cei international affairs
escuela diplomática de Barcelona

CENTRO ADSCRITO

UNIVERSITAT DE BARCELONA

PROTECCIÓN DE DATOS EN LA ESFERA PRIVADA. RETOS Y PERSPECTIVAS DEL MARCO LEGISLATIVO EUROPEO.

-Trabajo de Fin de Máster-

Máster Universitario en Diplomacia y Organizaciones Internacionales

Autor/a: Cecilia Alonso Vigil

Tutor/a: Daniel Iglesias Márquez

Fecha de entrega: 10 de mayo de 2014

RESUMEN

La progresiva transformación digital de la sociedad ha llevado a una proliferación de los mercados de datos, en una esfera que involucra a Estados, empresas e individuos a partes iguales. Mediante esta investigación, se pretenden esclarecer los orígenes de esta digitalización, y su impacto para los actores internacionales mencionados. En tal sentido, se destaca la importancia de la protección de datos, con el objetivo de generar una cierta conciencia sobre su creciente valor en el mercado y los consecuentes peligros que puede acarrear su sobreexposición indiscriminada. Siguiendo esta línea, resulta necesario alcanza un equilibrio justo entre la protección del ciudadano y la expansión económica y social del sector privado. Para ello, es indispensable promover la cooperación entre Estados y entidades supranacionales en el desarrollo de una normativa que regule las relaciones en el ciberespacio. Así pues, esta investigación analiza la labor de la Unión Europea a este respecto, y trata de plasmar los posibles retos que aún están pendientes de resolver para salvaguardar los intereses de los ciudadanos.

ABSTRACT

The progressive digital transformation of society has led to a proliferation of data markets, in a sphere that involves states, companies and individuals on equal terms. This research aims to shed light on the origins of this digitisation and its impact on the aforementioned international actors. In this sense, the importance of data protection is highlighted, with the aim of generating a certain awareness of its growing value in the market and the consequent dangers that its indiscriminate overexposure may entail. Along these lines, it is necessary to strike a fair balance between the protection of the citizen and the economic and social expansion of the private sector. To this end, it is essential to promote cooperation between states and supranational entities in the development of regulations governing relations in cyberspace. This research analyses thus the work of the European Union in this respect, and attempts to capture the possible challenges that remain to be met in order to safeguard the interests of citizens.

Palabras clave:

Autoridades de control, *Big data*, Cambridge Analytica, consentimiento, *cookies*, descentralización, Directiva ePrivacy, elaboración de perfiles, gobernanza multiactor, identificación y re-identificación, inferencia de información, mercado de datos, minimización de datos, *paywalls*, protección de datos, Reglamento IA, RGPD, transformación digital, vulnerabilidad.

ÍNDICE

ABREVIATURAS

AEPD – Agencia Española de Protección de Datos

ARPANET – Red de la Agencia de Investigación de Proyectos Avanzados

DDoS – Denial-of-service attack (Ataque de Denegación de Servicio)

EEE – Espacio Económico Europeo

GPAI – General Purpose Artificial Intelligence (Inteligencia Artificial de Propósito General)

HTML – HyperText Markup Language (Lenguaje Marcado del Hipertexto)

IA – Inteligencia Artificial

IP – Internet Protocol (Protocolo de Internet)

IoT – Internet of Things (Internet de las Cosas)

LAN – Local Area Network (Red de Área Local)

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

NCP – Network Control Protocol (Protocolo de Control de la Red)

OCDE – Operación para la Cooperación y el Desarrollo Económicos

OTAN – Organización del Tratado del Atlántico Norte

OTT – Over-The-Top (referidos a servicios de transmisión libre)

P2P – peer to peer (entre particulares)

REFIT – Regulatory Fitness and Performance Programme (Programa De Adecuación y Eficacia De La Reglamentación)

RGPD – Reglamento General de Protección de Datos

TCE – Tratado constitutivo de la Comunidad Europea

TCP – Transmision Control Protocol (Protocolo de Transmisión de Control)

TJUE – Tribunal de Justicia de la Unión Europea

UE – Unión Europea

VPN – Virtual Private Network (Red Privada Virtual)

INTRODUCCIÓN

La superposición del espacio físico con el aún naciente espacio virtual ha llevado a una transformación de la sociedad, dando lugar a una nueva dimensión más cercana, accesible e inmediata para todos; un nuevo mundo, en cierto sentido más homogéneo, donde las distancias se acortan y las posibilidades se multiplican. Pero al mismo tiempo se trata de un espacio en constante cambio y expansión; un espacio, donde el intuitivo funcionamiento de sus servicios transmite a los usuarios una falsa sensación de control; y cuya integración absoluta en la cotidianeidad, unida a su aparente gratuidad, perpetúa la idea cuasi inconsciente, si bien errónea, de que los servicios ofrecidos en esta nueva dimensión son públicos, y no ofrecidos por entes privados. La generalización de este tipo de ideas entraña una serie de vulnerabilidades a la seguridad de los ciudadanos y de sus datos personales, y los perjuicios derivados de ellas aumentan progresivamente con el avance de la tecnología. Por este motivo, resulta vital implementar una regulación eficiente, que proteja al individuo ante tales vulnerabilidades.

La creencia de los que los servicios ofrecidos en Internet son gratuitos es, posiblemente, la primera equivocación que entraña un peligro de considerable. Ha de tenerse en cuenta que detrás de cada uno de estos servicios opera una empresa, cuyo objetivo no es en absoluto ser caritativa, sino obtener un beneficio económico. Por lo tanto, cada vez que no se exige una remuneración por los servicios ofrecidos, la corporación obtiene ganancias a partir de los datos de los usuarios; datos que, en la mayoría de las ocasiones, son obtenidos con el consentimiento voluntario de dichos usuarios, que creen entender a la perfección el funcionamiento de la red, simplemente porque navegan por ella con fluidez. Sin embargo, la realidad es que estos individuos no son conscientes de que, el aceptar el tratamiento de sus datos sin ningún tipo de criterio, les posiciona en una situación vulnerable, cuya gravedad aumenta con el avance de las tecnologías; en este sentido, no solo han de considerarse riesgos económicos, tales como el acceso a la cuenta bancaria del interesado o la modificación de precios en función de su capacidad económica, búsquedas e intereses; sino también potenciales daños morales, como la sobreexposición de información personal que pueda dañar la integridad del individuo, o convertirlo en un blanco más fácil para su manipulación.

La falta de pericia general, unida a los grandes intereses económicos detrás del comercio de datos, hacen que esta cuestión sea enormemente difícil de regular. No obstante, se trata asimismo de un asunto de gran vigencia y relevancia para el conjunto de actores que conforman la sociedad actual, en tanto que potenciales afectados por las amenazas en este espacio virtual.

Tomando todo esto en consideración, cabe preguntarse ¿cuán eficiente es la regulación vigente en su misión de proteger al individuo en la red? Para responder a esta pregunta, la presente investigación toma como referencia la legislación europea en el contexto de la actividad empresarial privada. Así pues, el objetivo general de este trabajo será estudiar el papel desempeñado por la Unión Europea, y el conjunto del Espacio Económico Europeo en su totalidad, en la implementación de dicha regulación. No obstante, para alcanzar este primer propósito es preciso tomar en consideración una serie de objetivos específicos. Por un lado, este trabajo pretende esclarecer el funcionamiento del conocido como “ciberespacio”, así como sus implicaciones; ello resulta esencial no solo para la navegación consciente del individuo por la red, sino también para desarrollar una legislación eficiente, que permita maximizar los beneficios de las nuevas tecnologías, pero teniendo como objetivo principal la protección del individuo. En este sentido, se estudiarán las dificultades para hacer frente a las amenazas en la red y, especialmente, para regularlas. Por otro lado, se hará un análisis de las principales

regulaciones europeas en materia de ciberseguridad y protección de datos, tomando como núcleo el Reglamento General de Protección de Datos. A este respecto no solo se investigará el contenido de la regulación en sí, sino que tratará de plasmarse su evolución a lo largo de los años, y su pertinente adaptación a los cambios sociales y tecnológicos. Por último, una vez asentado el marco puramente teórico, se estudiarán cuestiones más prácticas, analizando casos en los que se ven involucradas grandes compañías, tales como Netflix o el complejo de Meta, e identificando ciertos retos para la regulación europea.

Persiguiendo este objetivo, para la elaboración de esta investigación se ha realizado un análisis cualitativo a varios niveles. Por un lado, con el objetivo de asentar los conocimientos generales en torno al contexto tecnológico actual y su reglamentación, se ha realizado una revisión bibliográfica de fuentes académicas que han investigado con anterioridad las cuestiones más generales planteadas, incluyendo el ciberespacio, la transformación digital y la protección de datos. Por otro lado, se ha llevado a cabo un seguimiento de la actualidad europea en materia de regulación de protección del usuario en la red. Una vez identificadas las normativas más importantes para alcanzar el propósito de la investigación, se ha realizado un análisis exhaustivo de su contenido, así como de su proceso evolutivo, contrastando las disposiciones actuales con sus predecesoras. Por último, se ha recurrido nuevamente a fuentes académicas, desarrolladas por particulares o por grupos de trabajo, con el objetivo de analizar más en profundidad la aplicación de la normativa a casos reales y las posibles lagunas jurídicas existentes.

El presente trabajo se divide en tres partes. Así pues, el primer capítulo se centra las dificultades generales en la reglamentación del espacio virtual. En este sentido, se aborda la complejidad de regular esta nueva dimensión, dado el rápido avance de las tecnologías; la falta de una jurisdicción claramente delimitada; y la multiplicidad de actores que operan en la red, que además no siempre son identificables. Entre estos actores, se destacan especialmente las empresas, en tanto que centros de tratamiento constante de los datos de sus usuarios, y cuya actividad es, en cierto sentido, la base sustantiva de la legislación actual.

El segundo capítulo estudia las principales regulaciones desarrolladas en el marco del Espacio Económico Europeo, a saber, el Reglamento General de Protección de Datos, la Directiva sobre la privacidad y las comunicaciones electrónicas, la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, y la nueva Ley IA.

Por último, el tercer capítulo aborda los retos que aún quedan por resolver para lograr una legislación que garantice el cumplimiento su objetivo, que no es otro que la protección del individuo en el ciberespacio. Así, este último capítulo toma como referencia una serie de casos reales que reflejan de forma clara el impacto degradante de la sobreexposición y falta de protección de la información personal ante entidades privadas, y cuestiona, asimismo, las lagunas en cuanto a su regulación.

CAPÍTULO I. EL CIBERESPACIO, LA TRANSFORMACIÓN DIGITAL Y SU IMPACTO EN LAS EMPRESAS Y EL INDIVIDUO

La creación de Internet en la segunda mitad del siglo XX y su rápida expansión a partir de los años 90 trae consigo una transformación tecnológica que da comienzo a la "Era Digital" o "Era de la Información". Con ella, se producen una serie de cambios revolucionarios a nivel socioeconómico, dando lugar a una sociedad globalizada y profundamente interconectada, basada en la omnipresencia de las redes electrónicas. Así, Internet constituye una infraestructura, compuesta por redes de datos, que permiten el intercambio de información en un espacio virtual e intangible, denominado ciberespacio.

En este capítulo se tratará de plasmar la rápida transformación del mundo digital, inducida por los avances de Internet, y sus implicaciones en la sociedad actual. Para ello, se tomará como centro el concepto de los datos y su creciente valor en la economía mundial. Igualmente, se considerará el impacto de estos activos tanto para el usuario como para las empresas que operan con ellos.

Con este fin, se realizará un breve repaso histórico de la evolución tecnológica que ha conducido al panorama actual, especialmente en el contexto de la digitalización de las empresas. Para ello también se realizarán algunas explicaciones de conceptos técnicos relevantes, que faciliten la comprensión el fenómeno de la transformación digital. Asimismo, se esbozarán algunas de las amenazas más comunes para la protección de estos datos, y su impacto en la actualidad. Por último, se expondrán los motivos por los que resulta extremadamente complejo establecer un marco jurídico robusto que desincentive la proliferación de las amenazas en el contexto digital y merme su impacto nocivo.

1.1. Orígenes y expansión de Internet

Los orígenes de Internet[1] se remontan a 1969, cuando, en el contexto de la Guerra Fría, el Departamento de Defensa de EE. UU. creó una red de ordenadores para optimizar las comunicaciones militares y reducir sus vulnerabilidades. Esta primera red computacional recibió el nombre de ARPANET (Red de la Agencia de Investigación de Proyectos Avanzados). Las universidades vieron su potencial para la investigación y la colaboración y, ese mismo año, se estableció el primer nodo de conexión entre las universidades de California, Standford, Santa Bárbara y Utah. Así, se convirtieron en pioneras en el uso de la red tal y como lo conocemos actualmente[2].

No obstante, la comunicación entonces tenía ciertas limitaciones. Paralelamente a ARPANET se habían desarrollado otras redes, tales como CYCLADES[3] o NPL Mark I[4]. Cada una de estas redes utilizaba su propio protocolo NCP (Network Control Protocol)[5], lo que

[1] De *Internetworking*, "interconexión de redes"
[2] LEINER, B.M. et al. "A Brief History of the Internet". *Internet Society*, 1997, pp. 23-24.
[3] Red desarrollada en Francia, 1972.
[4] Red desarrollada en Gran Bretaña, 1969.
[5] Es un protocolo simple que gestiona las conexiones unidireccionales entre dos puntos.

dificultaba la conexión entre redes diferentes[6]. El protocolo NCP utiliza un sistema de direcciones de 12 bits[7] para identificar a los dispositivos en una sola red, es decir, admite hasta 4096 dispositivos[8]. Así pues, su alcance era apropiado para una pequeña red de investigación, pero con su crecimiento exponencial demostró tener una flexibilidad insuficiente. Por este motivo, en la década de 1970, comenzó a desarrollarse un nuevo protocolo que fuera más flexible y escalable. El resultado de este trabajo fue el modelo TCP/IPv4[9] (Transmision Control Protocol & Internet Protocol), que fue adoptado en 1981[10]. Este modelo consiste en un conjunto de protocolos con una dirección de 32 bits – admitiendo, por tanto, hasta 4.294.967.296 dispositivos[11]. El TCP/Ipv4 utiliza un sistema de direcciones IP que identifica ordenadores de diferentes redes, permitiendo una conexión más global y accesible al público[12].

A pesar del incremento de ordenadores conectados a Internet, el uso de la red todavía era algo limitado, pues servía meramente para transferir archivos y usar correo electrónico. Esto cambiaría en 1991, cuando se accede al primer navegador[13] de la historia, la Word Wide Web[14], una red global que simplificó el uso de Internet[15] gracias a la invención del HTML[16] (hipertexto) y los hipervínculos. Estos elementos reestructuran la información, proporcionando un acceso inmediato a la misma. Su funcionamiento se basa en la creación de enlaces entre archivos y documentos electrónicos – las conocidas páginas web –, que permiten al usuario navegar de forma intuitiva por la red, gracias a una distribución más gráfica del contenido, utilizando textos resaltados y/o subrayados o imágenes. Así, el uso de la red, que hasta entonces requería conocimientos técnicos, comenzó a ser más atractivo y fácil de comprender, permitiendo el acceso a un público más amplio, y fomentando su difusión[17].

En un principio, Internet era unidireccional, es decir, los usuarios no podían interactuar o contribuir, sino simplemente acceder a información, facilitada por un número limitado de creadores de contenido. Esta primera etapa se denomina Web 1.0, o "web estática"[18].

