cabo ciertos comportamientos, cuya regulación específica debe estar establecida por la ley[63]. Esto se hace de acuerdo al artículo 18.4 CE, el cual estipula que el uso de la informática debe ser limitado por la ley, ya sea mediante la elaboración del derecho a la protección de datos o mediante el desarrollo de su ejercicio.

El derecho a la protección de datos fue reconocido como «derecho fundamental» por el Tribunal Constitucional en la STC 292/2000, de 30 de noviembre[64], en su fundamento jurídico 5.

EE.UU, tal y como se ha comentado al principio del documento, carece de una regulación unificada. En el caso del derecho a la protección de datos, tampoco hay una ley federal de

---

[60] Véase la STC 60/1998, 16 de Marzo de 1998 o la STS 803/2017, de 11 de Diciembre de 2017.

[61] 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 Recuperado el 12 de abril de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[62] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

[63] Kuner, C. (2007). *European data protection law: corporate compliance and regulation*. Oxford University Press.

[64] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

privacidad integral que lo incluya, sino que queda regulada por una serie de leyes estatales y federales fragmentadas y específicas por sector.

A nivel federal, la *Electronic Communications Privacy Act* (ECPA) y la *Digital Privacy Protection Act* (DPPA) ofrecen ciertas protecciones de privacidad en línea y para datos personales específicos, como los registros de llamadas y el historial de navegación en Internet.

Además, algunas leyes estatales, como la *California Consumer Privacy Act* (CCPA), han comenzado a establecer estándares más amplios de privacidad de datos personales. Sin embargo, la falta de una ley federal integral de privacidad de datos ha dado lugar a un complejo mosaico de normativas y ha dejado algunas lagunas en la protección de la privacidad de los consumidores en los Estados Unidos. Algunos expertos del sector cuestionan la adecuación de las soluciones legales actuales para proteger la privacidad y la reputación en línea[65].

Esto en Europa no ocurre, ya que existe el Reglamento General de Protección de Datos (GDPR). Además, también tenemos como referencia dos resoluciones relevantes del TJUE: la de 13 de mayo de 2014[66] y la de 6 de octubre de 2015[67]. La primera trató el famoso «derecho al olvido»[68] y determinó el derecho de supresión y bloqueo de datos, otorgando al buscador demandado—en este caso, *Google*—el deber de considerar y evaluar el tratamiento de todos los datos independientemente de su origen.

La segunda versó sobre la interpretación de los artículos 7, 8 y 47 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE), así como de los artículos 25.6 y 28 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; además, también se cuestionó la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de EE.UU.

---

[65] Solove, D. J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press.

[66] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 13 de mayo de 2014. Asunto C-131/12. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0131&from=ES.

[67] Sentencia del Tribunal de Justicia (Sala Primera) de 6 de octubre de 2015. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62014CJ0362

[68] Nos ocupamos de su estudio detallado en el epígrafe 4.5.

4. La protección de los datos en el ciberespacio

4.1 La personalidad virtual del usuario de Internet

Antes de proceder al análisis de uno de las cuestiones más abordados del derecho digital—la protección de datos—, vale la pena introducir la materia dando una pincelada a lo que es la personalidad virtual del usuario en el ciberespacio.

Cuando hablamos de la personalidad virtual del usuario en Internet, se hace referencia a la imagen o representación que una persona crea de sí misma a través de su actividad en línea. Con la tecnología que disponemos hoy en día, se nos permite expresarnos como antes no habíamos hecho; esto puede influir en nuestra identidad personal y social[69], puesto que la personalidad virtual no tiene por qué ser equivalente a la personalidad «real» de la persona. Esto se debe a que Internet se utiliza de manera frecuente para presentar los aspectos de uno mismo que se desean mostrar o para ocultar ciertos aspectos de la personalidad. Rara vez los usuarios muestran su verdadera personalidad con todas sus facetas.

Como íbamos diciendo, la personalidad virtual se construye mediante las interacciones que se realizan *on-line*, como publicaciones en redes sociales, comentarios en foros o comunidades virtuales e incluso conversaciones en chats o videojuegos en línea. Todas las actuaciones que tengamos en la Red son registradas por las *cookies* o tecnologías afines para posteriormente tratar esta información y elaborar el perfil de usuario[70].

Debe ser esencial que las personas sean conscientes de cómo construyen su personalidad virtual y de cómo pueden manejar su identidad en línea de manera efectiva y segura, ya que, a pesar de que los medios sociales han permitido nuevas formas de autoexpresión y de construcción de identidad, no hay que despreciar el hecho de que también han dado lugar a nuevos desafíos, como la privacidad y la seguridad en línea[71]. La mayoría de ocasiones, la recogida de datos personales y la elaboración del perfil de usuario se hace con fines publicitarios para mostrar a los cibernautas ofertas personalizadas de productos o servicios. Sin embargo, hay que hacer una reflexión sobre qué límites se deben establecer en este tratamiento de datos. Lo veremos en los siguientes epígrafes.

---

[69] Turkle, S. (1995). *La vida en la pantalla: la construcción de la identidad en la era de Internet*. Paidós.
[70] Navas Navarro, S. (2015). *Computación en la nube: big data y protección de datos personales* (p.186). Tirant lo Blanc.
[71] van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press.

4.2 El *Big Dat*a y los datos personales

Cuando se habla de tratamiento de datos, es inevitable que aparezca en el debate el concepto de *Big Data*, el cual se refiere a conjuntos de datos extremadamente grandes y complejos que requieren nuevas herramientas, técnicas y tecnologías para procesar, analizar y comprender[72]. Este conjunto de datos masivos, recopilados por los proveedores de servicios, tiene el potencial de cambiar la forma en que las empresas, los gobiernos y las personas toman decisiones, además de que se puede emplear para identificar patrones, hacer predicciones y descubrir nuevas ideas y oportunidades.

A medida que la tecnología del *Big Data* se ha expandido, se ha empezado a centrar el foco cada vez más en la protección de los datos personales. No obstante, ¿cómo se pueden identificar los datos personales? El ya mencionado Reglamento General de Protección de Datos[73], en su artículo 4 apartado 1), define los datos de carácter personal como «*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*.».

Por otro lado, en EE.UU, la definición de datos personales se halla en varias leyes y regulaciones federales y estatales que protegen la privacidad y la seguridad de la información personal de las personas. Como ya se ha comentado en más de una ocasión a lo largo del documento, no existe una definición única y específica de datos personales porque no cuentan con una normativa unificada. Sin embargo, la mayoría de las leyes y regulaciones federales y estatales que tratan sobre la protección de la privacidad y la seguridad de la información personal de las personas se refieren a los datos personales de una manera u otra. Por ejemplo, la Ley de Privacidad del Consumidor de California (CCPA) define los datos personales como «*cualquier información que identifique, se relacione con, describa, sea capaz de asociarse con*

[72] Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

[73] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L119/1-88. Recuperado el 12 de abril de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

o pueda ser razonablemente vinculada, directa o indirectamente, con una persona física en particular o un hogar.»[74]

Como podemos observar, en ambas definiciones se definen los datos personales de manera amplia e inclusiva, reconociendo que cualquier información que pueda identificar a una persona directa o indirectamente, ya sea por sí sola o en combinación con otros datos, se considera un dato personal.

Volviendo al tratamiento de datos y teniendo en cuenta que no existe una regulación común en el mundo del ciberderecho, las empresas y organizaciones que recopilan y utilizan estos datos deben asegurarse de que sus prácticas cumplan con las leyes y regulaciones de protección de datos personales en cada país en el que operan, dado que es evidente que hay transferencias de datos que se producen a nivel internacional[75]. En el mundo digital, sin embargo, resulta algo complicado supervisar la actuación de las empresas, dado que la sede de éstas puede encontrarse en un Estado diferente al del consumidor que origina los datos. Aquí entra en juego el derecho internacional, mediante el cual se debe velar por la protección al consumidor. No obstante, si existiera una estructura jurídica autónoma con su correspondiente normativa dedicada a las situaciones que se dan en la red, probablemente, se podrían resolver de forma más eficaz los casos que se originasen. Estudiemos las normativas más destacables de esta materia en los siguientes apartados.