Con el desarrollo de la tecnología y la popularización de Internet, en la primera década de los 2000, la Web entró en su fase 2.0. La denominada "web social" se convirtió en una red bidireccional e interactiva, que permitía a los usuarios convertirse también en creadores de

[6] SRI International. "75 years of innovation: Internetworking". *SRI International*, 19 noviembre 2020.
[7] La longitud de una dirección determina el número de dispositivos que se pueden conectar a la red.
[8] LEINER, B.M. et al., *op. cit*., p. 4.
[9] Es un conjunto de protocolos más robusto que asegura una gestión de las conexiones entre varios puntos de manera fiable y ordenada. Se divide en varias capas para optimizar funcionamiento y lo garantiza, en gran medida, con la división de los datos en segmentos.
[10] MUELLER, M. L., "Ruling the Root. Internet governance and the taming of cyberspace". Cambridge, Massachussetts: *MIT Press*, 2002, p. 36.
[11] Cabe destacar que este número comienza a ser insuficiente, puesto que cada usuario puede acceder a Internet a través de distintos dispositivos, por lo que se está implementando un nuevo protocolo IPv6, de 128 bits, esto es 340 sextillones de dispositivos.
[12] MUELLER, M. L, *op. cit.*, pp. 32-34.
[13] Los navegadores web interpretan el código HTML y muestran el contenido de la página web en la pantalla del usuario.
[14] En desarrollo desde 1989, por el científico informático Tim Berners-Lee.
[15] CERN. *A short history of the Web*.
[16] Es un lenguaje de marcado, es decir, un tipo de lenguaje informático que se utiliza para describir la estructura y el contenido de un documento. Utiliza etiquetas para indicar cómo mostrar el contenido de una página web.
[17] KRUSE, O. et al. "Hypertexts, Hyperlinks, and the World Wide Web", en *Digital Writing Technologies in Higher Education*. Springer Nature Switzerland AG, Cham, Suiza: 2023. pp. 51-52.
[18] CHHETRI, B. & KUJUR, P. "Evolution of World Wide Web: Journey From Web 1.0 to Web 4.0". *International Journal of Computer Science Trends and Technology*, junio-marzo 2015, p. 134.

contenido, y compartir y editar dicho contenido en las páginas web. De esta manera, aparecen las primeras redes sociales[19], tales como Facebook, YouTube o Twitter[20], si bien la pionera fue Sixdegrees[21]. No obstante, en esta etapa, la actividad de los usuarios se veía limitada, en cierta medida, por un control centralizado, es decir, el ejercido por la autoridad competente en la plataforma que se estuviera utilizando. Asimismo, estas plataformas, que están completamente monopolizadas, se nutren de la actividad del usuario, a través de la recolección de gran cantidad de datos e información[22], lo que les permite maximizar sus ganancias[23].

Los avances más recientes promueven la creación de una web más inteligente, lo que da pie a la web actual, denominada Web 3.0 o "web semántica". Esta tercera fase, operativa desde 2010 se basa, principalmente, en la integración de tecnologías de inteligencia artificial (IA), que permiten una mayor adaptación a las necesidades del usuario mediante un análisis más personalizado de sus datos – por ejemplo, estudiando sus patrones de comportamiento y de decisión[24]. Así, los instrumentos de IA son capaces de procesar y comprender la información relevante, interpretándola y emitiendo respuestas cada vez más precisas, lo que proporciona a los usuarios una interacción más personalizada e inmersiva en Internet[25].

Finalmente, con el objetivo de hacer la web más segura, se introducen una serie de cambios que pretenden llevar a una ligera transformación de la web, que pasa a denominarse Web3 o "web descentralizada". Como su propio nombre indica, el incremento de interacciones en la red fomenta el deseo por una descentralización de la gobernanza de los datos, en oposición a las fases anteriores[26]. Este modelo se caracteriza, principalmente, por la integración de tecnologías *blockchain*[27] – esto es, la transferencia del control de la información a una red distribuida, eliminando la figura del intermediario. De esta manera, los usuarios operan en una red *peer-to-peer*[28] (P2P), y son sus propios equipos los que comparten la información de manera transparente, y almacenan y procesan los datos intercambiados entre ellos, sin depender de un servidor o punto de control que pueda valerse de su información[29]. No obstante, este modelo no se encuentra todavía completamente implementado.

Adicionalmente, en los últimos años se ha comenzado a hablar de una nueva Web 4.0, que permitirá al usuario sumergirse completamente en un entorno digital, a través de la creación de un mundo virtual. Así, la combinación de todas las nuevas tecnologías, podrán ofrecer una experiencia inmersiva en un entorno que entremezcle lo físico y lo digital. No obstante, este es todavía un proyecto en evolución[30].

Gracias a la constante evolución de Internet y a su mayor alcance, el número de usuarios se ha multiplicado de manera exponencial, superando los 5 000 millones, lo que representa al

[19] *Ibidem,* pp. 134-135.
[20] Creadas en 2004, 2005 y 2006, respectivamente.
[21] Creada en 1997, pero cerrada en el año 2001.
[22] A menudo, sin conocimiento del usuario.
[23] WENSHENG GAN, V. et al. "Web 3.0: The Future of Internet". *In Companion Proceedings of the ACM Web Conference 2023 (WWW '23 Companion),* 30 abril - 4 mayo 2023, p. 2.
[24] *Ibidem*, pp. 3-5.
[25] CHHETRI, B & KUJUR, *op. cit*., p. 135.
[26] WENSHENG GAN, V. et al., *op. cit*., p. 2.
[27] También llamado "tecnología de cadena de bloques".
[28] Red de pares o red entre iguales.
[29] WENSHENG GAN, V. et al., *op. cit*., p. 3.
[30] Comisión Europea. *Hacia la próxima transición tecnológica: la Comisión presenta la estrategia de la UE para liderar la web 4.0 y los mundos virtuales*, 11 de julio de 2023. [Comunicado de prensa].

62,5% de la población mundial[31]. De esta manera, ha transformado la interconexión mundial, introduciendo una serie de cambios a nivel socioeconómico, que afectan a Estados, organizaciones, empresas e individuos[32]. Así, brinda a los ciudadanos la oportunidad de acceder a una gran cantidad información, que les ayuda a estar al tanto de la actualidad, a formarse en distintas áreas de interés, a desarrollar nuevas perspectivas personales y a fundamentar la toma de decisiones. Desde el punto de vista social, cabe destacar el papel de Internet en la construcción de relaciones y comunidades de interés[33].

Desde el punto de vista empresarial, Internet ha abierto las puertas a un crecimiento sin precedentes, estableciendo redes de conexión globales que permiten a las empresas operar en diferentes lugares del mundo, facilitando a los usuarios el acceso a servicios de manera telemática, y posibilitando a los profesionales trabajar de la misma manera. Así, se impulsa el crecimiento de las propias compañías y del mercado en general. Además, las posibilidades de comunicación con otras empresas y profesionales fomentan la innovación a través de la promoción de la investigación y el acceso a información actualizada, lo que permite a su vez la toma de decisiones sólidas y fundamentadas. Asimismo, cabe mencionar el importante papel que juega Internet en el contexto de la publicidad, ofreciendo plataformas ideales para la difusión de campañas de marketing, cuyo impacto puede ser analizado y optimizado con base a los resultados obtenidos. Así pues, en términos generales, Internet ha ayudado a expandir el comercio, a reducir ciertos costes[34] y a aprovechar las oportunidades que brindan las constantes innovaciones tecnológicas[35].

De esta manera, Internet ha posibilitado la creación de un entorno de interacción, que basa su crecimiento en la participación y retroalimentación de sus usuarios, cimentado, a su vez, en el intercambio de datos[36]. Esta nueva dimensión de interoperabilidad va a recibir el nombre de *ciberespacio*.

Así pues, y aunque parece indudable que este espacio proporciona una serie de ventajas al crecimiento económico, a la productividad y a la prosperidad, el flujo constante de información puede traer consigo ciertas implicaciones negativas, especialmente en términos de seguridad y privacidad. Por este motivo, es importante desarrollar un marco regulador que permita aprovechar las oportunidades que brinda el ciberespacio, y proteja a los usuarios de sus posibles vulnerabilidades.

1.2. El ciberespacio y los retos para su regulación

El ciberespacio, por lo tanto, se revela como un símbolo de la globalización y del desarrollo, en tanto en cuanto permite interconexiones a nivel internacional y una expansión comercial. No obstante, a su vez, trae consigo una serie de riesgos difíciles de evadir. Se trata, además, de un entorno completamente incierto, puesto que no sigue las estructuras tradicionales de territorio

[31] Statista. *Número de usuarios de Internet en el mundo entre 2005 hasta 2022*. Statista, 2023.
[32] DANDAURA, S. & MBANSO, U. "The Cyberspace: Redifining a New World". *IOSR Journal of Computer Engineering*, mayo-junio 2015. p. 17.
[33] *Ibidem*., p. 18.
[34] Por ejemplo, costes de inventario o de comunicación, y en el caso de los clientes, costes de búsqueda.
[35] MAZÓN CALPENA, C. & PEREIRA, P. "Las tecnologías de Internet y las empresas: riesgos y oportunidades". *Navarra y la sociedad del conocimiento: actas del congreso*, Gobierno de Navarra, 2000. p. 105.
[36] DANDAURA, S. & MBANSO, *op. cit*., p. 17.

ni de gobernanza del espacio físico. Así pues, presenta grandes retos, no solo para la evasión de amenazas, sino también para su regulación en el marco del Derecho Internacional[37].

Cabe señalar que, mientras que el ciberespacio es una dimensión de creación muy reciente, y en constante evolución – siempre paralela al rápido crecimiento de la infraestructura de Internet – la elaboración de las normas que lo regulan requiere un tiempo de análisis y desarrollo mucho más prolongado. Así pues, toda regulación referente al ciberespacio está sujeta a constantes reformas para tratar de adaptarse a los avances de Internet, pero se implementa a un ritmo mucho más lento[38], por lo que, a pesar de los esfuerzos por mantenerse actualizada, siempre parece ir un paso por detrás.

Un desafío que surge en torno a la regulación de esta nueva dimensión reside en la falta de uniformidad en la propia definición de "ciberespacio", dado que la carencia de una conceptualización armonizada y estandarizada dificulta una delimitación del alcance de sus normas[39]. Así, el Departamento de Defensa de los Estados Unidos lo describe como "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" [un dominio global dentro del entorno de la información formado por las redes interdependientes de infraestructuras de tecnología de la información y datos residentes, incluidos Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados][40].

Por su parte, en 2018, la UE lo define en su marco de políticas de ciberdefensa como "the fifth domain of operations, alongside the domains of land, sea, air, and space" [el quinto dominio de operaciones, junto con los ámbitos terrestre, marítimo, aéreo y espacial][41]. También la OTAN lo reconoce como un *"*domain of operations" [dominio de operaciones][42].

A pesar de no existir una uniformidad, todas estas definiciones hacen referencia al ciberespacio en tanto que un quinto dominio global. Esto trae consigo una serie de implicaciones, que pueden suponer grandes retos para su regulación y, simultáneamente, para la protección de todos los actores que interactúan en él. Así pues, cabe destacar tres factores importantes: por un lado, la dificultad de determinar la jurisdicción imperante en el ciberespacio, dada su naturaleza descentralizada; por otro lado, las complejidades en su gobernanza dada la pluralidad de actores influyentes en su funcionamiento y regulación; y por último, y como resultado de los anteriores, la dificultad para atribuir responsabilidad ante la perpetración de un hecho ilícito.

[37] KOBRIN, J. S. "Territoriality and the Governance of Cyberspace". *Journal of International Business Studies*, vol. 32, núm. 4, 2001, p. 690.
[38] KRAUS, S. et al. "Digital Transformation: An Overview of the Current State of the Art of Research". *SAGE Open*, julio-septiembre 2021, p. 1.
[39] KOBRIN, J. S., *op. cit*. 697.
[40] THEOHARY, C. *Defense Primer:* Cyberspace Operations. *Congressional Research Service*. Diciembre, 2023, p. 1.
[41] Council of the European Union. *EU Cyber Defence Policy, 15585/14*. Bruselas, 18 de noviembre, 2014, p. 2.
[42] North Atlantic Treaty Organization. *Cyber defence*. Septiembre, 2023

1.2.1. Descentralización y jurisdicción en el ciberespacio

La existencia del ciberespacio entra en conflicto con las bases del Derecho Internacional Público establecidos en la Paz de Westfalia. Los principios westfalianos se basan en la concepción de un mundo dividido en Estados soberanos, acotados por fronteras geográficas que delimitan el territorio en el que pueden ejercer su jurisdicción y sus competencias de manera exclusiva. Así, se establecen los principios de soberanía estatal, no intervención en asuntos internos e igualdad de representación con base a la territorialidad de los Estados[43]. Este aspecto resulta problemático en la medida que el ciberespacio supone, inherentemente, una desterritorialización. Se trata de una dimensión transfronteriza, en la que interactúan actores independientemente de su ubicación geográfica real, y cuyas acciones pueden tener repercusiones en terceros Estados, lo que comporta dificultades para su regulación[44].

Por un lado, cada Estado tiene su propia tradición cultural, política y legal, y, por lo tanto, es casi impracticable concebir unas normas específicas que se adapten a los ideales y expectativas de todos ellos[45]. Si bien es cierto que, a través de negociaciones, es posible llegar a ciertos acuerdos generales acerca de lo que es permisible y lo que no en el ciberespacio, el cumplimiento de estas normas comunes se revela como un reto más grave y de mayor complejidad[46]. Esto es especialmente notorio en lo referente a los desacuerdos sobre qué jurisdicción debe aplicar en cada caso, teniendo en cuenta la naturaleza descentralizada del espacio[47].

La naturaleza descentralizada del ciberespacio se basa en la distribución de la infraestructura de Internet[48] en diferentes Estados, a través de redes de proveedores y servidores interconectados. Esto limita la soberanía de aquellos Estados que despliegan dicha infraestructura en otros territorios[49], dado que se ven vinculados, al menos parcialmente, al derecho de interno de los mismos[50].

Así, el hecho de que el ciberespacio sea una dimensión transfronteriza no implica que no exista realmente una vinculación entre el espacio físico y virtual; la infraestructura que permite la existencia del ciberespacio es material; las acciones que se perpetran se dirigen desde una ubicación geográfica concreta; y sus consecuencias también pueden tener impacto en el mundo tangible[51]. Sin embargo, pueden surgir discrepancias acerca de si la jurisdicción debe ejercerla el Estado desde el que se dirige el ataque, o el Estado en el que se recibe.

Sea como fuere, al referirse a delitos cometidos en el ciberespacio, cabría preguntarse cuán legítimo es conferir jurisdicción en base a estos criterios de territorialidad. La descentralización de la infraestructura de Internet acarrea grandes dificultades para localizar de

[43] KOBRIN, J. S., *op. cit*., p. 688.
[44] IMBROGNO, A. "Internet: camino hacia un derecho globalizado". *Cartapacio Universidad Nacional del Centro*, núm. 7, 2004, pp. 4-5.
[45] FINNEMORE, M. & HOLLIS, D. "Constructing norms for global cybersecurity". *The American Journal of International Law*, vol. 110:425, 2016, p. 466.
[46] *Ibidem*, p. 478.
[47] IMBROGNO, A., *op. cit*., p. 5.
[48] Aquella que permite la existencia del propio ciberespacio.
[49] Por otro lado, ofrecen otras ventajas a Estados con menos capacidad económica e infraestructural para valerse de esta redistribución y asegurar una mayor participación en el ciberespacio que les permite defender y salvaguardar sus intereses.
[50] KOBRIN, J. S., *op. cit*., pp. 688-689.
[51] *Ídem*.

manera exacta la ubicación desde la que actúa un usuario; para identificar al responsable en caso de perpetración de un hecho ilícito; y, en base a ello, para determinar qué Estado tiene jurisdicción para realizar su enjuiciamiento[52]. Así pues, si bien es cierto que existen mecanismos de ciberseguridad cada vez más desarrollados, no deben infravalorarse las capacidades técnicas de otros agentes altamente especializados[53].

1.2.2. Gobernanza multiactor del ciberespacio

Siguiendo esta misma línea, ha de tenerse en cuenta la dimensión *multiactor*[54] que gobierna el ciberespacio, y que implica no solo la participación de diferentes Estados, sino también la de otros actores del derecho internacional, es decir, gobiernos, organizaciones internacionales, entidades privadas e individuos – todos ellos tienen un poder influyente en la gobernanza del ciberespacio[55].

Esta incorporación de agentes no estatales a la gobernanza del ciberespacio se basa, mayoritariamente, en el hecho de que tienen unas habilidades técnicas, que les permite adaptarse y responder más eficazmente que los gobiernos a los retos emergentes. Al mismo tiempo, si bien su especialización aporta gran riqueza, no ha de desestimarse el papel de los Estados, que tienen, al menos presumiblemente, la obligación de velar por los intereses de la comunidad internacional de manera transparente y responsable; por su parte, las empresas y los individuos tienen, a lo sumo, una responsabilidad moral, que no ofrece ninguna garantía de cumplimiento[56].