4.3 Reglamento (UE) 2016/679: de protección de datos de carácter personal

Como se ha comentado previamente, la Unión Europea no tardó en abordar esta materia y legisló sobre la protección de datos, sentando un precedente con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta Directiva estableció las bases para la legislación nacional de protección de datos en toda la UE.

---

[74] California Consumer Privacy Act of 2018 (CCPA). Artículo 1798.49 (v)(1): «*"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household».* Recuperado el 19 de abril de: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[75] Navas Navarro, S. (2016). Computación en la nube: big data y protección de datos personales. *InDret*, (4) [en línea] Recuperado el 17 de abril de https://indret.com/wp-content/themes/indret/pdf/1193_es.pdf

Sin embargo, esta no fue la primera referencia que se hizo a la protección de datos. Los primeros antecedentes en el derecho comunitario datan de 1981, cuando se firmó el Convenio 108 del Consejo de Europa, de 28 de enero, ratificado por España el 27 de enero de 1984[76]. En este convenio se asociaba la protección de datos a dos derechos fundamentales tradicionales: el derecho a la vida privada y el derecho a la intimidad[77], a pesar de ser un derecho fundamental autónomo. En España, esta materia también ha sido abordada de forma similar, aunque la protección de datos personales no está reconocida como derecho fundamental en la Constitución Española[78].

Volviendo a la creación de la Directiva 95/46/CE, cabe destacar que el 25 de mayo de 2018 entró en vigor la norma que la sustituiría—así como ampliaría su contenido—y actualmente regula esta materia: el Reglamento (UE) 2016/679, de protección de datos de carácter personal[79], también conocido como RGPD (o GDPR en inglés).

Como ya sabemos, la Directiva era una ley marco que requería que los Estados la transpusieran a la legislación nacional de cada Estado miembro, mientras que el Reglamento resulta una norma vinculante y directamente aplicable en todos los Estados miembros de la UE. Este es uno de los cambios que ha habido, además de un aumento de contenido, puesto que este Reglamento incluye a todas las empresas y organizaciones que procesan datos personales de individuos que se encuentran en la UE, independientemente de si la empresa u organización está ubicada dentro o fuera de la UE (art. 3[80]).

Aunque no vamos a realizar un análisis en profundidad del Reglamento, sí vamos a detenernos a comentar sus principales aspectos.

---

[76] Convenio 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. Ratificado por España el 27 de enero de 1984. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

[77] Rebollo, L. (2008). *Vida privada y protección de datos en la Unión Europea*. Dykinson.

[78] Campuzano, H. (2018). Cuatro décadas de protección jurídica del derecho a la privacidad frente a las TIC: del derecho a la autodeterminación informativa al derecho al olvido digital, en Álvarez, L. Y Punset, R. (Eds.), *Cuatro décadas de una constitución normativa (1978-2018)* (pp. 133-157). Thomson Reuters-Aranzadi.

[79] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). *Diario Oficial de la Unión Europea, L119/1-88*. Recuperado el 12 de abril de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[80] Este artículo establece que el Reglamento se aplicará a todas las empresas y organizaciones que procesan datos personales en el contexto de las actividades de una sucursal establecida en la UE, así como a aquellas que no tienen presencia en la UE pero que ofrecen bienes o servicios a individuos en la UE o que monitorean su comportamiento en la UE.

En primer lugar, analizaremos los seis principios que se describen en el artículo 5 del RGPD[81], los cuales se consideran la columna vertebral del Reglamento y deben guiar todas las decisiones que tomen las empresas y organizaciones en relación con el procesamiento de datos personales[82].

1. El **principio de licitud, lealtad y transparencia (*lawfulness, fairness and transparency*)**.

   Este principio se fundamenta en la idea de que el procesamiento de datos personales debe ser justo, transparente y legal. Hay autores que describen este principio como una «regla de oro» para el procesamiento de datos personales[83]. Este principio, pues, requiere que las organizaciones tengan una base legal para el procesamiento de datos personales, que el procesamiento se realice de manera justa y transparente, y que se proporcione información clara y concisa a los interesados sobre el procesamiento de sus datos personales[84].

2. El **principio de limitación de la finalidad (*purpose limitation*).**

   Este principio describe que los datos personales se deben recopilar con fines específicos, explícitos y legítimos; además, no deben ser procesados posteriormente de una manera incompatible con esos fines.

   Según Paul Voigt y Axel von dem Bussche, este principio implica que «*los datos personales deben ser procesados solo para fines determinados, explícitos y legítimos,*

---

[81] «*1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia"); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ("limitación de la finalidad"); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos"); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan ("exactitud"); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ("limitación del plazo de conservación"); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad")».*
2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva").»

[82] Voigt, P. & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing.

[83] Calder, A., & Watkins, S. (2016). *EU GDPR: A Pocket Guide*. IT Governance Publishing.

[84] IT Governance Publishing. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*.

y no deben ser procesados posteriormente de una manera incompatible con esos fines»[85]. Alan Calder y Steve Watkins también lo explican de forma similar[86], afirmando que «*los datos personales deben ser recopilados para fines específicos, explícitos y legítimos, y no deben ser procesados posteriormente de una manera incompatible con esos fines*».

3. El **principio de minimización de datos (*data minimisation*)**.

   El principio de minimización de datos establece que los datos personales deben ser adecuados, relevantes y limitados a lo necesario en relación con los fines para los que son procesados. Con este principio se debe entender la importancia de minimizar la cantidad de datos personales recopilados y de no retener los datos por más tiempo del necesario[87].

4. El **principio de exactitud (*accuracy*)**.

   El principio de exactitud determina que los datos personales deben ser precisos y estar actualizados. Además, también establece el deber de tomar medidas razonables para garantizar que los datos inexactos se rectifiquen o eliminen si es necesario. Mediante este principio, es importante también llevar a cabo una buena gestión de la calidad de los datos para poder asegurar la exactitud de los datos personales[88].

5. El **principio de limitación de almacenamiento (*storage limitation*)**.

   Este principio busca garantizar que los datos personales se almacenen solamente por un período de tiempo limitado y únicamente para los fines específicos para los cuales fueron recopilados. Esto es porque el objetivo es proteger la privacidad de las personas y prevenir el uso indebido de sus datos personales. Los expertos de la materia destacan la importancia de implementar medidas técnicas y organizativas para garantizar que los datos personales sean eliminados de manera efectiva y segura una vez que ya no sean necesarios[89].

---

[85] Ídem nº 73.
[86] Ídem nº74.
[87] Ídem nº73.
[88] Feiler, L., Forgó, N., & Weigl, M. (2018). *The EU General Data Protection Regulation (GDPR): A Commentary*. CH Beck.
[89] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2018). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.

6. El **principio de integridad y confidencialidad (*integrity and confidentiality*)**.

   Este principio está diseñado para asegurar que los datos personales sean tratados de forma confidencial. Mediante este principio, se quiere evitar el acceso, modificación, divulgación o destrucción a personas que no estén autorizadas[90].

Aparte de estos seis principios, el RGPD también establece el principio de responsabilidad proactiva (art. 5.2), que exige que «el responsable del tratamiento», esto es las organizaciones, tomen medidas para garantizar el cumplimiento de la ley de protección de datos, como la implementación de medidas técnicas y organizativas adecuadas para garantizar la seguridad y protección de los datos personales.

Una de las grandes aportaciones que ha realizado este Reglamento que vale la pena comentar ha sido la gestión de *cookies*, puesto que se ha establecido una nueva forma de prestar el consentimiento de forma estratificada por parte del consumidor. Este tema ha sido objeto de debate entre varios autores: mientras unos opinan que el RGPD ha aumentado la protección de la privacidad de los usuarios de Internet al exigir a las empresas que obtengan el consentimiento explícito para el uso de *cookies* y proporcionen información clara sobre su uso[91], otros autores han criticado que el RGPD ha introducido un mayor nivel de complejidad en el cumplimiento de las regulaciones de las *cookies*[92]. Piensan que se ha introducido una complejidad innecesaria y costosa en la regulación de las *cookies*, en particular, en lo que se refiere a la obtención de consentimiento y a la recopilación y gestión de datos.

Sin embargo, la aportación más relevante va más allá de la definición de un régimen general de protección de datos de carácter personal, siendo lo más destacable el impacto que ha tenido en el derecho de contratos[93]. Esto es debido a que ha demostrado la existencia de una viabilidad jurídica y técnica para compensar las negociaciones entre la parte dominante del contrato (empresario) y la débil (consumidor), creando un «consentimiento dinámico». Este consentimiento dinámico se origina mediante la comunicación activa y continua entre ambas partes para obtener, renovar o retirar el consentimiento del consumidor para el tratamiento de sus datos personales. Siguiendo los principios marcados por el RGPD, esto implica que las

[90] Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
[91] Hildebrandt, M. (2018). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. Forthcoming in Theoretical Inquiries of Law 2019, 19(1) *SSRN Electronic Journal*. Recuperado el 22 de abril de 2023: http://dx.doi.org/10.2139/ssrn.3081776
[92] Jacob, V. (2018). The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. *The University of Chicago Law Review*, 85(2), 535-582.
[93] Hidalgo, A. (2020). *Derecho digital en la Unión Europea: techlaw y mercado único digital en la década 2010-2020*. Comares.

empresas deben ofrecer a los consumidores información clara y accesible sobre el uso de sus datos, así como permitirles actualizar o retirar su consentimiento en cualquier momento.

En definitiva, la entrada en vigor del RGPD ha logrado instaurar un modelo de consentimiento estratificado que supera el antiguo enfoque de las condiciones generales de contratación, las cuales se basaban en modelos económicos e industriales obsoletos. Con la tecnología digital actual, es posible llevar a cabo negociaciones personalizadas con cada consumidor de forma viable, así como administrar contratos personalizados. Por lo tanto, hoy en día, los consumidores pueden manifestar su consentimiento con respecto a determinados aspectos o cláusulas de un acuerdo y rechazar las que no deseen aceptar.

4.4 La LOPD. Comentario sobre los derechos digitales en España

Después de haber realizado un comentario sobre el RGPD, vale la pena hacer mención a la norma que incorpora esta materia en el ordenamiento jurídico español, que actualiza la legislación española en materia de protección de datos y la adapta a los desafíos y oportunidades que presenta el entorno digital: la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD). Entró en vigor el 7 de diciembre de 2018 y, como ya se ha comentado con anterioridad, sustituyó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. La creación de la nueva LOPD tuvo una doble finalidad: la transposición del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), a la normativa interna; y asegurar los derechos digitales de los ciudadanos para preservar su honor e intimidad personal y familiar, así como el pleno ejercicio de sus derechos, de acuerdo a lo establecido en el artículo 18.4 de la Constitución[94].

La doctrina se ha pronunciado en más de una ocasión sobre los desafíos que plantea la aplicación de la normativa de protección de datos en un contexto digital cada vez más complejo y cambiante[95]. Entre los aspectos más comentados se engloba la necesidad de adaptarse a las nuevas formas de tratamiento de datos personales, la importancia de la privacidad y la protección de datos en el contexto de la economía digital y el comercio electrónico, y la

[94] «*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*».

[95] Por ejemplo: Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security*. Yale University Press; o Richards, N. M. (2015). *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford University Press.

necesidad de desarrollar herramientas y soluciones para garantizar la protección de datos personales *online*[96].

Lo más destacable de la nueva LOPD es el establecimiento de nuevas obligaciones para las empresas que procesan datos personales, incluyendo la necesidad de obtener el consentimiento explícito y específico para el tratamiento de los datos personales (art. 6) y la obligación de notificar cualquier violación de seguridad de los datos personales (art. 73). Esto implica que las empresas deben ser más transparentes y claras en su comunicación con los usuarios, puesto que es imperativo adaptarse a esta nueva legislación y disponer de políticas lo suficientemente claras y efectivas para poder garantizar la protección de los datos personales de los usuarios[97].

Por otro lado, la LOPD también incluye medidas para garantizar los derechos digitales de las personas, como el derecho al acceso universal a Internet (art. 81), el derecho a la educación digital (art. 83) o el derecho a la libertad de expresión en línea (art. 84).

Asimismo, esta ley también introduce nuevos derechos para los ciudadanos, como el derecho a la limitación del tratamiento de los datos (art. 16), el derecho a la oposición al tratamiento de los datos (art.18), el derecho a la neutralidad de Internet (art. 80), el derecho al olvido (art. 93 y 94) y el derecho a la portabilidad de los datos (art. 95).

De todas las novedades introducidas, una de las más interesantes es el derecho al olvido, descrito en los artículos 93 y 94. Este derecho también queda regulado en artículo 17 del RGPD y lo comentaremos en el siguiente epígrafe.

4.5 El derecho al olvido digital

El derecho al olvido digital, el cual encuentra su fundamento en el ya referido derecho a la protección de datos[98], se puede definir como «*el derecho de las personas físicas a hacer que se elimine información sobre ellas después de un periodo de tiempo determinado*»[99]. Es decir, se trata de un derecho que tienen los ciudadanos a solicitar que se supriman datos personales que circulan por internet ante el riesgo que esto supone en la vulneración de los derechos de la personalidad—concretamente, los derechos al honor y a la intimidad.

---

[96] Troncoso Reigada, A. & González Rivas, J. J. (2019). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*. Aranzadi.
[97] Arenas Ramiro, M. & Ortega Giménez, A. (2019). *Protección de Datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*. Sepin.
[98] Simón Castellano, P. (2015) *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014* (p. 185). Bosch.
[99] De Terwangne, C. (2012). Privacidad en internet y el derecho a ser olvidado/derecho al olvido, *Revista de Internet, Derecho y Política*, 13 (p. 53).

Es necesario destacar que el derecho al olvido no es un concepto que esté reconocido en la legislación de los Estados Unidos—aunque sí ha habido casos en los que se ha discutido sobre el equilibrio entre el derecho a la privacidad y la libertad de expresión en línea[100]—por lo que lo comentaremos en base a la legislación y jurisprudencia comunitarias.

El desarrollo del derecho al olvido digital tiene origen doctrinal y jurisprudencial[101], puesto que, hasta ahora, ningún texto normativo lo recogía expresamente—es decir, no estaba tipificado por ley—y, a pesar de que ahora está incluido en el RGPD (art. 17), no se ofrece una definición de lo que se debe entender por el mismo[102]. También lo encontramos en los artículos 93 y 94 de la LOPD, los cuales ofrecen dos vertientes de este derecho:

1) Artículo 93, sobre el derecho al olvido en búsquedas de Internet. Las personas tienen derecho a solicitar la supresión de los datos personales que estén siendo tratados por motores de búsqueda en relación con determinadas consultas.

   Para que proceda la eliminación de los datos, la persona afectada debe haber retirado su consentimiento para el tratamiento de los mismos, que los datos ya no sean necesarios para la finalidad para la que se recogieron o que el tratamiento no cumpla con la normativa de protección de datos. Además, la solicitud se debe dirigir directamente al motor de búsqueda y se debe evaluar de manera individualizada.