En este sentido, es relevante considerar la dependencia que tiene Internet de los actores particulares especializados. Así pues, la evolución de Internet se sustenta, en gran medida, en la actividad de agentes individuales con amplios conocimientos técnicos, que tienen la posibilidad de implementar funciones antes inexistentes[57]. Con ello, surgen grandes avances en desarrollos de software y de aplicaciones. Pero, al mismo tiempo, abre la puerta a actividad maliciosa[58], que pueden desestabilizar el funcionamiento de la red, sortear bloqueos[59] y acceder a los datos que circulan por la red, utilizándolos para lograr un beneficio, ya sea económico, o meramente estratégico[60]. De esta manera, estos actores irían no solo un paso por delante de la legislación, sino incluso, en algunos casos, de las capacidades de técnicos de ciberseguridad.

Por último, cabría considerar las consecuencias de la naturaleza híbrida del ciberespacio, en tanto que dimensión simultáneamente pública y privada. Así, si bien se trata de un espacio abierto y de libre acceso, esta libertad está sujeta a ciertas condiciones. Por un lado, dependerá de la capacidad económica del usuario, que determinará si tiene accesibilidad

---

[52] *Ibidem*, p. 690.
[53] RAYMOND, M. & DENARDIS, L. "Multi-stakeholderism: anatomy of an inchoate global institution". *International Theory*, 2015, p. 598.
[54] *Multistakeholder.*
[55] RAYMOND, M. & DENARDIS, L., *op. cit*., p. 596.
[56] MATTLI, W. & WOODs. "The Politics of Global Regulation". *Capítulo 2. The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State*. Princeton University Press, New Jersey, 2009, pp. 44-88.
[57] RAYMOND, M. & DENARDIS, L., *op. cit*., p. 598.
[58] FINNEMORE, M. & HOLLIS, D., *op. cit*., pp. 447-448.
[59] Como aquellos que pueden constituir los sistemas de antivirus.
[60] En ámbitos sociales y políticos, por ejemplo.

a un dispositivo o a la infraestructura y conectividad necesaria para darle un uso práctico al mismo[61]. Por otro lado, es relevante considerar que la libertad de acceso y la apertura de este espacio permite la intervención de los mencionados actores maliciosos, que, paradójicamente, pueden tener la capacidad de limitar el acceso a otros usuarios[62].

De esta manera, la regulación del ciberespacio debe desarrollarse de mutuo acuerdo entre todos estos actores, de forma que logren un equilibrio que asegure la estabilidad, accesibilidad y seguridad del espacio global, y supere las tensiones que puedan emerger por discrepancias e intereses enfrentados.

1.2.3. Atribución de responsabilidad

La superposición de jurisdicciones, la descentralización y la gobernanza *multiactor* del ciberespacio suponen grandes retos para la atribución de responsabilidad ante la perpetración de un hecho ilícito. Así, resulta importante insistir en las dificultades para la identificación y enjuiciamiento de los atacantes en el ciberespacio[63]. A este respecto, destaca el rol que juega el anonimato. Con ello no solo se hace referencia al uso de un pseudónimo, sino a todas las técnicas que permiten ocultar la identidad de un individuo o de un grupo. En el contexto de los ciberataques esto puede implicar el uso de una VPN[64] que dificulte el rastreo de la actividad del usuario[65], o el uso de un *proxy*[66], que puede ocultar la dirección IP[67] de un dispositivo[68].

Además, la consumación de un ciberataque involucra a múltiples actores, pues, si bien la *culpa* debe recaer sobre el perpetrador, es *responsabilidad* de otros sujetos proteger los objetivos de un posible ataque y limitar los agravios derivados del mismo. Así, en cierta medida, se puede atribuir responsabilidad a los gobiernos con jurisdicción sobre los actores involucrados, los proveedores de servicios que alojan los sistemas atacados, y las empresas víctimas de un ataque[69].

1.3. Transformación digital en las empresas

La introducción de Internet se ha convertido en un hecho irreversible e inevitable a todos los aspectos. Así, hoy por hoy, parece imposible llevar una vida al margen de Internet, lo que exige la inmersión de todos los agentes en el ciberespacio. A raíz de este fenómeno, la información

[61] Actualmente, el 62,5% de la población tiene acceso a dispositivos conectados a la red, lo que constituye una desventaja para el 37,5% restante, en términos de acceso a la información y productos y servicios que promuevan el desarrollo.
[62] FINNEMORE, M. & HOLLIS, D., *op. cit*., pp. 447-448.
[63] HOLLIS, B. D. "A Brief Primer on International Law and Cyberspace". *Carnegie Endowment for International Peace*. Junio, 2021, pp. 3-4
[64] Por sus siglas, Red Privada Virtual. Permite navegar por la red de forma privada y segura, ocultando la dirección IP personal.
[65] Por ejemplo, asignando una dirección IP temporal no asociada a la identidad real del usuario, o que no registre la actividad en línea del usuario.
[66] Es un servidor que actúa como intermediario entre el dispositivo del usuario y el sitio web al que pretende acceder.
[67] Es decir, el sitio web solo puede ver la dirección del servidor proxy y no la del dispositivo del usuario.
[68] HOLLIS, B. D., *op. cit*., p. 3.
[69] FINNEMORE, M. & HOLLIS, D., *op. cit*., pp. 435-436.

experimenta una digitalización[70] – esto es, pasa de ser análoga a digital – de manera que pueda ser almacenada y difundida con mucha más inmediatez y eficiencia[71]. Uno de los agentes que opera con más volúmenes de datos digitales es la empresa.

1.3.1. Sistemas de información, Big Data y cookies

Ante la revolución tecnológica, las empresas se ven en necesidad de adaptarse, pues de no hacerlo, corren el riesgo de volverse obsoletas. Una serie de motivaciones impulsan esta adaptación, a nivel externo e interno de la empresa. Por un lado, a nivel externo, se basan mayoritariamente en las expectativas del consumidor, los requisitos específicos del fabricante o del proveedor y las diferentes regulaciones en vigor. Por otro lado, a nivel interno, se basan en deseos de optimizar su eficiencia e innovar en sus productos y servicios, con el fin de mejorar su productividad, reducir sus costes de producción, mantenerse resilientes contra los riesgos y, en general, conservar su competitividad en el mercado[72].

La puesta en marcha de estrategias de adaptación a los procesos de digitalización se denomina *transformación digital*. A este respecto, cabe insistir en que las innovaciones tecnológicas están en constante evolución, lo que obliga a las empresas a mantenerse alerta y preparadas para introducir cambios con la misma constancia – pero siempre sujetos a altos niveles de incertidumbre. Es por este motivo que las empresas deben tratar de desarrollar una estructura administrativa flexible, que facilite la adaptación[73].

Uno de los pilares de la transformación digital es la creación de sistemas de información. Estos, como su nombre indican, son sistemas informáticos que operan, de forma estructurada, con datos que obtienen tanto de sus clientes como a lo largo de su cadena de producción. Incluye, entre otros, el almacenamiento, administración, procesamiento y transmisión de estos *inputs*[74]. No obstante, la información con la que operan estos sistemas se ve completada con un fenómeno aún más revolucionario – el *Big Data*.

Big Data es un concepto que alude a volúmenes ingentes de información digital estructurada y no estructurada, como registros de redes sociales, datos de sensores y de transacciones, o localización. Estos datos son recopilados por diferentes actores en tiempo real y analizados extensamente con el uso de algoritmos, con el objetivo de inferir de ellos hechos y tendencias ocultas. Así, los sistemas de información de las empresas operan no solo con los datos que recopilan en sus bases de datos tradicionales, sino también con los *insights* más valiosos extraídos de *Big Data*, con el objetivo de optimizar sus procesos de producción, comercialización y toma de decisiones de forma estratégica[75].

Por otro lado, el instrumento más conocido en la recopilación de datos de usuarios en línea son las *cookies*. Las *cookies* operan de manera similar al *Big Data*, pero no se centran en conjuntos masivos de información, sino más bien en datos de navegación individual. Su objetivo inicial era recordar las credenciales de cada usuario para facilitar su acceso a la red,

[70] Se empieza a dar en los 2000 (remitir al resumen de Internet). Implica a su vez una automatización de procesos.
[71] KRAUS, S. et al. *op. cit.,* p. 4.
[72] *Ibidem*., p. 1.
[73] KRAUS, S. et al., *op. cit*., p. 5.
[74] *Ibidem*, p. 11.
[75] GIL, E. *Big Data, privacidad y protección de datos* [Recurso electrónico]. Madrid, España: Imprenta Nacional de la Agencia Estatal. Boletín del Estado: 2016. Capítulo 1. La Revolución del *Big Data*, p. 17. <https://www.aepd.es/sites/default/files/2019-10/big-data.pdf>

pero posteriormente se empezaron a utilizar con el fin de analizar los patrones de comportamiento del consumidor, para ofrecer una experiencia adaptada a sus gustos[76].

No obstante, el uso de estas tecnologías implica también un riesgo, especialmente, en lo que se refiere al acceso a datos de carácter personal. Esto no se limita a nombres y apellidos, sino una lista cada vez más amplia de información, que incluye, entre otros, el domicilio, datos bancarios, el número de la Seguridad Social, o incluso las interacciones en las redes sociales o el sonido y el tono de voz[77] – lo cual puede resultar problemático en la medida que permiten la identificación del individuo a través de su actividad en la red[78]. Estos supuestos deben ser abordados por las empresas, en tanto que recopiladoras y procesadoras de datos personales, puesto que la filtración o el mal uso de esta información puede traer consigo grandes perjuicios para el usuario, además de constituir una vulneración de su derecho a la privacidad y a la intimidad[79].

1.3.2. Potenciales riesgos y perjuicios de la ciberinseguridad

El procesamiento de estos datos por parte de la empresa está sujeto a una serie regulaciones y condiciones que se comprometen a salvaguardar los intereses de los consumidores. Sin embargo, los datos se convierten en un activo especialmente valioso y, por este motivo, los sistemas de información se convierten en objetivo susceptible de ser atacado a tres niveles distintos: vulnerabilidades, amenazas y riesgos[80].

Primeramente, una vulnerabilidad en el sistema implica un defecto de este que puede comprometer la seguridad de la información almacenada. En segundo lugar, las amenazas conllevan a una explotación de la vulnerabilidad, lo que provoca un daño o un perjuicio. Por último, el riesgo consiste en la probabilidad de que dicha amenaza culmine y provoque un daño o perjuicio[81].

Así pues, en primer lugar, el atacante debe identificar una vulnerabilidad en un sistema de información. Dada la complejidad de los códigos y protocolos existentes en la red, las vulnerabilidades son prácticamente inherentes a estos sistemas, por lo que se dan ataques de manera frecuente. De esta manera, entre las amenazas más típicas de una empresa, cabe mencionar: (1) ataques de secuestro de datos o *ransomware*, en los que un software introduce un virus en el sistema, bloqueando el funcionamiento del dispositivo y exigiendo una suma de dinero a cambio de restablecer el acceso al mismo; (2) ataques distribuidos de denegación de servicios o *denial of service attacks*[82], que privan al usuario acceder a un servidor o a un sistema de datos; (3) "programas maliciosos" o *malware*, que dañan al dispositivo impidiendo su funcionamiento o robando sus datos; (4) amenazas de ingeniería social o *phising*, provocadas por el error humano, al convencer al usuario de proporcionar información personal a través de una página web falsa[83]; (5) suplantación de identidad, en combinación con la anterior, para hacerse pasar por un agente de confianza para convencer al usuario de compartir sus datos

[76] *Ibidem*, p. 18.
[77] *Ídem*.
[78] Comisión Europea. *¿Qué son los datos personales?*
[79] Conceptos que se abordarán más en profundidad en el capítulo 2, especialmente en términos del Reglamento General de Protección de Datos.
[80] FINNEMORE, M. & HOLLIS, D., *op. cit*., p. 432-434
[81] *Ibidem,* p. 433.
[82] *DDoS* por sus siglas en inglés.
[83] Se refiere al uso de un enlace que descarga un *malware* en el dispositivo.

privados; (6) ataques a redes LAN inalámbricas o *wireless attack*, que, utiliza herramientas conjuntamente a los ataques (4) y (5) para tratar de acceder a una red inalámbrica y a otros dispositivos; (7) ataques a dispositivos del Internet de las cosas o IoT[84], que busca impedir el funcionamiento normal de Internet, dirigiendo ataques a toda infraestructura habilitante[85]; y (8) ataques a la cadena de suministro, que aprovechan la distribución de procesos para atacar al sector más vulnerable y crear un efecto en cascada que alcance al resto de los sectores de la cadena[86].

A todas estas amenazas, conocidas y ampliamente contempladas por los expertos en materia de ciberseguridad, cabe añadir otras no documentadas ni catalogadas. Estas se denominan "vulnerabilidades del día cero", porque no dan tiempo de reacción a los técnicos del sistema atacado[87], que tienen, literalmente, cero días para corregirla. Así, al tratarse de vulnerabilidades que no se han dado nunca antes, no se encuentran registradas, y son descubiertas inicialmente por el atacante. No existe una manera de combatirlas de forma inmediata, sino que una defensa debe ser desarrollada e instalada *a posteriori* en los equipos de los usuarios, lo que da tiempo al delincuente para explotar la vulnerabilidad. Esta amenaza resulta especialmente grave teniendo en cuenta que, en ocasiones, se tardan semanas o incluso años en identificarla, así como en descubrir las consecuencias del ataque sufrido[88].

1.3.3. Efectos de la ciberinseguridad

La circulación constante de datos de carácter personal, su análisis a través de nuevas tecnologías y el riesgo de que sean atacados debido a las vulnerabilidades de los sistemas de información, exponen al individuo a una serie de riesgos. Estos se clasifican, en la comunidad de seguridad informática, bajo las siglas CIA, refiriéndose a las pérdidas de confidencialidad, integridad y accesibilidad[89].

Por un lado, las pérdidas de confidencialidad pueden provocar perjuicios en la medida en la que se revele información personal que se pretendía mantener en privado. Esto incluye datos de carácter económico, tales como información de la cuenta bancaria o nóminas; pero también de carácter personal, como pueden ser aquellos referidos a la salud[90].

Por otro lado, las pérdidas de integridad se pueden dar ante la manipulación de los datos del usuario o la suplantación de su identidad. Estos ataques pueden dar lugar a pérdidas de confidencialidad; pero también consistir en perjuicios de tipo moral[91] u otros especialmente denigrantes, como aquellos que incluyen asuntos de naturaleza sexual.

---

[84] *Internet of things*.
[85] CANDO-SEGOVIA, M. R., y MEDINA-CHICAIZA, P. "Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica". *Cuadernos de desarrollo aplicados a las TIC*, 2021, p. 27-35.
[86] European Commission. *Infographic - Top cyber threats in the EU*. Febrero, 2023.
[87] FINNEMORE, M. & HOLLIS, D. *op. cit*., p. 432.
[88] *Ídem*.
[89] POPESCUL, D. "The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation", en Khalid S. Soliman (ed.) *Innovation and Knowledge Management: A Global Competitive Advantage* [Recurso electrónico]. Proceedings of The 16th International Business Information Management Association Conference. Kuala Lumpur, 29-30 junio 2011, p. 1139.
[90] GIL, E., *op. cit*., pp. 45-46.
[91] POPESCUL, D., *op. cit.,* p. 1139.

Por último, la privación de accesibilidad constituye una clara limitación de las posibilidades del usuario en términos de comunicación y acceso a información, así como a servicios completamente implantados en la sociedad actual, como pueden ser múltiples actividades laborales que requieran una conexión y un funcionamiento adecuado de Internet.

Velar por la seguridad informática y la protección de los datos acumulados en sus plataformas, es una responsabilidad de las empresas. No obstante, además del usuario, la propia entidad corporativa puede verse asimismo amenazada por estas potenciales pérdidas de confidencialidad, integridad y accesibilidad.

Esto puede llevar, por un lado, a filtraciones de información confidencial de la empresa y de sus profesionales, exponiendo, por ejemplo, información relativa a los impuestos sobre las ventas, o los números de licencia de los comerciales.

Además, por otro lado, cada vez son más comunes los robos de identidad corporativa, en los que los atacantes suplantan la marca en cuestión[92] para lucrarse de la misma, difundir información falsa, estafar a consumidores y dañar la imagen y reputación de la empresa, que, inevitablemente, pierde la confianza de sus clientes.

Por último, la privación de accesibilidad implica una clara desventaja competitiva para las empresas, en tanto en cuanto, se limita la comunicación con colaboradores y clientes, se ralentiza el proceso de producción y se priva a la entidad del acceso a información inmediata y actualizada.