   Por otro lado, también se establece el deber de los motores de búsqueda de informar a los usuarios que realizan una búsqueda sobre la existencia de solicitudes de eliminación de datos relacionados con los resultados de la búsqueda en cuestión. Por otro lado, también se deben adoptar medidas técnicas necesarias para asegurar la efectiva supresión de los datos en cuestión, incluso cuando éstos estén en la página web de origen y no sean responsabilidad directa del motor de búsqueda.

---

[100] Por ejemplo, el caso *Google, Inc. v. Equustek Solutions, Inc*, en el que en el que *Equustek Solutions*, una compañía canadiense, demandó a Google por mostrar resultados de búsqueda que vinculaban a los sitios web de *Datalink Technologies Gateway Inc*., empresa que estaba vendiendo productos aprovechando los secretos comerciales de *Equustek*. La Corte Suprema de Canadá dictaminó que Google debía eliminar los resultados de búsqueda a nivel mundial—y no solo en Canadá—para proteger los derechos de propiedad intelectual de *Equustek Solutions*. No obstante, *Google* se opuso a esta orden y argumentó que se estaba extralimitando en su jurisdicción y que la orden violaba la Primera Enmienda de la Constitución de Estados Unidos. La Corte argumentó que *Google* estaba participando en la actividad ilegal de *Datalink* al permitir que sus resultados de búsqueda dirigieran a los usuarios a sitios web que contenían secretos comerciales robados y, además, también señaló que la orden no violaba la Primera Enmienda de Estados Unidos, ya que no se estaba exigiendo que se eliminara ningún contenido de Internet, sino simplemente que se eliminara el acceso a ese contenido a través de los resultados de búsqueda de *Google*. Sentencia disponible en: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

[101] Touriño, A. (2014). *El derecho al olvido y a la intimidad en internet*. La Catarata.

[102] Murga Fernández, J.P. (2018). La difícil relación entre los motores de búsqueda en internet y el derecho al olvido, en R. García Crespo (Ed.), *Derecho digital: retos y cuestiones actuales* (pp. 279-299). Thomson Reuters-Aranzadi.

Respecto a esta dimensión del derecho al olvido, tenemos la STJUE de 13 de mayo de 2014[103]—ya mencionada con anterioridad. Está considerada como un hito en la jurisprudencia europea en materia de derecho al olvido digital[104], pues reconoció el derecho al olvido digital, permitiendo a las personas solicitar la eliminación de enlaces a información personal que fuese inexacta, inadecuada, no pertinente o excesiva, siempre y cuando no existiese un interés legítimo superior que prevaleciera en la difusión de la información.

> Dicha sentencia abarca el litigio centrado en la eliminación de los datos solicitada por el demandante contra *Google* (*Google Spain SL* y *Google Inc*.). *Google Spain SL* negó tener legitimación pasiva en supuestos de ejercicio del derecho al olvido alegando lo siguiente: 1) La normativa europea y española relativa a la protección de datos no le era aplicable porque no asumía la responsabilidad de indexar información contenida en otras páginas web. 2) La actividad desempeñada no podía tener la consideración de «tratamiento de datos personales», puesto que se limitaban a poner a disposición de los usuarios información publicada por terceros.
>
> El TJUE se opuso a estas consideraciones y argumentó que el hecho de almacenar información publicada por terceros para luego ponerla a disposición de los internautas podía ser calificado como «tratamiento de datos personales» (FJ 40).
>
> Por otro lado, en base al art. 4.1.a) de la Directiva sobre Protección de Datos, los Estados miembros pueden aplicar las disposiciones derivadas de la transposición de la Directiva a cualquier tratamiento de datos personales cuando «*sea efectuado en el marco de las actividades de un establecimiento del responsable en el territorio del Estado miembro*». Esto se traduce a que, dado que la actividad del motor de búsqueda engloba la promoción y venta de espacios publicitarios, y teniendo en cuenta que la aparición de datos personales en una página de resultados de una búsqueda va acompañada de publicidad relacionada con los términos de búsqueda, se puede determinar que el tratamiento de datos se lleva a cabo en territorio europeo—por lo que la normativa sobre protección de datos de la UE y España son de aplicación.
>
> El TJUE dictaminó, además, que «*el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este*

[103] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 13 de mayo de 2014. Asunto C 131/12. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0131&from=ES

[104] Rallo Lombarte, A. (2014). *El derecho al olvido en internet. Google versus España*. Centro de estudios constitucionales.

nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita» (FJ 88).

2) Artículo 94, sobre el derecho al olvido en servicios de redes sociales y servicios equivalentes. Este artículo establece que las personas tienen derecho a que se supriman sus datos personales cuando así lo soliciten en estos servicios, siempre y cuando se cumplan ciertas condiciones: cuando sus datos personales resulten inadecuados, no pertinentes o ya no sean necesarios para la finalidad para la que fueron recogidos. Además, también se puede solicitar la supresión de los datos cuando se haya retirado el consentimiento para su tratamiento, se hayan tratado de manera ilícita o se deba hacerlo para cumplir con una obligación legal.

También se determina que los servicios de redes sociales y servicios equivalentes deben proporcionar mecanismos sencillos y gratuitos para que los usuarios puedan ejercer este derecho. Asimismo, se establece que estos servicios deben garantizar la efectividad del derecho al olvido y la supresión de los datos en un plazo máximo de un mes desde la recepción de la solicitud del interesado.

Respecto a esta segunda dimensión del derecho al olvido digital, podemos comentar la STJUE de 3 de octubre de 2019[105].

Esta sentencia analiza el alcance de la obligación de los prestadores de servicios de intermediación en línea, como *Facebook*, de retirar o bloquear el acceso a contenido ilegal. En este supuesto, la demandante solicitó que se retirara un mensaje difamatorio publicado por un usuario en *Facebook*. Aunque el mensaje fue retirado en Austria, la demandante también exigió que se eliminara de todo el territorio de la Unión Europea.

El TJUE señaló que, a pesar de que las empresas no pueden ser responsables de forma automática por el contenido publicado por los usuarios, sí deben eliminar el contenido ilegal en cuanto tengan conocimiento de ello (FJ23). En este sentido, también se estableció que los servicios de redes sociales pueden ser obligados a eliminar contenido ilegal y ofensivo incluso a nivel mundial—y no solo en los países donde se originó la publicación (FJ 35 a 37).

Además, la sentencia recuerda que el derecho de la UE exige que los prestadores de servicios de intermediación en línea deben retirar contenido ilegal a nivel mundial

[105] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera) de 3 de octubre de 2019. Asunto C 18/18. Disponible en https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62018CJ0018

cuando se les notifique, siempre y cuando la orden sea compatible con la normativa comunitaria y no haya peligro de censura de la información legítima (FJ 53).

5. Cibercrimen

Ya hemos asumido que las nuevas tecnologías han cambiado la forma de acceder a la información y han abierto posibilidades que antes no barajábamos. Entre estas posibilidades, ha surgido una forma de crimen no existía antes del surgimiento de Internet: el cibercrimen. Si bien ha habido controversia sobre su concepto y los diferentes términos que se emplean[106]—a lo que no vamos a entrar en detalle—, este se puede definir como «*un conjunto de comportamientos delictivos y no delictivos que se relacionan con el conocimiento, la cultura y la tecnología de la información, que producen daño o riesgo de daño a los bienes individuales o colectivos y a la sociedad en general y que son llevados a cabo mediante la utilización de una infraestructura de red o de los sistemas de información*»[107]. En otras palabras, se trata de un tipo de delito cometido mediante Internet o tecnologías de la información y la comunicación (TIC) que puede incluir todo tipo de comportamiento delictivo en línea.

La cuestión de la criminalidad informática no supone un tema realmente novedoso hoy en día, pues ya han transcurrido más de treinta años desde que comenzó a hablarse de ello y más de veinte desde que se acuñó el término *cybercrime*[108]. No obstante, el cibercrimen sigue siendo objeto de debate actualmente, dado que ya forma parte de la realidad criminológica de nuestra sociedad y lleva generando cambios significativos en el ámbito de la asistencia judicial internacional desde que apareció[109], entre ellos, la elección de la normativa aplicable o las normas procedimentales para la obtención de la prueba, dado que la determinación de la ubicación de la comisión del delito, en la mayoría de ocasiones, resulta compleja.

Es obvio que esta era digital ha venido para quedarse y no cabe duda de que seguirá evolucionando, por lo que la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas[110]. Por ello, es fundamental el papel de los organismos internacionales, puesto que son los únicos que pueden establecer medidas que vinculen a los Estados. El esfuerzo de armonización más logrado en esta materia se refleja en el Convenio de Budapest[111] o «convenio sobre la ciberdelincuencia», del Consejo de Europa,

---

[106] Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons Ediciones Jurídicas y Sociales. Recuperado el 28 de abril de https://elibro.net/es/ereader/uab/58741?page=26

[107] Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. John Wiley & Sons.

[108] Ídem nº100.

[109] del Carril, E. & Deluca, S. (2017). Cooperación internacional en materia penal en el MERCOSUR: el cibercrimen. *Revista de la Secretaría del Tribunal Permanente de Revisión*, 5(10) (pp.13-28).

[110] Ídem nº99.

[111] Convenio sobre la Ciberdelincuencia del Consejo de Europa, hecho en Budapest el 23 de noviembre de 2001. Ratificado por España el 20 de mayo de 2010. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

el cual es referido como el acuerdo internacional de mayor extensión en materia de cibercriminalidad[112]. La particularidad de este convenio es que fue abierto a la firma de cualquier país del mundo[113] y estableció pautas tradicionales para la determinación de la jurisdicción de los delitos[114] y la base jurídica para la asistencia internacional y la extradición[115]. Fue ratificado por España el 20 de mayo de 2010 y entró en vigor el 1 de octubre de ese mismo año.

El Convenio de Budapest, junto a la Convención de las Naciones Unidas contra la delincuencia organizada transnacional[116] son los únicos instrumentos internacionales vigentes en la materia[117]. En EE.UU, existe la Ley de Fraude y Abuso Informático (CFAA en inglés)[118], una ley federal que penaliza la distribución de *software* malicioso, el fraude en línea, la manipulación de datos en sistemas informáticos, el acceso no autorizado a estos sistemas y la obtención de información de estos. Se promulgó el 16 de octubre de 1986 y se ha modificado en numerosas ocasiones para abordar la evolución de las tecnologías de la información y las comunicaciones. La ley ha sido empleada en varios casos significativos, como el caso contra el *hacker* Gary McKinnon[119] y el caso contra el fundador de *WikiLeaks*, Julian Assange[120].

El caso McKinnon V. EE.UU tuvo un gran impacto mediático, pues McKinnon había accedido de forma no autorizada a más de 97 ordenadores del gobierno estadounidense—incluyendo la

---

[112] Tapia Sánchez, L. S. (2022). Tecnología y Derecho una mirada al Comercio Electrónico, el Cibercrimen y el Soft Law. *AIS: Ars Iuris Salmanticensis*, 10(1), (pp. 199–226). Recuperado el 30 de abril de https://doi.org/10.14201/AIS2022101199226

[113] Art. 37.1: «*Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros*.»
Art. 38: «*1. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá especificar el territorio o territorios a los que se aplicará el presente Convenio.*
2. En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.»

[114] Artículo 22.

[115] Capítulo III.

[116] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2000). Disponible en https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

[117] Ídem nº 102.

[118] *Computer Fraud and Abuse Act of 1986* (CFAA) https://www.congress.gov/bill/99th-congress/house-bill/4718/text

[119] Sentencia de la *Queen's Bench Division (Administrative Court)* del 3 de abril de 2007. Caso CO/5897/2006. Recuperado el 30 de abril de: https://vlex.co.uk/vid/mckinnon-v-united-states-793612009

[120] Sentencia de la *Queen's Bench Division (Administrative Court)* del 12 de octubre de 2021. Caso CO/150/2021. Recuperado el 30 de abril de https://www.judiciary.uk/wp-content/uploads/2022/07/USA-v-Assange-judgment101221.pdf

NASA y el Departamento de Defensa—en busca de información sobre ovnis. El gobierno de los Estados Unidos solicitó la extradición de McKinnon a los Estados Unidos para ser juzgado por los cargos, pero su defensa argumentó que McKinnon padecía de un trastorno de Asperger y que había riesgo de que se suicidara si se llevaba a cabo la extradición. Finalmente, después de varios años de apelaciones, la entonces Secretaria de Interior del Reino Unido, Theresa May, decidió en 2012 que McKinnon no sería extraditado por motivos de salud mental.

Por otro lado, el caso Assange V. EE.UU también se ha seguido de cerca por los medios. En 2010, Julian Assange—el fundador de *WikiLeaks*—y su equipo publicaron cientos de miles de documentos clasificados relacionados con las guerras en Irak y Afganistán, además de cables diplomáticos del Departamento de Estado de EE.UU.

La publicación de estos documentos originó una gran controversia y una fuerte reacción de los gobiernos involucrados, especialmente de Estados Unidos. Por ello, Assange y otros miembros de *WikiLeaks* han sido objeto de investigaciones y acusaciones de varios delitos en distintos países, incluyendo EE.UU, Suecia y Reino Unido. En abril de 2019, Julian Assange fue detenido por la policía británica en la embajada de Ecuador en Londres, donde había estado refugiado desde 2012. Finalmente, en septiembre de 2021, el Reino Unido autorizó la extradición de Assange a Estados Unidos, donde se enfrenta cargos de espionaje y otros delitos.

5.1 Tipos de cibercrímenes

Después de haber realizado una breve inmersión al mundo del cibercrimen, vale la pena comentar los delitos más comunes que pueden tener lugar en el ciberespacio. Para ello, seguiremos la estructura del Convenio de Budapest anteriormente referido. En esta línea, pues, lo estructuraremos de la manera siguiente[121]: 1) Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos; 2) Delitos asociados a la informática; 3) Delitos de contenido; 4) Delitos relativos a las infracciones contra la propiedad intelectual y derechos conexos.

[121] Estructura también seguida por Barrio Andrés, M. (2011). La ciberdelincuencia en el Derecho español. *Revista de las Cortes Generales*, (83) (pp. 273-305). Recuperado el 1 de mayo de https://doi.org/10.33426/rcg/2011/83/473.

5.1.1 Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos

a) Intrusismo e interceptación de las comunicaciones (*hacking*)

El *hacking* se define como «*el conjunto de comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicaciones y a la utilización de los mismos sin autorización o más allá de la misma*»[122].

El descifrado de contraseñas (*password guessing*), la creación de puertas traseras (*backdoors*), la interceptación de los paquetes de datos (*sniffers*), el acceso o control remoto y la propagación de virus son algunas de las prácticas más comunes en el *hacking*[123]. Las sanciones aplicables a esta actividad se recogen en la reforma del artículo 197 de nuestro Código Penal[124].

b) Daños y sabotaje (*cracking*)

En este apartado se incluyen aquellos actos categorizados como «vandalismo digital», «ciberterrorismo» y también los de «cracking» dirigidos a la producción de daños[125].

El delito de *cracking* se refiere a la actividad de acceder o ingresar a sistemas informáticos sin la debida autorización o permiso[126]. Esta actividad está calificada como una violación de la seguridad informática y se considera como un delito en la mayoría de los países[127].

El término «*cracking*» se utiliza para distinguir esta actividad de otras formas de acceso ilegal a sistemas informáticos, como el «*hacking* ético», que se realiza con el permiso del propietario del sistema con el objetivo de identificar vulnerabilidades y mejorar la seguridad[128]. El

---

[122] Morón Lerma, E. (1999) *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red* (p. 42), Aranzadi.