1.4. Creación de normas en materia de ciberseguridad

La existencia de un ciberespacio, posibilitado por el desarrollo de la infraestructura de Internet, implica, por lo tanto, una serie de ventajas que son ya inherentes en la sociedad actual. No obstante, el acceso a estas oportunidades no está exenta de riesgos. Es por este motivo que, con el objetivo de mantener un equilibrio entre los beneficios y posibles perjuicios, es necesario desarrollar una serie de normas.

Los desafíos en la creación de estas normas se basan, mayoritariamente, en la naturaleza transfronteriza de los ataques, así como en la falta de consenso ante la pluralidad de actores reguladores. A esto se le suman otras cuestiones relevantes, como la rápida evolución de la tecnología y la falta de recursos, tanto financieros como humanos, para responder a ella[93].

No obstante, a pesar de estas dificultades, la creación de un marco normativo se revela como necesaria. Para desarrollarlo, deben tomarse en consideración varias cuestiones: a quién se dirige la norma; qué exigencias presenta; qué se considera apropiado e inapropiado dentro de tales exigencias; y las expectativas colectivas a nivel subjetivo de la comunidad[94].

De esta manera, una norma debe definir a qué comunidad va a estar destinada. Así, puede aplicarse a legislaciones nacionales, a grupos regionales de Estados (la Unión Europea), a Estados vinculados a través de un tratado bilateral (acuerdos entre China y EE. UU. contra el *ciberespionaje*) o Estados con ideas afines (OTAN); pero también a individuos (Convención de

[92] Por ejemplo, a través de una suplantación de identidad en una red social.
[93] DANDAURA, S. & MBANSO, U., *op. cit.*, p. 17.
[94] FINNEMORE, M. & HOLLIS, D. *op. cit*., p. 443.

Budapest) o a miembros dentro de la propia industria informática (desarrolladores de *software*, proveedores de servicios de Internet…)[95].

En segundo lugar, las exigencias de una norma pueden variar dependiendo de su especificidad. Por un lado, por el hecho de que pueden estar destinadas a la creación de obligaciones, prohibiciones o permisos. Por otro lado, porque cabe hacer una distinción en función de la rigidez de su contenido. Así, por ejemplo, en el marco de la UE se hace una distinción entre reglamentos, en tanto que instrumentos jurídicos vinculantes, que obligan a todos los miembros de la UE al cumplimiento de una serie de normas; decisiones, que solo son vinculantes para aquellos a quienes están dirigidas; directivas, que establecen una serie objetivos, pero su implementación es flexible; recomendaciones, que introducen especificaciones técnicas destinadas a lograr mejores prácticas; y los principios introducen consideraciones generales a tener en cuenta, pero no son determinativas, sino más bien orientativas[96].

Dada la complejidad de coordinar tales normas a nivel internacional, sea cual fuere su especificidad, lo más común hasta el momento ha sido la propuesta de normas voluntarias, no vinculantes, de manera que puedan evolucionar y adaptarse, y respetar las diferencias entre la política, cultura, religión o legislación nacional de cada Estado. Así, cada Estado tiene su propia normativa y, si bien es común que los Estados más afines desarrollen acuerdos, la mayoría son directrices no vinculantes[97].

No obstante, siguiendo en la misma línea, cabe destacar nuevamente el carácter evolutivo del ciberespacio, así como el de la elaboración de normas. Las normas deben entenderse como construcciones sociales, que existen en la medida que el colectivo que las adopta las considera apropiadas[98]. Así pues, las normas evolucionan en función de las necesidades del momento – con lo que dependerá de la capacidad de la comunidad en cuestión de identificar la existencia de un problema o un peligro digno de atención y promover el desarrollo de normas que prevengan y/o prohíban el comportamiento dañino y atenúen su impacto.

Por lo tanto, la creación de un marco normativo, si bien conlleva grandes desafíos, es necesario para mejorar los niveles de ciberseguridad y optimizar las ventajas que ofrece el uso de la red. Así, debe desarrollarse en una comunidad donde la peligrosidad de los ciberataques constituya un incentivo lo suficientemente fuerte como para alinear sus perspectivas, poner en común sus afinidades y desarrollar unas regulaciones, o en su defecto, directrices, estándares o principios que, a pesar de no ser vinculantes, puedan promover una mayor seguridad en el ciberespacio.

[95] *Ibidem*, pp. 439-440.
[96] Unión Europea (s.f.). *Tipos de legislación*.
[97] FINNEMORE, M. & HOLLIS, D., *op. cit*. p. 441.
[98] *Ibidem*, pp. 443-444.

CAPÍTULO 2. REGULACIÓN EN MATERIA DE SEGURIDAD Y PROTECCIÓN DE DATOS EN EL ÁMBITO DIGITAL EN LA UNIÓN EUROPEA

2.1. Contextualización: marco regulatorio europeo

Ante los avances de la tecnología y la multiplicación de oportunidades en el mercado, la Unión Europea[99] ha comenzado a establecer un marco normativo cada vez más robusto, que pretende impulsar la innovación digital. No obstante, las amenazas cibernéticas también se han multiplicado, por lo que, al mismo tiempo, este nuevo ordenamiento jurídico persigue salvaguardar la seguridad digital, con el fin de evitar comprometer la estabilidad de la región y asegurar la privacidad de los ciudadanos europeos[100].

En este contexto, la transformación digital se convirtió en una de las prioridades de la UE, hasta el punto de erigirse como una de las mayores promotoras de regulación en términos de digitalización. De esta manera, la transición hacia una economía digital pasó a ser una de las siete "iniciativas emblemáticas"[101] de la Estrategia Europa 2020, en concreto, la denominada Agenda Digital para Europa[102] de 2010. Esta Agenda Digital se convierte así en una de las prioridades fundamentales de la Unión[103], en tanto que promotora de una "economía inteligente, sostenible e integradora que disfrute de altos niveles de empleo, de productividad y de cohesión social"[104].

Siguiendo esta línea, en 2015 se reforzaron estas provisiones, mediante la elaboración de la Estrategia para el Mercado Único Digital, que, como su nombre indica, establece una serie de objetivos y líneas de actuación claves para crear un mercado único digital en la Unión[105]. Este plan de acción se mantiene abierto a reformas para adaptarse a la realidad del entorno contemporáneo, como la inducida por la pandemia de la COVID – 19; la crisis evidenció aún más la necesidad de promover la digitalización, lo que exigió una actualización de la estrategia en 2020, esta vez centrada en la recuperación económica y en la mejora de la resiliencia, y haciendo especial énfasis en sectores esenciales, tales como el sanitario[106].

Así pues, la UE se ha propuesto proporcionar a sus ciudadanos un espacio digital seguro, inclusivo y accesible que proteja sus derechos fundamentales y su privacidad, a la par que refuerce la competitividad y soberanía digital de Europa[107]. Esta visión se refleja en la elaboración de diferentes normativas, así como en la actualización de reglamentación obsoleta. Ejemplo de ello es la adopción en 2022 del paquete de Ley de Servicios Digitales, que engloba la Ley de Servicios Digitales y la Ley de Mercados Digitales[108]; a través de su implementación

[99] En adelante, UE o Unión.
[100] Consejo Europeo & Consejo de la Unión Europea (s.f.). *Un futuro digital para Europa.* 7 de febrero de 2024.
[101] Comunicación de la Comisión Europea 2020. *Una estrategia para un crecimiento inteligente, sostenible e integrador*. Bruselas, COM (2010) 2020 final, del 3.3.2010, p. 5.
[102] *Ibidem*, p. 6
[103] PÉREZ DE LAS HERAS Beatriz. "Hacia el Mercado Único Digital en la Unión Europea: retos y potencialidades para los entes subestatales", *Ekonomiaz,* núm. 98, 2020, p. 151
[104] Comunicación de la Comisión Europea, 2020, *op.cit*, p. 5
[105] Comisión Europea. "Paquete de la Ley de Servicios Digitales". *Configurar el futuro digital de Europa*, 16 de febrero de 2024. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/digital-services-act-package>
[106] *Ídem*.
[107] PÉREZ DE LAS HERAS Beatriz, *op. cit*., pp. 153-154.
[108] Entrada en vigor de forma progresiva desde el 16 de noviembre de 2022 y desde el 2 de mayo de 2023, respectivamente.

se deroga la directiva vigente hasta el momento, que databa del año 2000, con el fin de responder a las necesidades actuales y exigir responsabilidad, especialmente a las grandes plataformas, en cuestiones relacionadas con la propagación de desinformación y contenido dañino[109].

Asimismo, con el objetivo de proteger infraestructuras críticas – tales como redes y sistemas de información – y mejorar la resiliencia de las entidades públicas y privadas de la Unión, se desarrolla la Directiva NIS-2[110]. A través de esta, se pretende reforzar la cooperación entre los Estados miembro, estableciendo una normativa uniforme con medidas de seguridad claras de obligado cumplimiento y unas sanciones que desincentivan los potenciales ataques. Así pues, la directiva persigue simplificar las diferentes legislaciones vigentes, de manera que se favorezca la colaboración entre Estados y las operaciones entre empresas, para que puedan dar una respuesta armonizada y eficiente a los posibles ataques cibernéticos[111].

Si bien son muchas las normativas elaboradas – y en proceso de elaboración – por la UE, todas ellas tienen un núcleo común que puede considerarse la base del desarrollo tecnológico, y, por ende, normativo, en este contexto: el valor de los datos[112]. En este contexto, y con el objetivo de proteger los derechos fundamentales de los ciudadanos europeos, se desarrolla el Reglamento General de Protección de Datos. Mediante su implementación se disponen una serie de obligaciones a las empresas y organizaciones que operan con datos. Así, se aspira a conceder al individuo su derecho a tener bajo su control su información personal[113].

Por esta razón, a lo largo del presente capítulo se introducirán los principios y bases regulatorias de este reglamento, así como de normativas adicionales, en concreto, la directiva y propuesta de reglamentación para la protección de comunicaciones electrónicas, y la nueva Ley de Inteligencia Artificial.

2.2. Reglamento General de Protección de Datos

El avance de las nuevas tecnologías se ve impulsado por la proliferación de datos, y su consecuente procesamiento y difusión. Este fenómeno ha generado una economía de datos[114], en la que estos se han convertido en un activo cuyo valor se encuentra en un constante ascenso. Así, se espera que se triplique entre los años 2018 y 2025, y que se duplique asimismo el número de profesionales dedicados a este campo[115].

---

[109] COLOMINA Carme et. al, "The World in 2024: ten issues that will shape the international agenda", *CIDOB notes internacionals*, ISSN 2013-4428, 2023, pp. 7-8.

[110] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) núm. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto pertinente a efectos del EEE). *DOUE*, L 333/80, de 27 de diciembre de 2022.

[111] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) núm. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto pertinente a efectos del EEE). *DOUE*, L 333/80, de 27 de diciembre de 2022.

[112] Parlamento Europeo. "Una Agenda Digital para Europa". *Fichas temáticas sobre la Unión Europea*, 30 de noviembre de 2023.

[113] *Ídem*.

[114] Consejo Europeo & Consejo de la Unión Europea, *op.cit.*

[115] *Ídem*.

Bajo esta premisa, la UE establece un marco regulador cuyo objetivo es aprovechar y optimizar los beneficios de este nuevo paradigma revolucionario, al mismo tiempo que proteger los derechos de privacidad de los afectados.

2.2.1. Antecedentes y evolución

La importancia de la protección de datos personales es reconocida explícitamente en tanto que derecho de los ciudadanos europeos, desde la aprobación del Tratado constitutivo de la Comunidad Europea (TCE) en 1957[116], cuyo artículo 286[117] establecía que "[t]oda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"[118]. No obstante, este acuerdo no contemplaba aún cuestiones vinculadas a datos digitales, puesto que Internet ni siquiera había sido creado. Así pues, no existiría un instrumento jurídico con disposiciones referidas al tratamiento automatizado de datos hasta 1981, año de aprobación del Convenio núm. 108[119] del Consejo de Europa[120]. Este tratado sentaba las bases de una importante doctrina para salvaguardar el derecho fundamental a la vida privada en todas las dimensiones posibles, incluyendo la cibernética.

Posteriormente, en 1995, se adoptó la Directiva 95/46/CE[121], que extendía la concepción de la libre circulación de mercancías, personas, servicios y capital del mercado interior europeo, y tomaba igualmente en consideración la circulación y utilización de datos personales a través de límites transfronterizos.

La Carta de los Derechos Fundamentales[122], aprobada en el año 2000, reconocía nuevamente, en su artículo 8, el derecho de toda persona a la protección de sus datos personales, que deben ser tratados "de modo leal, para fines concretos y sobre la base del consentimiento" o bien para "otro fundamento legítimo previsto por la ley"[123]. Sobre esta base, todo individuo debe poder tener acceso a los datos que le conciernen, así como ejercer su derecho a rectificarlos. En este sentido, la Carta se aplica a los Estados miembro en el marco del Derecho de la Unión, velando por el cumplimiento de las directivas y reglamentos pertinentes, y siempre bajo la fundamentación de los Tratados europeos[124].

Toda esta labor acabó derivando, finalmente, en la firma del Reglamento General de Protección de Datos (RGPD)[125], en vigor desde mayo de 2016. Bien es cierto que no es de aplicación obligatoria hasta dos años más tarde[126], en una pretensión por conceder un plazo de

[116] Actualmente: Versión consolidada del Tratado de Funcionamiento de la Unión Europea (C 326/47), del 26 de octubre de 2012.
[117] Actual artículo 16 del TFUE.
[118] Versión consolidada del Tratado de Funcionamiento de la Unión Europea, del 26 de octubre de 2012, p. 55.
[119] *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, Estrasburgo, 28 de enero de 1981, Serie de Tratados Europeos núm. 108 del Consejo de Europa..
[120] Tomar en consideración que no debe confundirse con una institución de la Unión, sino que se trata de una organización intergubernamental para la protección de derechos humanos.
[121] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 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, *DOCE*, L 281/31, de 23 de noviembre de 1995
[122] Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), del 18 de diciembre del 2000.
[123] *Ibidem*, p. 10.
[124] Tratados comunitarios, TUE y TFUE.
[125] Reglamento (UE) núm. 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *DOUE*, L 119/46, de 4 de mayo de 2016.
[126] *Ibidem*, art. 99., p. 87.

adaptabilidad a todas las entidades e instituciones afectadas. Este reglamento sustituye a la Directiva 95/46/CE, con el objetivo reforzar su eficiencia y actualizarlo al contexto actual y al creciente abuso de utilización de datos que ponen en riesgo la integridad y seguridad de la población[127].

2.2.2. Contenido de la regulación

El RGPD aspira a proteger los derechos de los usuarios sobre sus datos personales, y, por lo tanto, regula su tratamiento – incluyendo la forma en la que son recopilados, procesados, almacenados y eliminados – y su circulación. Así, pretende dar a los usuarios un control sobre sus propios datos[128].

El contenido del texto se basa en la necesidad de proteger "datos personales", definidos[129] en el artículo 4 como "toda información sobre una persona física identificada o identificable"[130]. Más específicamente, establece que[131] "se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa[132] o indirectamente[133]", por ejemplo, a través de un nombre, dirección, correo e-mail, dirección IP, o material audiovisual como fotografías o vídeos.

Cabe señalar, en el mismo artículo, una subclasificación de tres tipos de datos personales especiales, cuyo tratamiento queda estrictamente prohibido a través del artículo 9 del reglamento[134]. En primer lugar, los "datos relativos a la salud"[135], tanto física como mental; dentro de estos se incluye toda información referida al sometimiento a atención sanitaria, que pueda desvelar el estado de salud del sujeto. En segundo lugar, los "datos genéticos", que pueden considerarse una especificación del anterior, dado que conciernen a "las características genéticas heredadas o adquiridas", que brinden "información única sobre la fisiología o salud" [136] del individuo en cuestión; esto puede incluir desde muestras de ADN hasta test de paternidad. Por último, los "datos biométricos" proporcionan información acerca de las "características físicas, fisiológicas o conductuales"[137] que posibilitan la identificación de la persona, lo que incluye, por ejemplo, imágenes o datos dactiloscópicos.