[123] Barrio Andrés, M. (2011). La ciberdelincuencia en el Derecho español. *Revista de las Cortes Generales*, (83) (pp. 273-305). Recuperado el 1 de mayo de https://doi.org/10.33426/rcg/2011/83/473.

[124] «*3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. Cuando de acuerdo con lo establecido en el artículo 31.bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66.bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.*
[...] 8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado»

[125] Ídem 118.

[126] Mitnick, K., & Simon, W. L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons.

[127] Aparte de Europa, en EE.UU, el *cracking* es un delito federal y está previsto en la *Computer Fraud and Abuse Act of 1986;* en el Reino Unido, está regulado en la *Computer Misuse Act* of 1990; también se incluye como delito en Australia, Canadá y Japón.

[128] Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the human element of security*. John Wiley & Sons.

cracking, en cambio, se lleva a cabo sin autorización y con fines maliciosos, como el robo de información o la destrucción de datos.

Encontramos la pena impuesta a esta delito en el artículo 264 del Código Penal.

c) Abuso de sistemas informáticos

Se encuentra tipificado en el artículo 256 del Código Penal. Este precepto condena al que haga uso de cualquier equipo terminal de telecomunicación (como el teléfono, el fax, el correo electrónico…) sin tener el consentimiento de su propietario y, además, habiéndole ocasionado un perjuicio de más de 400 euros.

Este artículo, actualmente, se refiere a defraudaciones telefónicas y al pirateo de contraseñas de acceso a servicios de pago, mayoritariamente[129].

5.1.2 Delitos asociados a la informática

En esta categoría se incluyen las estafas y fraudes cometidos en Internet del artículo 248 del Código Penal. Algunas de las prácticas más destacables[130] son:

- Subastas en Internet: puede ocurrir que no se reciba el producto por el que se pujó o que se reciba uno con menos valor.
- Uso no autorizado de tarjetas de crédito.
- Ofertas fraudulentas con títulos atractivos relacionados con ganancias económicas rápidas.
- Prestación de servicios inexistentes, como la promoción de un alojamiento que luego no existe.

Los delitos asociados a la informática fueron una novedad que apareció con la llegada del Internet. La inclusión de estos en el Código Penal de 1995 resultó una respuesta al uso criminal de las nuevas tecnologías[131].

5.1.3 Delitos de contenido

Como indica su nombre, en este apartado se incluyen los delitos que persiguen la creación, publicación y distribución de contenidos ilegales.

[129] Posada Maya, R. (2013). El delito de acceso abusivo a sistema informático. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías* (pp. 131-132).
[130] Antón Oneca, J. (1958). Voz «Estafa». *Nueva Enciclopedia Jurídica*, Francisco Seix (pp. 56 y ss).
[131] Ídem 118.

Se distinguen dos tipos de contenidos[132]: 1) contenidos nocivos o perjudiciales para el receptor; 2) contenidos ilícitos.

> Mientras que los primeros, a pesar de que pueden ser ofensivos o inadecuados para el receptor debido a ideologías o juicios de valor del emisor, no son delictivos, los contenidos ilícitos abarcan aquellos que no estén de acuerdo a la ley.

Algunos ejemplos de estos delitos son la pornografía infantil (art. 189 CP), el acoso en línea (no está previsto como tal pero se incluye en el art. 172 ter.), la incitación al odio (art. 510 CP) y la difamación en línea (art. 205, 206 y 208 CP).

Cabe destacar que los delitos de contenido suponen un problema cada vez más frecuente y grave en esta era digital, pues cada vez hay más personas que pasan tiempo *online*, por lo que los responsables de estos delitos lo tienen más más fácil para escoger un objetivo. Asimismo, el anonimato y, por ende, la facilidad que hay para ocultar la identidad real en Internet no facilitan el rastreo y proceso de los sujetos activos de estos delitos[133].

5.1.4 Delitos relativos a las infracciones contra la propiedad intelectual y derechos conexos

En esta categoría se recogen los delitos más habituales en Internet. Se encuentran en los artículos 270 y ss. del Código Penal[134] y se incluye: la reproducción, el plagio, la distribución o comunicación pública de una obra literaria, artística o científica—o su transformación—, sin la autorización de los titulares de los correspondientes derechos. No es desconcertante saber que, con el asentamiento de la informática, este tipo de delitos se expandieron como nunca se había hecho antes, pues la rapidez de transfusión de datos lo ha hecho posible.

Cabe apuntar que en el área de la propiedad intelectual existe una clara internacionalización respecto a su protección y, además, también hay organizaciones creadas con el fin de preservar estos derechos[135].

Por otro lado, el marco legal que engloba la comisión de estos delitos en España—aparte del Código Penal—se manifiesta en la Ley de Propiedad Intelectual, cuyo Texto Refundido fue aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y ha sido modificado en diversas ocasiones posteriores.

---

[132] De Miguel Asensio, P.A (2001). *Derecho Privado de Internet* (pp. 538 y ss). Civitas.
[133] Brenner, S. W. (2011). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Edward Elgar Publishing.
[134] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444). Modificada por la Ley Orgánica 5/2010, de 22 de junio. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-9953
[135] Organización Mundial de la Propiedad Intelectual (OMPI) o Sociedad General de Autores y Editores (SGAE).

5.2 Discusión entre el *hard* y el *soft law*

Como hemos visto, los delitos cibernéticos se definen como «*actitudes ilícitas que se tiene a la cibernética como instrumento o fin*»[136]. Estos se cometen por medio de Internet con la ayuda de dispositivos electrónicos y, generalmente, afectan al patrimonio y/u honor de las víctimas.

Antes de hacer un comentario, recordemos la diferencia entre el *hard* y el *soft* law. El término «*hard law*» engloba las leyes y normas que tienen una fuerza vinculante y que son de obligado cumplimiento, mientras que el término «*soft law*» se refiere a las normas de conducta sin fuerza vinculante pero con efectos prácticos[137]. En el contexto del cibercrimen, el «*soft law*» se refiere a las normas y reglas de las propias redes sociales, que regulan el uso y manejo de sus plataformas.

El «*hard law*» es necesario para regular y sancionar los cibercrímenes, mientras que el «*soft law*» es útil para fomentar una cultura de respeto y protección de la privacidad y la seguridad en línea. Es decir, ambos tipos de normas son importantes para abordar el cibercrimen, dado que el *hard law* proporciona un marco legal sólido para perseguir y sancionar a los delincuentes, mientras que el *soft law* puede proporcionar orientación y mejores prácticas para prevenir el delito y proteger a los usuarios de Internet[138].

[136] Téllez Valdés, J. (1998) Delitos Cibernéticos. *Revista Iberoamericana de Derecho Informático*, 27-29 (pp. 113-122).

[137] Pastore, B. (2014). Soft Law y las Teorías de las Fuentes del Derecho. *Soft Power*. Università degli Studi di Ferrara, 1(1).

[138] Tapia Sánchez, L. S. (2022). Tecnología y Derecho una mirada al Comercio Electrónico, el Cibercrimen y el Soft Law. *AIS: Ars Iuris Salmanticensis*, 10(1), (pp. 199–226). Recuperado el 30 de abril de https://doi.org/10.14201/AIS2022101199226

6. Conclusiones

Para poder dar un cierre a este trabajo, es necesario retrotraerse al objetivo planteado en el inicio: el estudio del derecho digital, las amenazas que pueden surgir y los mecanismos para prevenir peligros y riesgos.

Después de haber realizado un análisis sobre la nueva era digital en la que estamos inmersos, incluyendo el marco jurídico con el que contamos actualmente y las amenazas potenciales que existen en este nuevo contexto, podemos concluir que el ciberderecho o derecho digital es un área a la que se deberá prestar más atención próximamente, pues cada vez va siendo más necesaria una disciplina jurídica que recoja todas las posibilidades que plantea la Red.

Tal y como se ha comentado en más de una ocasión a lo largo del documento, el hecho de que no exista un marco jurídico armonizado a nivel global que pueda abordar adecuadamente los nuevos desafíos que se abren con las nuevas tecnologías supone un obstáculo importante para poder mantener el ritmo al que se evoluciona como sociedad. Si bien es cierto que existe regulación que prevé ciertas novedades, cada ordenamiento dispone de su propio texto normativo; a pesar de la existencia de convenios, no hay un cuerpo normativo globalizado y común para todos los usuarios de la Red, por lo que, a pesar de que se cometan delitos o lesiones de derechos en un mismo lugar—el ciberespacio—, no en todos los Estados se procede de la misma manera.

Cabe tener en cuenta que Internet y las nuevas tecnologías, irremediablemente, forman parte de un mundo paralelo al real. La globalización con la que contamos actualmente, unida a las posibilidades que ofrece el ciberespacio, manifiestan la urgencia de la implementación de un marco legal en el que el ciberderecho se contemple como una disciplina jurídica autónoma y globalizada, dado que se van a materializar en un futuro próximo supuestos nuevos de acuerdo con la nueva tecnología, y estos requerirán de una respuesta coherente y adecuada para poder abordarlos.

Si bien el ciberderecho ya es una disciplina que empieza a tener más reconocimiento, no se puede considerar que esté suficientemente consolidada como para ser valorada como una herramienta esencial en la sociedad de hoy en día, por lo que aún queda mucho por hacer para conseguirlo.

7. Referencias y bibliografía

7.1 Normativa

Convenio 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. Ratificado por España el 27 de enero de 1984. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2000). Disponible en https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

Convenio sobre la Ciberdelincuencia del Consejo de Europa, hecho en Budapest el 23 de noviembre de 2001. Ratificado por España el 20 de mayo de 2010. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Constitución de EE.UU. Recuperado el 26 de diciembre de 2022 de: https://www.archives.gov/founding-docs/constitution

Privacy Act of 1974. Recuperado el 26 de diciembre de 2022 de: https://www.justice.gov/opcl/privacy-act-1974

Computer Fraud and Abuse Act of 1986 (CFAA) https://www.congress.gov/bill/99th-congress/house-bill/4718/text

Gramm-Leach-Bliley Act, also known as Financial Services Modernization Act of 1999 (GLBA). Recuperado el 26 de diciembre de 2022 de https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

California Consumer Privacy Act of 2018 (CCPA). Recuperado el 19 de abril de: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. *Diario Oficial de la Unión Europea, L 257/73-142*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=ES

Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015R2120

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). *Diario Oficial de la Unión Europea, L119/1-88*. Recuperado el 12 de abril de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Directiva 2000/31/CE, del Parlamento Europeo y Consejo de 8 de junio de 2000. Directiva relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular el comercio electrónico en el mercado interior. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000L0031&from=ES

Resolución del Parlamento Europeo, de 3 de octubre de 2017, sobre la lucha contra la ciberdelincuencia (2017/2068(INI)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0361_ES.html

Comisión Europea (2020, 19 de febrero), *Shaping Europe's Digital Future*. COM. 67 (p. 2). Recuperado el 20 de diciembre de 2022 https://eufordigital.eu/wp-content/uploads/2020/04/communication-shaping-europes-digital-future-feb2020_en_4.pdf

Constitución Española. (1978). Artículo 18. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-9953

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales

vigentes sobre la materia. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

7.2 Jurisprudencia

Sentencia de la Corte Suprema de Canadá de 28 de junio de 2017. Caso *Google Inc.* v. *Equustek Solutions Inc*. SCC 34. Recuperado de https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do

Sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, asunto C-293/12. Recuperado de https://curia.europa.eu/juris/document/document.jsf;jsessionid=0A176C3D89F9EFC98B28C32B1C820D44?text=&docid=150642&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=3191586

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 13 de mayo de 2014. Asunto C-131/12. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0131&from=ES.

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera) de 6 de octubre de 2015. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62014CJ0362

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera) de 3 de octubre de 2019. Asunto C 18/18. Recuperado de https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62018CJ0018

Sentencia del Tribunal Constitucional Federal alemán del 15 de diciembre de 1983. Recuperado el 22 de abril de 2023 de: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

Sentencia del Tribunal Constitucional 254/1993, de 20 de julio. Recuperado el 12 de abril de: https://www.boe.es/buscar/doc.php?id=BOE-T-1993-21425

Sentencia del Tribunal Constitucional 60/1998, de 16 de Marzo. Boletín Oficial del Estado, núm. 96, de 22 de abril de 1998. Recuperado de: https://hj.tribunalconstitucional.es/es/Resolucion/Show/3562

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

Sentencia de la *Queen's Bench Division (Administrative Court)* del 3 de abril de 2007. Caso CO/5897/2006. Recuperado el 30 de abril de: https://vlex.co.uk/vid/mckinnon-v-united-states-793612009

Sentencia del Tribunal Supremo 803/2017, de 11 de Diciembre. Recuperado de: https://www.poderjudicial.es/search/AN/openCDocument/af49061622914e2008edc0d7f106b1b14dd0d95d43218c7e

Sentencia de la Q*ueen's Bench Division (Administrative Court)* del 12 de octubre de 2021. Caso CO/150/2021. Recuperado el 30 de abril de https://www.judiciary.uk/wp-content/uploads/2022/07/USA-v-Assange-judgment101221.pdf

7.3 Artículos, obras y textos jurídicos

Abomhara, M. and Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. Artículo presentado en la *International Conference on Privacy and Security in Mobile Systems (PRISMS)* de 2014 (pp. 1-8), Aalborg, Denmark. Recuperado el 18 de marzo de 2023 de https://doi.org/10.1109/PRISMS.2014.6970594

Aranda, F. J. (2021) *Derecho y nuevas tecnologías: la influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español.* Dykinson, S.L.

Arenas Ramiro, M.; Ortega Giménez, A. (2019). *Protección de Datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*. Sepin.

Antón Oneca, J. (1958). Voz «Estafa». *Nueva Enciclopedia Jurídica*, Francisco Seix (pp. 56 y ss).

Barrio Andrés, M. (2011). La ciberdelincuencia en el Derecho español. *Revista de las Cortes Generales*, (83) (pp. 273-305). Recuperado el 1 de mayo de https://doi.org/10.33426/rcg/2011/83/473

Barrio Andrés, M. (2018): *Ciberderecho: Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*. Tirant lo Blanch.

Barrio Andrés, M. (2021). Génesis y desarrollo de los derechos digitales. *Revista de las Cortes Generales* (pp.197-233). Recuperado el 24 de diciembre de 2022 en: https://doi.org/10.33426/rcg/2021/110/1572

Barrón Arniches, P. (2019): *La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)*, *Cuadernos europeos de Deusto*, 61 (pp. 33-34).

Brenner, S. W. (2011). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Edward Elgar Publishing.

Calder, A., & Watkins, S. (2016). *EU GDPR: A Pocket Guide*. IT Governance Publishing.

Campuzano, H. (2018). Cuatro décadas de protección jurídica del derecho a la privacidad frente a las TIC: del derecho a la autodeterminación informativa al derecho al olvido digital, en Álvarez, L. Y Punset, R. (Eds.), *Cuatro décadas de una constitución normativa (1978-2018)*, (pp. 133-157). Thomson Reuters-Aranzadi.

del Carril, E. & Deluca, S. (2017). Cooperación internacional en materia penal en el MERCOSUR: el cibercrimen. *Revista de la Secretaría del Tribunal Permanente de Revisión*, 5(10) (pp.13-28).

Crawford, S. (2013). Captive audience: *The telecom industry and monopoly power in the new gilded age* (pp. 113-114). Yale University Press.