Un aspecto crucial de esta regulación es que afecta a todas las personas físicas y jurídicas[138] que operen con datos de la UE, independientemente de si se trata de una entidad

[127] Consejo Europeo & Consejo de la Unión Europea, *op. cit*.
[128] Reglamento (UE) 2016/679, *op. cit.,* párr. 7., p. 2.
[129] Esta definición solo aplica en algunos Estados, como los de la UE; pero en otros países, como EE. UU., solo se consideran datos personales aquellos que permitan la identificación de una persona de forma directa.
[130] Reglamento (UE) 2016/679, *op. cit.,* art. 4(1) p. 33.
[131] *Ídem*.
[132] Se entienden como directamente identificables todos aquellos datos que son exclusivos al individuo, tales como el número de identidad.
[133] Se entienden como indirectamente identificables todos aquellos datos que no son exclusivos al individuo, pero que pueden revelar información importante sobre su identidad, como por ejemplo el lugar de nacimiento.
[134] Si bien recogen excepciones tales como, entre otras, el consentimiento explícito para el fin señalado, el cumplimiento de obligaciones específicas, la seguridad, la protección de intereses vitales o intereses públicos esenciales, siempre y cuando sean proporcionales con el objetivo perseguido, o en pos de la salud pública o investigaciones científicas o históricas.
[135] Reglamento (UE) 2016/679, *op. cit.,* art. 4(15), p. 34.
[136] *Ibidem*, art. 4(13), p. 34.
[137] *Ibidem*, art. 4(14), p. 34.
[138] La protección se aplica sobre los datos de las personas físicas, pero el reglamento se aplica a las personas jurídicas que se ven afectadas en el marco de su operación con tales datos.

cuya sede se encuentre dentro de las fronteras de esta región o en un tercer Estado; basta con que parte de su actividad implique el trato de datos de ciudadanos europeos[139]. Además, se aplica de manera uniforme en todos los Estados miembro, con el objetivo de evitar disparidades en las legislaciones nacionales[140]. Así, por ejemplo, la empresa Twitter, de origen estadounidense, debe regirse por los principios del RGPD en lo que respecta a los datos europeos. Esto implica que, si bien la legislación de Estados Unidos solo considera "datos personales" aquellos que permiten la identificación de un individuo de manera *directa*, al operar con datos de ciudadanos europeos, deberá adherirse a la definición de la UE, que incluye la posibilidad de identificación *indirecta*, y comprometerse con la protección pertinente de esos datos.

Así pues, toda entidad o institución que opere con datos de la UE debe adherirse a los principios recogidos en el artículo 5 del reglamento que incluyen

a) el trato lícito, leal y transparente de los datos[141], que asegure su integridad y confidencialidad[142];
b) la limitación clara de los propósitos para la recogida y tratamiento de tales datos[143];
c) la "minimización de datos", es decir, la recopilación de los mínimos datos necesarios para el propósito establecido;
d) el respeto por la exactitud y, en la medida de lo posible, actualización de los datos almacenados, permitiendo al usuario rectificar y exigir la supresión (el conocido como "derecho al olvido"[144]) de los datos recopilados[145];
e) la conservación de los datos por parte del responsable durante el tiempo estrictamente necesario, y nunca más del requerido[146];
f) el deber del responsable de demostrar su compromiso con el cumplimiento de sus obligaciones, por ejemplo, a través del almacenamiento de registros[147] o la realización de evaluaciones de impacto[148].

El último principio, referido a la obligación del responsable de demostrar la licitud en la recopilación y el procesamiento de datos personales, se ve desarrollado en el artículo 6, y es novedoso con respecto a la Directiva anterior. Las condiciones expuestas en esta cláusula para demostrar el cumplimiento lícito[149] de las empresas incluyen, entre otras, la necesidad de que el usuario proporcione su consentimiento expreso de forma "libre, específica, informada e inequívoca"[150] para el procesamiento de sus datos. Para ello, además, el reglamento indica que es necesario que, en caso de que el consentimiento se conceda de manera escrita, la solicitud del consentimiento se presente de forma clara, sencilla e inteligible, de manera que no obstaculice ni confunda en ninguna manera al interesado. De la misma manera, el responsable debe facilitarle al interesado toda la información referente a sus derechos y, de forma

[139] Reglamento (UE) 2016/679, *op. cit.*, párr. 22., p. 4.
[140] *Ibidem*, párr. 10., p. 2.
[141] Desarrollado en el art. 6 del Reglamento.
[142] Desarrollado en el art. 32 del Reglamento.
[143] Desarrollado en el art. 18 del Reglamento.
[144] Reglamento (UE) 2016/679, *op. cit.*, art. 17, pp. 43-44.
[145] Desarrollado en los art. 16 y 17 del Reglamento.
[146] Reglamento (UE) 2016/679, *op. cit.*, art. 5(1)(e), p. 36.
[147] *Ibidem*, art. 30., pp. 50-51.
[148] *Ibidem*, art. 35., pp. 53-54.
[149] *Ibidem*, art. 7., p. 37.
[150] *Ibidem*, art. 4(11), p. 34.

igualmente concisa y de fácil lectura, brindarle aclaraciones acerca de la recopilación, almacenamiento, procesamiento y aseguramiento de sus datos[151].

Si bien todas las disposiciones anteriores son importantes, en la medida en la que permiten a los responsables ajustarse a una serie de principios y demostrar su cumplimiento, cabe considerar la opción de implantar una serie de medidas de seguridad que minimicen los riesgos en sí. Esta posibilidad se contempla en el artículo 6.4.e) y 32.1.a), que permiten al responsable o al encargado recurrir a técnicas tales como la seudonimización y el cifrado de datos personales cuando la evaluación de riesgos inherentes a su tratamiento pueda desafiar lo dispuesto en el Reglamento[152].

Por último[153], cabe señalar la creciente relevancia de la "elaboración de perfiles"[154], esto es, el tratamiento automatizado de datos personales, para, a través de un análisis de estos, tratar de predecir comportamientos y tendencias futuras, relativas a las preferencias del individuo, pero también a su ubicación, situación económica y profesional o salud. Este fenómeno pasaría a involucrar no solo aspectos relacionados con datos personales, sino también con el rendimiento del sistema de información operativo y el algoritmo.

Para cumplir con estas obligaciones, todos los Estados miembro deberán designar a una o varias "autoridades de control"[155] para que velen de forma independiente por la aplicación de la presente regulación, promuevan la sensibilización de los ciudadanos, asesoren a los organismos que operen con los datos contemplados y cooperen entre ellos para tratar de asegurar la coherencia en la ejecución del reglamento[156].

Estas autoridades deben responder a su vez ante un Comité Europeo de Protección de Datos, organismo que goza de personalidad jurídica. Este cuerpo está compuesto por el director de la autoridad de control de cada Estado y por el Supervisor Europeo de Protección de Datos[157]. Además, puede contar con la participación de la Comisión Europea[158]. Este Comité se encarga, entre otros aspectos, de supervisar y garantizar la correcta aplicación del Reglamento; de asesorar a la Comisión Europea en toda cuestión referente a la protección de datos personales en la UE, concretamente con vistas a una potencial modificación del Reglamento; de promover la cooperación entre los Estados miembro y sus respectivas autoridades competentes, así como, en algunos casos, con terceros países; de acreditar organismos de certificación; y de emitir dictámenes y recomendaciones y buenas prácticas[159].

Asimismo, todos los organismos y entidades que traten con datos de la UE nombrarán a un "responsable"[160] que se comprometa con las obligaciones del reglamento y se ponga a disposición del interesado, cuando este último necesite contactar con el organismo en cuestión para aplicar sus derechos.

---

[151] *Ibidem*, art. 12.
[152] *Ibidem*, párr. 83., p. 16.
[153] El RGPD es, por supuesto, mucho más extenso de lo desarrollado en los puntos anteriores. No obstante, no pretende hacerse un análisis exhaustivo de sus disposiciones, sino tan solo esclarecer los puntos más importantes para el desarrollo del presente escrito.
[154] Reglamento (UE) 2016/679, *op. cit.*, art. 4(4), p. 33.
[155] *Ibidem*, art. 51, p. 65.
[156] *Ibidem*, arts. 51 y 57.
[157] Reglamento (UE) 2016/679, *op. cit.*, art. 68, p. 76.
[158] Si bien no tiene derecho a voto en la toma de decisiones.
[159] Reglamento (UE) 2016/679, *op. cit.*, art. 70, pp. 66-67.
[160] *Ibidem*, art. 4(7), p. 33.

A su vez, el "responsable" puede delegar su actividad en un "encargado"[161], si lo estimara necesario u oportuno. La autoridad de control deberá, por lo tanto, comunicarse con estas figuras particulares, supervisar su actividad e incluso cooperar con ellas en operaciones conjuntas[162]. Para asegurar el cumplimiento de sus obligaciones, el responsable y/o el encargado deberá llevar un registro de las actividades de tratamiento de datos ejercidas bajo su responsabilidad[163].

En el caso español, por ejemplo, la adopción de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)[164] adapta la normativa española a la legislación europea, y designa a la Agencia Española de Protección de Datos (en adelante, AEPD) como autoridad de control, encargada de velar por el cumplimiento y aplicación del reglamento[165]. Este cuerpo se encarga, entre otros aspectos, de la promoción de la sensibilización del público en cuanto a los riesgos y normas existentes; de la sensibilización, asimismo, de los responsables y su asesoramiento; de la cooperación con autoridades de control de otros Estados[166]; del impulso de mecanismos de certificación de protección de datos; del seguimiento periódico de dichas certificaciones expedidas; del registro de infracciones del reglamento; o del ejercicio de sus poderes de investigación, de autorización, consultivos y correctivos[167].

Adicionalmente, el título V de esta Ley 3/2018 se ocupa de la figura del "encargado del tratamiento de datos", que, en este caso, se denomina "responsable" cuando actúa en su propio nombre y establezca relación con los afectados; o bien cuando en su función de encargado utilice los datos en pos de un objetivo propio[168].

Con el objetivo de tratar de desincentivar el incumplimiento de sus disposiciones, el presente reglamento comunitario establece un régimen sancionador, cuyas multas administrativas pueden ascender hasta los 20 millones de euros, o, si el infractor es una empresa, hasta el 4% de su facturación total anual. No obstante, la imposición de la cantidad exacta recaerá en la autoridad nacional competente, que debe evaluar cada caso de forma individual[169].

De esta manera, el RGPD sienta las bases para el marco normativo de protección de datos. No obstante, el desarrollo tecnológico y el surgimiento de nuevos actores y dimensiones exigen el desarrollo de directivas y reglamentos adicionales que complementen al primero.

2.3. Protección de datos en comunicaciones electrónicas

El desarrollo de Internet impulsó el crecimiento de los mercados, revolucionando las infraestructuras tradicionales de prestación de servicios, así como la disposición de la información. Con la creación de redes móviles digitales accesibles para un público amplio, se

[161] *Ibidem*, art. 4(8), p. 33.
[162] *Ibidem*, art. 62, p. 72-73.
[163] *Ibidem*, art. 30, pp. 50-51.
[164] Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, *BOE*, núm. 294, de 06 de diciembre de 2018.
[165] *Ibidem*, art. 47, p. 32.
[166] *Ibidem*, art 58., pp. 37-38.
[167] Es decir, aquellos señalados en los arts. 57 y 58 del RGPD.
[168] Ley Orgánica 3/2018, *op. cit*., art. 33., p. 26.
[169] Reglamento (UE) 2016/679, *op. cit.*, art. 83(2), p. 82.

multiplicaron las posibilidades de los usuarios, si bien también supuso un incremento de los riesgos para sus datos personales e intimidad[170].

Por este motivo, paralelamente a la regulación en materia de protección de datos, comienza a manifestarse la necesidad de contar con una cierta reglamentación complementaria en sectores específicos. En este contexto, se elabora la Directiva 2002/58/CE[171], del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas el de servicios de comunicaciones electrónicas.

2.3.1. Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas)

Esta directiva pretende garantizar una serie de derechos fundamentales en el marco de las comunicaciones electrónicas; concretamente, el derecho a la intimidad de las personas físicas y la seguridad de sus datos personales[172]; aspira, asimismo, a salvaguardar los intereses legítimos de personas jurídicas[173]. En este contexto, se aplica a todos los proveedores de servicios de comunicaciones electrónicas, independientemente de si están establecidos o no en la UE, siempre y cuando oferten sus servicios a otros proveedores o usuarios finales en el territorio de la Unión.

La Directiva 2002/58, también llamada Directiva ePrivacy, presenta numerosos paralelismos con el RGPD[174], si bien se concibe como meramente complementaria, con el objetivo de precisar aspectos adicionales que entremezclan diferentes tecnologías[175]. De esta manera, una de sus bases principales es la armonización regulatoria entre los Estados miembro para evitar obstáculos en el mercado interior europeo, garantizando la libre circulación de datos y servicios de comunicaciones electrónicas[176]. Así pues, trata de promover el desarrollo transfronterizo de las comunicaciones, para lo cual precisa contar con la confianza de los usuarios en la protección de su intimidad.

Debe, asimismo, adherirse a los mismos principios que están recogidos en el artículo 5 del RGPD, siendo de nuevo especialmente destacados los conceptos de consentimiento y confidencialidad. Ambos se ven profundamente interconectados, en la medida que el consentimiento pretende poner en conocimiento del usuario las posibilidades de confidencialidad disponibles[177].

---

[170] ALONSO LECUIT Javier. "Privacidad, confidencialidad e interceptación de las comunicaciones". *Real Instituto Elcano*. ARI 92/2018, 24 de julio de 2018, pp. 2-3.

[171] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, *DOCE*, L 201/37, de 31 de julio de 2002

[172] Bajo la disposición del art. 52.3 de la Carta de Derechos Fundamentales de la UE, relativo al alcance de los derechos garantizados, son de aplicación los arts. 7 y 8 de la misma Carta y el art. 8 del Convenio Europeo de Derechos Humanos

[173] La intención de proteger los intereses de las personas jurídicas se manifiesta a lo largo de la directiva se fundamenta vagamente, como "garantizado en el marco de la legislación comunitaria" (párr. 12). En la propuesta de reglamentación posterior, este principio presenta una mayor base argumentativa, referenciando jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos.

[174] La comparación debería establecerse más bien con respecto a su contemporánea, la Directiva 95/46/CE, predecesora del actual RGPD.

[175] Directiva 2002/58/CE, *op. cit.,* párr. 46, p. 42.

[176] *Ibidem*, art. 1(1), p. 42.

[177] Directiva 2002/58/CE, *op. cit.,* párr. 34, p. 41.

Los datos que son tratados en las redes de comunicaciones electrónica incluyen en este caso, una concretización de los expuestos en el RGPD, introduciendo una diferenciación entre y "datos de localización"[178] y "datos de tráfico"[179]. Los primeros permiten conocer la ubicación física de un dispositivo conectado[180], mientras que los segundos involucran los relativos al propio funcionamiento de la red[181].

Sin embargo, la distinción entre ambos no siempre es clara, puesto los datos de localización pueden ser a su vez datos de tráfico. Así, por ejemplo, la dirección IP se considera un dato de localización, en la medida en la que determina la ubicación de un equipo; pero también un dato de tráfico, en tanto que factor en el análisis del patrón de utilización de Internet por parte del usuario.

Además de esto, al realizar una comunicación, entendida en la presente directiva como "cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas"[182], se proporcionan, por ejemplo, el nombre o a la dirección del remitente y/o del destinatario; los datos de tráfico pueden incluir una conversión de esta información[183].

No obstante, si los datos de tráfico permiten establecer una relación con un usuario identificable, estarán sujetos a las disposiciones del artículo 5, referido a la confidencialidad de comunicaciones[184]. Mediante este artículo se prohíbe "la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados"[185], salvo autorización legal, y con la excepción del almacenamiento técnico.

Es necesario, pues, distinguir los datos de tráfico que están incluidos en el concepto de "comunicación" de aquellos que no lo están. Así, se excluyen los datos tratados por proveedores de una red pública[186] o de un servicio de comunicaciones electrónicas abierto al público, cuando se transmiten como parte de un servicio de radiodifusión[187]. Con respecto a este último caso cabe destacar que el tratamiento de los datos suele estar vinculado a un propósito de promoción comercial o de prestación de servicios de valor añadido[188], si bien debe estar sujeto al consentimiento del usuario, y siempre bajo la premisa de concederle la debida información[189].

[178] *Ibidem*, art. 2(c), p. 43.
[179] *Ibidem*, art. 2(b), p. 43.
[180] Según el párr. 14 de la Directiva (p. 38), indica, entre otras, "la latitud, la longitud y la altitud del equipo (…) o la hora en la que la información de localización ha sido registrada".
[181] Según el párr. 15 de la Directiva (p. 38), referida "al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo (…), a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión (…), al formato en que la red conduce la comunicación."
[182] Directiva 2002/58/CE, *op. cit.,* art. 2(3), p. 43.
[183] De nuevo, en el caso de una dirección IP.
[184] Debe estar protegida conforme al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.
[185] Directiva 2002/58/CE, *op. cit.,* art. 5(1), p. 43.
[186] *Ibidem*, párr. 16, p. 38.
[187] Y, por lo tanto, no se da entre un número finito de usuarios identificables.
[188] Entendidos en el art. 2 de la Directiva (p. 43) como aquellos que operan con datos que van "más allá de lo necesario para la transmisión de una comunicación o su facturación".
[189] Directiva 2002/58/CE, *op. cit.,* párr. 26, p. 40.

Un ejemplo claro de esto es el uso de las *cookies*[190] o "chivatos". Esta directiva los considera un tipo legítimo de *spyware*[191] o "programa espía", en la medida en la que se utiliza con el conocimiento de los usuarios, y concediéndoles la posibilidad de denegar el almacenamiento de dichas *cookies* en su equipo. Esto puede ofrecer una serie de ventajas, facilitando la navegación del usuario y ofreciéndole un trato más personalizado, por ejemplo, recordando su nombre de usuario y contraseña, o el idioma de preferencia[192]. No obstante, el almacenamiento de tales datos puede suponer también un importante riesgo a la privacidad.

Si bien el caso de las *cookies* es especialmente polémico, son varias las problemáticas que se identificaron en la presente directiva. Así, tras una evaluación de la Comisión, se estimó que la Directiva no era suficientemente eficaz ni adecuada al contexto actual, especialmente dada la constante evolución tanto en el plano tecnológico como en el económico[193] y la inexistencia de un mecanismo de control autorizado para supervisar del cumplimiento de las disposiciones expuestas.

Por este motivo, con el objetivo de precisar las cláusulas de la normativa existente, aumentar la seguridad en las comunicaciones digitales y asegurar la coherencia con el RGPD, se introdujeron sugerencias innovadoras a la Directiva 2002/58/CE, que acabaron derivando en una nueva propuesta de reglamentación, denominada Reglamento sobre la privacidad y las comunicaciones electrónicas[194].

2.3.2. Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas

La presente propuesta pretende precisar el contenido del RGPD en el sector de las comunicaciones electrónicas, por lo que se presenta como una *lex specialis*, que complementa las obligaciones recogidas en el RGPD, manteniendo para ello el mismo alcance territorial aplicable[195]. Así, mientras el RGPD se ocupaba de la protección de los datos personales de manera general, la nueva propuesta trata de garantizar específicamente la confidencialidad en las comunicaciones, independientemente de si involucra datos personales o de carácter no personal, o incluso datos relacionados con personas jurídicas[196]. Adicionalmente, se refuerza el compromiso con la armonización regulatoria, con el objetivo de evitar interpretaciones dispares entre los Estados miembro[197].

---

[190] Pequeños archivos de datos guardados por un sitio web cuando se visita. Almacenan información para recordar las preferencias del usuario (por ejemplo, el idioma) y hacer un seguimiento de su actividad.

[191] Definidos en el párr. 24 de la Directiva (p. 39) como "identificadores ocultos (…) que pueden introducirse en el terminal del usuario (…) para acceder a información, archivar información oculta o rastrear las actividades del usuario".

[192] Directiva 2002/58/CE, *op. cit.,* párr. 25, p. 40.

[193] Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. Final Report: A study prepared for the European Commission DG Communications Networks, Content & Technology by Deloitte, 2017, p. 162.

[194] Propuesta de Reglamento 2017/0003 (COD) del Parlamento Europeo y del Consejo, de 10 de enero de 2017, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE.

[195] *Ibidem*, art. 3, p. 28.

[196] Se argumenta en este sentido (p. 4) que según el alcance del artículo 7 de la Carta de Derechos Fundamentales, de la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos, "las actividades profesionales de personas jurídicas no pueden quedar excluidas de la protección de derechos garantizada por el artículo 7 de la Carta y el artículo 8 del CEDH".

[197] Propuesta de Reglamento 2017/0003, *op. cit.*, párr. 7, p. 15.

Una de las mayores preocupaciones en lo referente al uso de Internet y las comunicaciones telemáticas es la emergencia de nuevos servicios que dejan atrás la regulación vigente, incapaz de seguir el ritmo de la evolución tecnológica. Así, por ejemplo, se manifiesta una falta de regulación de los servicios de transmisión libre (en inglés, *Over-the-Top*[198] o, por sus siglas, "OTT") en el marco legislativo de la Unión[199]. Si bien es cierto que varios proveedores de estos servicios OTT se ajustan total o parcialmente a los requisitos de confidencialidad, depender de su autorregulación puede suponer un peligro para la protección de los derechos fundamentales del ciudadano europeo.

Por lo tanto, si bien los objetivos y principios dictaminados en la Directiva 2002 se mantenían apropiados, tras realizar una evaluación (denominada REFIT, por sus siglas en inglés[200]), la Comisión determinó que esta no había alcanzado los propósitos establecidos[201]. Este fracaso se atribuyó, mayoritariamente, a la falta de precisión y a la formulación de disposiciones ambiguas[202], y, por lo tanto, abiertas a interpretaciones divergentes, con lo que obstaculizaban la actividad transfronteriza de las empresas. No obstante, también cabe considerar la evolución en las innovaciones tecnológicas y económicas, que han transformado Internet en un escenario vital de comercio[203].

En este sentido, se hace hincapié en la cuestión de las *cookies*. A este respecto, se resalta el hecho de que, a pesar de que exista una definición del concepto de "consentimiento", esta no tiene valor alguno si los usuarios no comprenden la noción de *cookies* ni sus implicaciones. Esto se da hasta el punto de que, en la mayoría de las ocasiones, permiten su instalación de manera inconsciente[204].

Tomando en consideración todo lo anterior, la nueva propuesta contempla nuevas perspectivas para el tratamiento de datos, y comienza señalando la necesidad de una centralización de la normativa referente a los proveedores OTT. De esta manera, el reglamento ampliará el alcance personal de la directiva para incluir a nuevos proveedores de servicios – lo que puede incluir servicios de mensajería instantánea o comunicaciones interpersonales – que tendrán que adaptarse a las nuevas condiciones y al principio del consentimiento, asumiendo los costes adicionales pertinentes[205].

Siguiendo esta línea, se simplifica el control de la privacidad en programas, aplicaciones y navegadores, proporcionando información más clara sobre la configuración disponible. Al respecto del uso de *cookies*, cabe destacar la introducción de ajustes predeterminados en el navegador o en una aplicación[206] para rechazar *cookies* de terceros[207], posibilitando la reducción de mensajes y anuncios. Esta configuración debe ofrecerse de manera transparente y sencilla de comprender. Así, una de las condiciones es que se realicen formulaciones claras como, por

[198] Servidores que distribuyen contenido audiovisual o de otro tipo directamente al usuario, sin depender de una operadora tradicional de televisión por cable o satélite. Por ejemplo, Netflix, WhatsApp, Skype.
[199] ALONSO LECUIT J., *op. cit*., pp. 2-4.
[200] Regulatory Fitness and Performance Programme.
[201] ALONSO LECUIT J., *op. cit*., pp. 2-4.
[202] Por ejemplo, párr. 25 de la Directiva 2002/58/CE: "la presentación de la información y del pedido del consentimiento o posibilidad de negativa debe ser tan asequible para el usuario *como sea posible*".
[203] Evaluation and review of Directive 2002/58, *op. cit*., pp. 42-43.
[204] KUBICECK, K. (2024). *Automated analysis and enforcement of consent compliance* [Tesis de doctorado, Universidad Masaryk], p. 16.
[205] Propuesta de Reglamento 2017/0003, *op. cit.*, párr. 17, pp. 17-18.
[206] Evaluation and review of Directive 2002/58, *op. cit*., p 61.
[207] Archivos de texto creados por sitios web que el usuario no está visitando. Por ejemplo, si ese sitio web tiene un anuncio en la página web que el usuario está visitando, puede introducir una *cookie*.

ejemplo, "aceptar *cookies* siempre", "no aceptar nunca *cookies*", "rechazar *cookies* de terceros" o "solo aceptar *cookies* de origen"[208].

Asimismo, se exige que se proporcione la debida información, con el objetivo de que el usuario pueda tomar su decisión de manera libre. Queda prohibida toda información – o en su defecto, toda omisión de información – que pretenda disuadir usuario de elegir una configuración con mayor privacidad[209]. Así, el primer ejemplo claro sería la omisión de información al usuario acerca de su posibilidad del usuario de elegir la configuración de privacidad. Otros ejemplos podrían ser la ocultación de información relevante respecto a los plazos de conservación del historial de navegación, o la utilización de datos personales para el envío de publicidad personalizada.

Otro de los grandes focos de la nueva propuesta de reglamentación es la conceptualización de "mercadotecnia directa", definida como "cualquier forma de publicidad mediante la cual una persona física o jurídica envía comunicaciones comerciales directas a uno o varios usuarios finales identificados o identificables empleando servicios de comunicaciones electrónicas"[210]. Así, la intensificación de la publicidad puede constituir una intromisión en la privacidad del usuario cuando se le transmita de forma no solicitada[211]. Mediante la presente propuesta, se señala el derecho de los usuarios a bloquear estas comunicaciones[212], haciendo uso de unos datos de contactos de fácil disponibilidad o una configuración de manejo claro y sencillo[213].

La función de supervisar la aplicación de este reglamento pretende delegarse a las mismas autoridades designadas en el RGPD; y de igual manera, se contemplan los sistemas de sanciones establecidos en dicho reglamento[214].

Así, la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas constituye un pilar fundamental para asegurar la privacidad y confidencialidad de las comunicaciones electrónicas, y, al mismo tiempo, la coherencia del RGPD, que se revela como incompleto ante la falta de regulaciones adicionales que cubran los desafíos que suponen las constantes innovaciones tecnológicas.

2.4. Reglamento de Inteligencia Artificial

El crecimiento constante de los revolucionarios de Inteligencia Artificial (en lo sucesivo, "IA") sienta las bases para una un impulso económico y social sin precedentes. A pesar de su impacto revolucionario y su gran atractivo, para optimizar sus beneficios y reducir sus riesgos es necesario establecer un marco de cooperación que fomente la confianza en su desarrollo y proteja la privacidad y seguridad de los ciudadanos.

Las potenciales amenazas derivadas de su desarrollo han demostrado la insuficiencia del RGPD para velar por los intereses de los ciudadanos de la UE en la protección de sus datos personales. Por este motivo, en abril de 2021, la Comisión presentó una propuesta de reglamentación de IA. Tras meses de negociación, el Consejo y el Parlamento Europeo

[208] Propuesta de Reglamento 2017/0003, *op. cit.*, párr. 23, p. 20.
[209] *Ibidem*, párr. 24., pp. 20-21.
[210] *Ibidem*, párr. 32, p. 23.
[211] *Ibidem*, párr. 33, p. 23.
[212] Recogido en el art. 16 de la propuesta, con excepciones expuestas en el art. 17.
[213] Propuesta de Reglamento 2017/0003, *op. cit.*, párr. 34., pp. 23-24.
[214] *Ibidem*, Capítulos IV y V.

alcanzaron un acuerdo provisional[215] el 9 de diciembre de 2023[216], por el que se establece el Reglamento de IA[217]. Ello constituye un hito para la Unión, en tanto en cuanto se ha convertido en la primera región en legislar esta tecnología, y, por lo tanto, puede sentar las bases de un modelo a imitar por otros Estados[218].

2.4.1. ¿Qué es la IA?

La Inteligencia Artificial es un fenómeno relativamente nuevo y en permanente desarrollo. Se trata de un concepto muy extenso, aplicable a un enorme rango de tecnologías, por lo que resulta complejo de delimitar. De manera algo simplificada, el Grupo de expertos de alto nivel sobre inteligencia artificial define la IA como "sistemas que demuestran un comportamiento inteligente analizando el entorno y actuando – con cierto grado de autonomía – para alcanzar unos objetivos específicos"[219]. De la misma manera, el Grupo internacional de trabajo sobre protección de datos y telecomunicaciones[220] la define como la "teoría y desarrollo de sistemas informáticos capaces de llevar a cabo tareas que normalmente requieren inteligencia humana"[221]. Ambos Grupos incluyen el concepto "inteligencia" en su definición, término que, tanto aplicado a humanos como a máquinas, es, en cierta medida, abstracto. Por este motivo suele hablarse más bien de "racionalidad", haciendo referencia a la capacidad de escoger la opción óptima para alcanzar un objetivo concreto[222].

La manera de lograr esto no es otra que recopilando datos, tanto estructurados como no estructurados, y a partir del análisis de ese *input* inferir el *output* deseado. Así, el Grupo de expertos de alto nivel sobre IA, propone un ejemplo sencillo; una máquina que limpie el suelo cuando esté sucio. Este aparato recibirá un *input*, pongamos, una fotografía, y, a través de este, la IA deberá analizar si detecta suciedad y si, por lo tanto, debe generar un *output*, que en este caso sería activar su opción de limpieza[223]. La cuestión es que, para que esta máquina esté

[215] Si bien, por el momento, sigue pendiente la adopción del texto oficial.
[216] Consejo Europeo & Consejo de la Unión Europea, *op. cit.*
[217] Propuesta de Reglamento 2021/0106 (COD) del Parlamento Europeo y del Consejo, de 21 abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión.
[218] ARNAL, Judith & JORGE RICAT, Raquel. "Inteligencia artificial: el 'efecto Bruselas', en juego", *Real Instituto Elcano*, 3 de octubre del 2023.
[219] High-Level Expert Group on Artificial Intelligence, "A definition of AI: Main capabilities and scientific disciplines", *Directorate-General for Communication, European Commission*, 18 de diciembre de 2023, p. 1. Traducción propia. Texo original: "[AI refers to] systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."
[220] Compuesto por representantes de las autoridades de protección de datos y otros organismos de administraciones públicas nacionales, organizaciones internacionales y científicos de todo el mundo.
[221] International Working Group on Data Protection in Telecommunications: 675.57.14, "Working Paper on Privacy and Artificial Intelligence", 64ª reunión, Nueva Zelanda, 29-30 de noviembre de 2018, p. 2. Traducción propia. Texto original: "the theory and development of computer systems able to perform tasks normally requiring human intelligence".
[222] High-Level Expert Group on Artificial Intelligence, *op. cit.,* pp. 1-2.
[223] *Ibidem*, p. 3.

preparada para identificar la suciedad, debe ser "enseñada" mediante técnicas como pueden ser el *machine learning*[224], el *deep learning*[225], o árboles de decisión[226].

El perfeccionamiento de las tecnologías de IA lleva al despliegue de esta en una pluralidad de ámbitos, lo que la ha llevado a convertirse en un fenómeno totalmente implantado en nuestra sociedad. La herramienta de IA que más ha dado que hablar en los últimos meses es, posiblemente, el ChatGPT; se trata de un modelo de procesador de lenguaje y, como tal, puede reconocer el habla, transcribirla, traducirla, entender órdenes, y optimizar o corregir la escritura, entre otras opciones. No obstante, existen otras herramientas, como las encargadas de filtrar contenido – por ejemplo, identificando contenido spam o moderando contenido en una plataforma –, identificar contenido audiovisual – por ejemplo, reconociendo objetos y personas o movimientos[227] –, clasificar riesgos – por ejemplo, elaborando informes de riesgo crediticio o prediciendo un potencial fraude en transacciones[228] –, o recomendar algoritmos – a través del análisis de patrones y tendencias de comportamientos, normalmente con el fin de recomendar productos con un objetivo comercial[229].

Las dos últimas herramientas – referidas a clasificación de riesgos y recomendación de algoritmos – son un claro ejemplo de "elaboración de perfiles"[230], que pretenden realizar predicciones y tomar decisiones a partir del análisis de los datos del interesado, y, por lo tanto, están especialmente vinculadas con la normativa del RGPD. En este sentido, es importante proteger al individuo, ya que, si bien el procesamiento de sus datos para dar como resultado un *output* crecientemente personalizado, también conlleva un riesgo potencial cada vez mayor. Además, debe tenerse en cuenta que la recopilación y procesamiento de datos que lleva a cabo la AI implica, básicamente, que se nutre con todo el Big Data que puede acumular, lo cual contrasta en gran medida con el principio de minimización establecido en el RGPD[231].