De Miguel Asensio, P.A (2001). *Derecho Privado de Internet* (pp. 538 y ss.). Civitas.

De Terwangne, C. (2012). Privacidad en internet y el derecho a ser olvidado/derecho al olvido, *Revista de Internet, Derecho y Política*, 13 (p. 53).

Eichenhofer, J., & Gusy, C. (2017). Chapter 6: Courts, privacy and data protection in Germany: Informational self-determination in the digital environment. En *Courts, Privacy and Data Protection in the Digital Environment*. Cheltenham, UK: Edward Elgar Publishing. Recuperado el 21 de abril de 2023 de https://doi.org/10.4337/9781784718718.00013

Faraj, S.; Renno, W.; Bhardwaj, A. (2021). Unto the Breach: What the COVID-19 Pandemic Exposes about Digitalization. *Journal of Information and Organization*, 31(1), artículo 100337. Recuperado el 20 de diciembre de 2022 de https://doi.org/10.1016/j.infoandorg.2021.100337

Feiler, L., Forgó, N., & Weigl, M. (2018). *The EU General Data Protection Regulation (GDPR): A Commentary*. CH Beck.

Hidalgo, A. (2020). *Derecho digital en la Unión Europea: techlaw y mercado único digital en la década 2010-2020*. Comares.

Hildebrandt, M. (2018). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. Forthcoming in Theoretical Inquiries of Law 2019, 19(1) *SSRN Electronic Journal*. Recuperado el 22 de abril de: http://dx.doi.org/10.2139/ssrn.3081776

IT Governance Publishing. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*.

Jacob, V. (2018). The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. *The University of Chicago Law Review*, 85(2), (pp. 535-582).

Kuner, C. (2007). *European data protection law: corporate compliance and regulation*. Oxford University Press.

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2018). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.

Leo-Castla, J.I. (2019, octubre 4). Compliance y gestión del riesgo normativo en el contexto del Reglamento europeo de protección de datos. *La Ley.* Sección Ciberderecho, núm. 32. Recuperado el 8 de diciembre de 2022 de https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAEAC1NwW7CMAz9GnJBmtqxipMvXY8IIah2dxMrjRRiSJxC_37ewPKT_eT3_O6V8jrSU8CyC563N0oYTVkTp_UKY65kBKcCzWZvW8WnQSsV48AWvvZ_JCw04gSN4ewo96tuwoLxTAXatutMmflxxCV4lMCpx_x6G5yDYWy0dtptZxbKRQXwEzwlITMHPx8U8tIXwmznE3oCDa9X1fAHltvzfemriLonSZd_bmzUOaDQN0ZK7p37C14AdqryAAAAWKE

Lohr, S. (2015). *Data-ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else*. HarperBusiness.

Martínez Quirante, R. y Rodríguez Álvarez, J. (2018). *Inteligencia artificial y armas autónomas letales* (p.108). Trea.

Martínez-Quirante, R. y Rodríguez-Álvarez, J. (2019). *Towards a new AI race. The challenge of lethal autonomous weapons systems (LAWS) for the United Nations* (p.110). Thomson-Reuters Aranzadi.

Mayer-Schönberger, V. y Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Ed. Houghton Mifflin Harcourt.

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for internet freedom* (p. 135). Basic Books.

McChesney, R. (2013). *Digital disconnect: How capitalism is turning the internet against democracy* (p. 181). The New Press.

Miró Llinares, F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons Ediciones Jurídicas y Sociales. Recuperado el 28 de abril de https://elibro.net/es/ereader/uab/58741?page=26

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the human element of security*. John Wiley & Sons.

Mitnick, K., & Simon, W. L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons.

Morón Lerma, E. (1999) *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*. Aranzadi (p. 42).

Mueller, M. N. (2010). *Networks and States. The Global Politics of Internet Governance*. The MIT Press (p.9).

Navas Navarro, S. (2015). *La Personalidad virtual del usuario de Internet Susana Navas Navarro*. Tirant lo Blanc.

Navas Navarro, S. (2016). Computación en la nube: big data y protección de datos personales. *InDret*, (4).

Papier, H.-J. (2009). The Development of Data Protection in Germany. *International Data Privacy Law*, 1(3), (pp. 150-160).

Pastore, B. (2014). Soft Law y las Teorías de las Fuentes del Derecho. *Soft Power*. Università degli Studi di Ferrara, 1(1).

Pauwels, E. (2011). El principio de buena fe en el derecho de Internet. *Revista de derecho privado*, (20), (pp. 63-89).

Penney, J.W. (2009). Understanding the New Virtualist Paradigm. *Journal of Internet Law*. Recuperado el 18 de diciembre de 2022 de https://ssrn.com/abstract=1355392

Posada Maya, R. (2013). El delito de acceso abusivo a sistema informático. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías* (pp. 131-132).

Rallo Lombarte, A. (2014). *El derecho al olvido en internet. Google versus España*. Centro de estudios constitucionales.

Rebollo, L. (2008). *Vida privada y protección de datos en la Unión Europea*. Dykinson.

Reed, D. (2009). *The end of end-to-end: Preserving the architecture of the internet in the broadband era* (p. 13). The Association for Computing Machinery.

Richards, N. M. (2015). *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford University Press.

Rifkin, J. (2014). *La sociedad de coste marginal cero*. Paidós.

Schaar, P. (2008). The Fundamental Right to Data Protection. *Common Market Law Review*, 45(4), (pp. 1103-1123).

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Sieber, U. (2019). *Datenschutzrecht*. C.H.Beck.

Simón Castellano, P. (2015) *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014* (p. 185). Bosch

Solove, D. J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Ed. Yale University Press.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security*. Yale University Press.

Stewart, D. (2018). Recent Developments in U.S. Cyberlaw. *Agenda internacional*, 25(36), (p.113.)

Suo, H., Wan, J., Zou, C., y Liu, J. (2012). Security in the Internet of Things: A Review. En la *International Conference on Computer Science and Electronics Engineering* (ICCSEE) de 2012 (pp. 648-651). Hangzhou, China. Recuperado el 18 de marzo de 2023 de: https://doi.org/10.1109/ICCSEE.2012.373

Tapia Sánchez, L. S. (2022). Tecnología y Derecho una mirada al Comercio Electrónico, el Cibercrimen y el Soft Law. *AIS: Ars Iuris Salmanticensis*, 10(1), (pp. 199–226). Recuperado el 30 de abril de https://doi.org/10.14201/AIS2022101199226

Teubner, G. (2017). *El derecho como sistema autopoiético de la sociedad global*. Olejnik.

Téllez Valdés, J. (1998) Delitos Cibernéticos. *Revista Iberoamericana de Derecho Informático*, 27(29), (pp. 113-122).

Touriño, A. (2014). *El derecho al olvido y a la intimidad en internet*. La Catarata.

Troncoso Reigada, A. & González Rivas, J. J. (2019). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*. Aranzadi.

Turkle, S. (1995). *La vida en la pantalla: la construcción de la identidad en la era de Internet*. Paidós.

Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press.

Van Schewick, B. (2012). *Internet architecture and innovation* (p. 100). MIT Press.

Voigt, P. & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Springer International Publishing.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. John Wiley & Sons.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), (pp. 23-30). Recuperado el 15 de marzo de 2023 de https://doi.org/10.1016/j.clsr.2009.11.008

Wu, T. (2011). *The master switch: The rise and fall of information empires* (p. 311). Vintage Books.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

7.4 Páginas web y otros documentos

ICANN. Recuperado el 5 de febrero de 2023 de https://www.icann.org/es/system/files/files/getting-to-know-icann-quicklook-30apr20-es.pdf

ISOC. Recuperado el 5 de febrero de 2023 de https://www.internetsociety.org/es/about-internet-society/

World Wide Web Consortium. Recuperado el 5 de febrero de 2023 de https://www.w3.org/