Así pues, el desarrollo de la Inteligencia Artificial presenta grandes conflictos para la protección de derechos fundamentales, especialmente, aquellos relacionados con la privacidad y la protección de datos. Es por este motivo que la propuesta de Ley IA actual está concebida con la pretensión de que se ajuste y respete, en primer lugar, la regulación vigente en materia de protección del individuo en estos ámbitos[232].

---

[224] O "aprendizaje computacional". Campo de la IA en el que el dispositivo no tiene que ser programado explícitamente, sino que aprenden a partir del *input* de datos que reciben y mejoran su rendimiento.

[225] O "aprendizaje profundo". Subcampo especializado de *machine learning*, basado en la creación de redes neuronales artificiales que pretenden imitar el cerebro humano, para aprender a partir del *input* de datos. Es capaz de operar con algoritmos más complejos que el anterior.

[226] Modelo de aprendizaje automático utilizado para tomar decisiones o realizar predicciones. Se representa como un diagrama con forma de árbol, que incluye las posibles decisiones y las ramificaciones de las potenciales consecuencias de esa decisión.

[227] Por ejemplo, un coche autónomo.

[228] Por ejemplo, a través del análisis de patrones, identificando comportamientos inusuales o redes de cuentas bancarias utilizadas para blanquear dinero.

[229] Fieldfisher [Fieldfisher Data & Privacy Team] (1 de febrero de 2024). *Debunking the EU AI Act: an overview of the new legal framework* [Video]. YouTube.

[230] International Working Group on Data Protection in Telecommunications, *op. cit*., pp. 6-7.

[231] GIL. E., *op. cit,* p. 52.

[232] MADIEGA, T. *Artificial intelligence act* [Legislative Briefing]. European Parliamentary Research Service, marzo, 2024. p. 10.

2.4.2. Propuesta de Reglamento de Inteligencia Artificial

Uno de los propósitos principales perseguidos con la elaboración de este proyecto es convertir a la UE en la primera región del mundo en adoptar una legislación que regule el uso de la IA, y que, a su vez, incentive a otros países a desarrollar un reglamento similar[233], generando así el denominado "efecto Bruselas"[234].

Al igual que en el RGPD, las disposiciones de la presente propuesta van dirigidas a todos los actores involucrados en la cadena de valor del producto de IA, así como a los organismos públicos y privados que operen con datos de la UE, independientemente de si están establecidos en un Estado miembro o no. Asimismo, se aplica, por supuesto, a las personas que se vean potencialmente afectadas por estos sistemas[235].

El artículo 3 de la Ley IA define el sistema de IA como un "software […] que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa". Esta definición, muy similar a las anteriormente expuestas, está desarrollada de manera muy generalizada[236], con el objetivo de alinearse lo más posible con la elaborada por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), que la describe como un "sistema basado en máquinas que, por objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales"[237]. Así, trata de alcanzar la una cierta convergencia internacional a este respecto[238].

El reglamento, sin perjuicio de los cambios que puedan introducirse en las negociaciones vigentes, se fundamenta en la jerarquización de los sistemas de IA de acuerdo con los riesgos que implican; así, se realiza una distinción entre riesgo (1) inaceptable, (2) alto, (3) limitado y (4) bajo o mínimo[239]. En base a los mismos, se aplican obligaciones y sanciones[240] diferenciadas, si bien, al igual que en el caso del RGPD, la determinación de la cantidad concreta recaerá en una autoridad nacional.

En primer lugar, los sistemas de IA de riesgo (1) inaceptable[241] son aquellos que desafían los principios de la UE, como puede ser la violación de un derecho fundamental – por ejemplo, el mencionado derecho a la vida privada – o que sean susceptibles de provocar perjuicios a la salud del individuo. Así, en este rango, se engloban las prácticas referidas a la explotación de

---

[233] ARNAL, J. & JORGE RICAT, R., *op. cit.*

[234] Acuñado por analogía al concepto "Efecto California", fenómeno a través del cual el marco normativo de la UE se convierte en un modelo que afecta al ordenamiento jurídico de terceros Estados, convirtiéndose, de manera indirecta, una potencia reguladora mundial.

[235] Propuesta de Reglamento 2021/0106, *op. cit*., art. 2., p. 44

[236] Para tratar de alcanzar la una cierta convergencia internacional a este respecto.

[237] OECD/LEGAL/0449, "Recommendation of the Council on Artificial Intelligence", del 22 de mayo de 2019, p. 7. Traducción propia. Texto original: "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

[238] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Plan coordinado sobre la inteligencia artificial*. Bruselas, 07.12.2018. COM (2018) 795, p. 23.

[239] Propuesta de Reglamento 2021/0106, *op. cit*., p. 14.

[240] El art. 71(1) de la Propuesta determina que el régimen de sanciones será determinado por los Estados miembro, *contra el principio de uniformidad*.

[241] Propuesta de Reglamento 2021/0106, *op. cit*., Título II, pp. 49-51.

vulnerabilidades[242] o a las técnicas especialmente manipulativas que puedan provocar daños físicos o psicológicos, tanto al usuario afectado como a otras personas. Asimismo, prohíbe la realización de calificaciones social en base al *output* generado por la IA, que pueda resultar en un trato discriminatorio o desfavorable; y, salvo excepciones[243], prohíbe el "uso de sistemas de identificación biométrica en tiempo real en espacios de acceso público con fines de aplicación de la ley". Las multas administrativas aplicadas por el incumplimiento de esta disposición ascienden hasta los 30 millones de euros, o el 6% de facturación anual si el infractor es una empresa[244].

En segundo lugar, los sistemas de riesgo (2) alto[245] se definen como aquellos que pueden suponer un daño a la salud o seguridad de los derechos fundamentales de las personas e incluyen, por lo tanto, todos los sistemas de identificación biométrica[246]. Si bien son de uso aceptado en el mercado europeo, están sujetos a unos requisitos obligatorios[247], referidos al establecimiento de un sistema de gestión de riesgos actualizado periódicamente[248]; a la implementación de unas prácticas adecuadas en la gobernanza de datos adecuada[249]; al registro y manejo de una documentación técnica detallada[250]; al archivamiento de registros de actividad transparentes[251]; al sometimiento a supervisión humana[252]; y la comunicación de información a los interesados[253], además de otras especificidades técnicas[254]. Asimismo, deben someterse a unos procedimientos de evaluación de conformidad *ex ante*, y a sistemas de mitigación de riesgos, que se comprometa a proporcionar un alto nivel de precisión y solidez[255]. Las multas aplicadas en este caso ascienden hasta los 20 millones de euros, o el 4% de facturación anual en caso de una empresa[256].

En tercer lugar, los sistemas de riesgo (3) limitado[257] son aquellos que interactúan con individuos. Son capaces de identificar emociones o establecer una asociación a una categoría social a partir de datos biométricos, así como de generar *deepfakes*[258] a través de la producción o manipulación de contenido. Este grupo se ve sujeto a una serie de requisitos de transparencia que, entre otros, obliga a los sistemas a informar al usuario de manera clara e inequívoca de que no está comunicándose con un ser humano, sino con una máquina. Un claro ejemplo de un sistema de riesgo limitado sería una IA generativa, como un *chatbot*. Si bien las obligaciones impuestas a estos sistemas son diferentes a las establecidas para los sistemas de riesgo alto, las multas aplicables son las mismas.

---

[242] *Ibidem*, art. 5(1)(b), p. 49. Se destacan en este caso los grupos vulnerables concretos, debido a su edad, salud o situación social o económica.
[243] Por ejemplo, búsqueda de víctimas, prevención de ataques terroristas u otras amenazas específicas.
[244] Propuesta de Reglamento 2021/0106, *op. cit*., art. 71(3), p. 92.
[245] *Ibidem*, Título III, pp. 51-66. Grupo que engloba la mayoría de las provisiones de la regulación.
[246] Entre otros sistemas. Clasificados en el Anexo III del reglamento.
[247] Propuesta de Reglamento 2021/0106, *op. cit*., Título III, Capítulo 2, pp. 53-59.
[248] *Ibidem*, art. 9, p. 53.
[249] *Ibidem*, art. 10, pp. 54-55.
[250] *Ibidem*, art. 11, pp. 55-56.
[251] *Ibidem*, arts. 12 y 13, pp. 56-57
[252] *Ibidem*, art. 14, pp. 57-58.
[253] *Ibidem*, art. 13, pp. 56-57.
[254] *Ibidem*, art. 15, pp. 58-59.
[255] *Ibidem*, p. 13.
[256] *Ibidem*, art. 71(4), p. 92.
[257] *Ibidem*, Título IV, pp. 77-78.
[258] O "ultrafalsificaciones".

Por último, los sistemas de riesgo (4) bajo o mínimo[259] no se ven sometidos a ninguna obligación especial ni a ninguna multa administrativa[260], dado que, generalmente, no son susceptibles de suponer una amenaza a la seguridad, salud, libertad o derechos fundamentales de los usuarios. Ejemplos de este último grupo serían filtraciones de spam o videojuegos.

Adicionalmente, si bien es importante partir de la base de esta clasificación, también lo es tener en cuenta la evolución constante de los sistemas de IA. De acuerdo con este patrón, resulta esencial hacer referencia a los sistemas de IA de propósito general (GPAI por sus siglas en inglés[261]), que son aquellos que se entrenan de manera que terminan por cumplir un propósito para el que originalmente no estaban concebidos. Por lo tanto, aunque no fuera el caso inicial, podrían acabar por convertirse en sistemas de alto riesgo, y teniendo que adherirse a los requisitos obligados de este reglamento[262].

El reglamento dispone de una multa administrativa adicional, aplicable a todos los sistemas, independientemente de su clasificación en la escala de riesgos. Se trata de una sanción de hasta 10 millones de euros, o bien el 2% de la facturación anual de la empresa, en el supuesto de que se presente "información inexacta, incompleta o engañosa"[263], como respuesta a la solicitud de organismos notificados o autoridades nacionales competentes.

Con el objetivo de supervisar la aplicación de las disposiciones expuestas, el reglamento propone, nuevamente, el nombramiento por parte de los Estados miembro de autoridades nacionales, si bien, en esta ocasión, no se explicita que deban ser las mismas designadas por el RGPD, a pesar de que sus funciones y poderes presenten grandes paralelismos; una de estas similitudes es la recogida en el artículo 68, que dispone que conformarán, junto con el Supervisor Europeo de Protección de Datos, el denominado "Comité Europeo de Inteligencia Artificial", cuerpo presidido por la Comisión Europea. Este Comité se encargará de armonizar las prácticas de los Estados miembros a través de la puesta en común de conocimientos técnicos. Asimismo, deberá emitir dictámenes o recomendaciones pertinentes, referentes tanto a aspectos puramente técnicos, como a cuestiones administrativas – lo que puede incluir desde especificaciones para la armonización de normas, hasta documentos orientativos en el marco del régimen sancionador[264].

2.4.3. Aplicabilidad y entrada en vigor

Si bien se dispone la entrada en vigor de la Ley IA 20 días después de su publicación en el Diario Oficial, al igual que en el caso del RGPD, su aplicación pretende llevarse a cabo de manera progresiva, con el fin de dar a las personas físicas y jurídicas afectadas un margen de adaptación[265]. Así pues, uno de los aspectos que se contempla actualmente, es el establecimiento de plazos de implementación, que pueden dividirse en cuatro etapas.

La primera etapa concierne a los Títulos I y II, referidos, respectivamente a (I) el ámbito de aplicación y las definiciones y (II) las prácticas de IA prohibidas. La aplicación de estos se hará

[259] Propuesta de Reglamento 2021/0106, *op. cit*., Título IV, pp. 77-78.
[260] Comisión Europea. "Ley de IA". *Configurar el futuro digital de Europa*, 2024.
[261] General Purpose Artificial Intelligence (Inteligencia Artificial de Propósito General).
[262] MADIEGA, T., *op. cit.*, p. 9
[263] Propuesta de Reglamento 2021/0106, *op. cit*., art. 71(5), p. 92.
[264] *Ibidem*, Título VI, Capítulo I, pp. 81-82.
[265] MADIEGA, T. *op. cit*., p. 10

obligatoria en los 6 meses siguientes a la entrada en vigor del reglamento[266], con el objetivo de delimitar el alcance de las definiciones recogidas, y prohibir lo antes posible aquellas actuaciones consideradas inaceptables en la UE.

La segunda etapa atañe a los Títulos III, VI, VIII y X, y concede un plazo de 12 meses para su aplicación tras la entrada en vigor del reglamento[267]. El Título III hace referencia a los sistemas de alto riesgo; el nombramiento de autoridades notificantes y organismos notificados; y el establecimiento de normas, evaluaciones de conformidad, certificados y registros[268]. El Título VI concierne la gobernanza de la IA, para la cual se constituye un Comité Europeo de Inteligencia Artificial, y se designan las autoridades nacionales competentes[269]. El Título VIII se ocupa del seguimiento posterior a la comercialización de sistemas de IA de alto riesgo, así como de su supervisión en el mercado[270]. Por último, el Título X recoge las sanciones aplicables ante las potenciales infracciones[271].

La tercera etapa concibe la aplicación completa del reglamento en un plazo de 24 meses[272], periodo que se considera suficiente para la adaptación total de los interesados a la nueva realidad. Sin embargo, existe una excepcional cuarta etapa, para la que se estiman necesarios hasta 36 meses de adaptación[273]. Esta se refiere a la aplicación total de los anexos[274], concretamente del Anexo II, que contempla la armonización total de la legislación de la UE[275].

A pesar de la delimitación de estas etapas, muchas empresas han empezado su proceso de adaptación para obtener cierta ventaja competitiva, identificando los tipos de IA que utilizan, evaluando su riesgo y su potencial estructura de gobernanza y facilitando la instrucción de sus empleados mediante cursos y campañas informativas.

2.5. Reflexiones generales sobre el capítulo

Si bien el desarrollo digital es una prioridad en la Unión Europea, toda la regulación desarrollada a su alrededor tiene como principal preocupación la protección del individuo. Bajo esta premisa se erige el Reglamento General de Protección de Datos, que se convierte en la pieza clave de la legislación europea en lo relativo a, como su propio nombre indica, la protección de datos de los ciudadanos europeos[276]. Así, sienta las bases esenciales para la navegación segura por la red, en un marco jurídico que busca una normativa armonizada entre los Estados miembros[277]. Por un lado, otorga a los usuarios derechos sobre sus datos personales, como el derecho al acceso, rectificación, supresión u oposición al tratamiento[278]. Por otro lado, establece los principios básicos del tratamiento de datos, siendo estos trato lícito, leal y

[266] *Ídem*.
[267] *Ídem*.
[268] Propuesta de Reglamento 2021/0106, *op. cit*., pp. 51-77.
[269] *Ibidem*, pp. 81-83.
[270] *Ibidem*, pp. 84-90.
[271] *Ibidem*, pp. 91-93.
[272] MADIEGA, T. *op. cit*., p. 10
[273] Fieldfisher, *op. cit.*
[274] Anexos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021. COM (2021) 206.
[275] *Ibidem*, pp. 2-3.
[276] Reglamento (UE) 2016/679, *op. cit.*, párr. 22., p. 4.
[277] *Ibidem*, párr. 10, p. 2.
[278] *Ibidem*, art. 13(2)(b), p. 41.

transparente, limitación de finalidad, minimización, exactitud y actualización, limitación de tiempo de conservación y deber de demostrar el debido cumplimiento[279].

Siguiendo esta misma línea, la Directiva ePrivacy pretende proteger, de forma más específica, las comunicaciones electrónicas, por ejemplo, el correo o la mensajería instantánea[280]. Se concibe de forma complementaria al RGPD, y está vinculado más directamente a cuestiones comerciales. En este sentido, destaca especialmente por constituir el marco normativo de las *cookies*[281]. No obstante, al tratarse de una directiva, cada Estado tiene cierta libertad para adoptar las medidas que considere oportunas, alejando así a la Unión de su objetivo de uniformidad. Esta cuestión, sumada a su aparente falta de eficacia en general[282], termina llevando a la elaboración de una propuesta de reglamentación.

La propuesta de reglamento ePrivacy, además del objetivo evidente de armonizar las legislaciones nacionales, persigue adaptar la directiva vigente a la realidad tecnológica del momento, añadiendo disposiciones para regular servicios de transmisión libre de manera centralizada[283]. Además, introduce propuestas para puntualizar ciertos aspectos en torno a las *cookies*, presentando un modelo más intuitivo y fácil de comprender para el usuario, en el que pueda elegir una configuración predeterminada[284]. Cabe mencionar, adicionalmente, la incorporación del derecho del usuario a bloquear publicidad no solicitada[285].

Por último, el auge de la inteligencia artificial ha conducido, inevitablemente, a la elaboración de un marco legal para su desarrollo, implementación y uso en el territorio de la Unión. Esta regulación establece una clasificación de sistemas de IA en función de su nivel de riesgo; mediante la misma, se establecen normas de mayor y menor severidad, con sus consecuentes sanciones administrativas, también diferenciadas[286]. Asimismo, se crean unos plazos diferenciados para la implementación de medidas, que no entrarán en vigor en su totalidad hasta pasados 36 meses de su publicación en el Diario Oficial de la Unión Europea[287].

[279] *Ibidem*, art. 5, pp. 35-36.
[280] Directiva 2002/58/CE, *op. cit.,* art. 1(1), p. 42.
[281] Directiva 2002/58/CE, *op. cit.,* párr. 24, p. 40
[282] Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, op. cit*., p. 162.
[283] ALONSO LECUIT J., *op. cit*., pp. 2-4.
[284] Evaluation and review of Directive 2002/58, *op. cit*., p. 61.
[285] Propuesta de Reglamento 2017/0003, *op. cit.*, arts. 16-17, pp. 35-36.
[286] Propuesta de Reglamento 2021/0106, *op. cit*., p. 14.
[287] MADIEGA, T. *op. cit*., p. 10

CAPÍTULO 3. LOS RETOS DE LA APLICACIÓN DE LA NORMATIVA EUROPEA DE LA PROTECCIÓN DE DATOS

La legislación europea es una de las más robustas del mundo, en lo que se refiere a la protección de la privacidad de los datos del individuo. Así todo, el avance de la tecnología sigue un ritmo claramente superior al de la elaboración de normativa. Además, la evolución de esta reglamentación debe darse en un relativo equilibrio con respecto al ordenamiento jurídico de otras regiones, de manera que pueda existir un balance entre la cooperación tecnológica y social, el crecimiento económico, y la protección de los derechos de los ciudadanos europeos[288].

En este capítulo se abordarán algunas de las dificultades que entraña el desarrollo de nuevas tecnologías para el cumplimiento de la regulación europea, a saber; la imposibilidad de cumplir con el principio de minimización de datos; la falta de consciencia general de la población al brindar su consentimiento para el tratamiento de sus datos; las dificultades para especificar la finalidad de dicho tratamiento dada la imprevisibilidad del valor de los datos; los potenciales peligros de la transmisión de datos a terceros; el fenómeno de las *cookies* y las limitaciones de su regulación ante la carencia de una categorización clara; la licitud y riesgos de las *paywalls*; y la subestimación de la IA a la hora de inferir datos y reconocer la identidad del individuo mediante la elaboración de perfiles.

3.1. Innovación vs minimización de datos

Uno de los mayores retos a los que se enfrenta la regulación europea en la actualidad es su incompatibilidad con la realidad tecnológica. En este sentido, una de las cuestiones a las que la normativa no ha sabido dar respuesta hasta el momento es el fenómeno del *Big data*.

Al hablar de tecnologías de *Big data*, se hace referencia a un modelo de trabajo que opera con cantidades inabarcables de datos, que engloban tanto aquellos proporcionados por el usuario como los extraídos a partir de su análisis con el uso de algoritmos y otros instrumentos[289]. Por lo tanto, debe tenerse en cuenta que estas tecnologías son intrínsecamente incompatibles con el principio de minimización de datos[290], recogido en el artículo 5 del RGPD[291].

Así todo, cabe plantearse por qué parece primarse el uso de *Big data* sobre la protección de la privacidad del interesado, y cuáles son los potenciales riesgos de su promoción, en vulneración del principio de minimización de datos. Para poder responder a estas preguntas y entender sus implicaciones, debe comprenderse, primeramente, el funcionamiento de estas tecnologías. De manera simplificada, Elena Gil lo divide en dos fases.

La primera fase consiste en la recopilación de datos y su análisis a partir de algoritmos y otros medios automatizados, con el objetivo de inferir tendencias de comportamiento. Mediante

[288] FINNEMORE & HOLLIS, *op. cit*., 465-466.
[289] Tal y como se explica en el apartado 3.1 del capítulo 1.
[290] GIL. E., *op. cit.,* p. 52.
[291] Mencionadas en el capítulo 2, pero, a saber; el trato transparente de los datos; la limitación clara de los propósitos de su recogida; la minimización de datos recogidos para cumplir con un fin establecido; la conservación de dichos datos durante un tiempo delimitado, y nunca más del estrictamente necesario; y el respeto por el derecho de rectificación y de olvido por parte del usuario.

dicho análisis se persiguen una serie de objetivos, tales como la obtención de información relevante o la maximización de un beneficio económico[292].

En el campo de la investigación, el *Big data* resulta una herramienta especialmente útil para adquirir nuevos conocimientos que propulsan la innovación y el progreso social. Así, por ejemplo, el sector sanitario saca provecho del *Big data* realizando estadísticas esclarecedoras a partir de la comparación entre datos de pacientes y resultados de análisis clínicos u otro tipo de pruebas; de esta manera, se puede determinar con precisión la efectividad de un medicamento o la potencialidad de contraer una enfermedad en base a los genes de un individuo, entre otros muchos aspectos[293].

Por otro lado, las empresas pueden utilizar *Big data* para predecir con mayor exactitud el rendimiento de un nuevo proceso o recurso disponible, o para conocer la demanda de un producto o servicio en el mercado; así pueden reducir sus costes, lograr un mayor rendimiento y acelerar la innovación en su cadena de producción. Asimismo, cabe destacar su utilidad para la optimización de estrategias de *marketing*, a partir de la inferencia de los gustos de los clientes, en base a sus búsquedas, compras o reseñas; así, son capaces de personalizar sus sugerencias y publicidad en el navegador, adaptando el contenido ofrecido a sus tendencias de consumo, e impulsando las posibilidades de que realicen una compra[294].

En esta primera fase, por lo tanto, se asocian una serie de datos como pertenecientes a una misma persona[295], para, posteriormente, compararlos con otros datos de otro individuo e inferir variables comunes. El uso que se le da posteriormente a estas correlaciones se recoge en la segunda fase.

La segunda fase consiste en tomar una serie de decisiones, una vez se han recopilados un conjunto de datos y se han extraído unas conclusiones – que se sobreentienden de valor reforzado por el análisis anterior. Así pues, a partir del modelo de correlaciones conformado en la primera fase, se obtienen una serie de conclusiones, cuyo contenido se personaliza a cada individuo[296]. En el sector sanitario, por ejemplo, se estudiarán los datos y circunstancias personales de un paciente (edad, sexo, síntomas, intolerancias…) en tanto que variables de análisis; en función de las correlaciones establecidas en tal análisis, se inferirá la patología del paciente y se decidirá, entre otros aspectos, la medicación o el tratamiento más adecuado para el mismo[297].

Cabe recordar que, de acuerdo con el artículo 6 del RGPD, se precisa del consentimiento previo del usuario para ambas fases, pues tanto su recopilación como su uso se consideran modalidades específicas e independientes de tratamiento de datos[298].

Las ventajas que ofrecen las tecnologías *Big data* son muchas. Retomando el ejemplo anterior, en el sector sanitario un paciente será sometido al tratamiento más ajustado a sus circunstancias personales; y en el sector comercial, un consumidor encontrará el producto más adecuado a sus necesidades y a su capacidad económica, de manera sencilla – por ejemplo,

[292] GIL, E., *op. cit*., pp. 56-58.
[293] European Data Protection Supervisor. "Opinion 7/2015 on Meeting the challenges of big data", del 19 de diciembre de 2015, p. 7.
[294] GIL, E., *op. cit.,* p 124.
[295] Esto no implica la identificación del individuo, sino que su identidad puede permanecer oculta, por ejemplo, tras un código.
[296] GIL, E., *op. cit*., p. 58.
[297] *Ídem*.
[298] Definido en el artículo 4(2).

obteniendo los resultados de búsqueda en su idioma de manera predeterminada –, intuitiva – obteniendo primero los resultados de páginas en las que haya navegado previamente y donde, por lo tanto, se encuentre cómodo –, y rápida –teniendo su dirección de correo registrada, de manera que no tenga que introducirla en repetidas ocasiones[299].

Sin embargo, los riesgos para la privacidad del usuario merecen también especial atención. En los siguientes apartados se hará un repaso de algunas de las problemáticas más importantes en lo referente a la proliferación de datos y ciertas lagunas en la legitimación de su tratamiento.

3.2. Limitación de la finalidad y consentimiento del usuario

Uno de los mayores peligros para la protección de datos de los ciudadanos reside en el conocimiento del usuario, o más bien, en su falta de conocimiento, a la hora de ejercer sus derechos sobre sus datos, o bien, de tener un control consciente de los mismos. Así, la normativa establece que el tratamiento de datos debe darse siempre con el consentimiento del usuario al que le conciernen. No obstante, son varias las problemáticas en torno a las políticas de consentimiento.

3.2.1. Lenguaje sencillo y comprensible o detallado y complejo

En primer lugar, en lo que se refiere a la obtención de consentimiento existe una polémica paradójica. Por un lado, parece necesario que el usuario disponga de información ampliamente detallada sobre el tratamiento que se va a dar a sus datos antes de que lo acepte[300]. Sin embargo, el artículo 7 del RGPD mantiene que el consentimiento debe brindarse bajo unas condiciones concretas, entre ellas, que se otorgue "de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo"[301].

La cuestión está, simplemente, en que los usuarios rara vez leen las condiciones de las políticas de privacidad; y de entre los pocos que sí las leen, la mayoría no alcanza a entender sus implicaciones[302]. Así, se abre un debate entre si es preferible ofrecer un texto completo, pero demasiado largo y difícil de comprender para el interesado; o si, por el contrario, es más adecuado redactar una política con un lenguaje sencillo y breve, de forma que el usuario lo lea y le resulte comprensible. No obstante, el riesgo de esta segunda opción es que pueda dar lugar a imprecisiones y vacíos legales[303].

Asimismo, cabe destacar otro tipo de procedimientos que entorpecen la comprensión del usuario y desincentivan su interés[304]. Un ejemplo claro es la comunicación de cambios en las políticas de términos y condiciones de uso; en estos casos, si bien lo más sencillo sería, simplemente, compartir con los interesados solamente los cambios realizados, es más común que la empresa remita la política entera, que, de nuevo, será demasiado larga y compleja para que el usuario dedique tiempo a leerla.

[299] GIL, E., *op. cit*., pp. 28-32.
[300] European Data Protection Supervisor, *op. cit*., p. 15.
[301] Reglamento (UE) 2016/679, *op. cit.,* art. 7, p. 37.
[302] GIL, E. *op. cit*., pp. 132-133.
[303] *Ibidem*, pp. 71-72.
[304] European Data Protection Supervisor, *op. cit*., p. 13.

3.2.2. Especificidad de la finalidad

Independientemente de si los usuarios leen o no tal política, existe una problemática adicional acerca del alcance de su consentimiento. El artículo 6 del RGPD señala que el tratamiento de los datos solo se considera lícito cuando "el interesado dio su consentimiento (…) para uno o varios fines *específicos*[305]". No obstante, las tecnologías *Big data* operan con grandes cantidades de datos que se intercambian de forma constante e impredecible[306], y que realmente adquieren valor una vez han sido recopilados y comparados con otros, al dar lugar a resultados aprovechables[307].

Así pues, a pesar de que el usuario dé su consentimiento para la finalidad señalada en la política inicial, las conclusiones obtenidas de estos datos, y el uso secundario que se haga de esta información, debe contar con un consentimiento adicional. Por lo tanto, es incorrecto asumir que los datos inferidos a partir de un análisis son propios de las empresas que lo realizan; pues la realidad es que siguen siendo datos personales[308].

Más allá de esto, cabe destacar que el alcance del término "específico" se ha ido precisando progresivamente. Por ejemplo, en la jurisprudencia española, la AEPD ha señalado que la referencia a fines *publicitarios*[309] es insuficiente[310]. Así lo expresa también, de manera inequívoca, en su Informe Jurídico 325/2004:

> *"(...) la mera referencia al uso de los datos con fines de 'publicidad' o 'remisión de información' de productos o servicios, sin especificar el sector al que los mismos vienen referidos no resultaría suficiente para considerar el consentimiento prestado como 'específico' e 'inequívoco'"* [311].

Por lo tanto, la finalidad del uso de datos debe expresarse de manera exhaustiva, pues cualquier actuación ligeramente improvisada, en base a la obtención de resultados impredecibles, se debería desestimar, en tanto que es considerada contraria a la normativa europea[312].

3.2.3. El caso de Cambridge Analytica como reflejo de la importancia de las políticas de consentimiento

Un caso claro del uso secundario – y, adicionalmente *no consentido*[313] – de datos personales, es el escándalo Facebook-Cambridge Analytica[314].

---

[305] Cursiva añadida.
[306] GIL, E. *op. cit*., p. 73.
[307] *Ibidem*, p. 18.
[308] Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación (2020/2717(RSP)). Párr. 9, p. 15.
[309] Cursiva añadida
[310] ROSELLÓ MALLOL, V. "Marketing y Protección de Datos (VI): comunicación de datos a terceros y encargo del tratamiento de datos. Transferencias internacionales de datos". *Noticias Jurídicas*.
[311] Agencia Española de Protección de Datos: 325/2004. "Comunicación de datos entre empresas de un mismo grupo", 28 de julio de 2004
[312] European Data Protection Supervisor, *op. cit*., pp. 13-15.
[313] Cursiva añadida
[314] Ha de tenerse en cuenta que en este caso el RGPD todavía no estaba completamente implementado en el momento del escándalo. Este ejemplo se presenta con el único fin de hacer entender de forma clara lo que se

Cambridge Analytica era una empresa británica especializada en la recopilación y análisis de datos destinados a la segmentación publicitaria; esto es, la creación de publicidad conductual personalizada, en base al perfil del usuario. Con este fin, la compañía creo una aplicación llamada "thisisyourdigitallife"; básicamente, su actividad consistía en la realización de un test de personalidad, basándose en las respuestas de usuarios a una encuesta. Esta prueba estaba destinada, inicialmente, a fines académicos[315], y se incentivaba su uso a través de un pequeño pago – de uno o dos euros – a cambio de completar la encuesta. La problemática de este caso se divide en dos ramificaciones.

Por un lado, para realizar la encuesta, los usuarios tenían que conectarse a través de su cuenta de Facebook, lo que daba a la empresa acceso al perfil de los participantes en la red social, y a todos sus datos generados en la plataforma. Pero, además, la compañía podía acceder a los contactos de los usuarios en la red; es decir, si un usuario tenía cien "amigos" en Facebook, Cambridge Analytica podía acceder al perfil y datos de cada uno de ellos, independientemente de si habían utilizado la aplicación 'thisisyourdigitallife' o no[316].

Así, presuntamente, Facebook permitió que, aunque fueron unas 270 000 personas las que respondieron a tal encuesta, brindando su consentimiento – dicho sea de paso, de manera cuestionable – la empresa pudiera recopilar datos de 50 M de usuarios, sin que estos fueran conocedores de ello. Esto conlleva indiscutiblemente una vulneración del derecho de los usuarios que no dieron, en ningún momento, su consentimiento para la recopilación de sus datos[317].

Por otro lado, Cambridge Analytica fue acusada de incumplir el principio de limitación de finalidad; pues, si bien había alegado que la recopilación de datos a través de la aplicación 'thisisyourdigitallife" perseguía fines de investigación, el escándalo surgió, precisamente, por la revelación de que los datos habían sido utilizados en campañas electorales, concretamente, la del Brexit y la de Donald Trump, en 2016[318].

A través de este ejemplo, pueden apreciarse los diferentes problemas de la normativa en lo referente al consentimiento:

(1) Los usuarios no leyeron las condiciones de uso, y no eran conscientes de estar compartiendo sus datos de Facebook.
(2) La finalidad inicial y consentida (la investigación) no se correspondía con el uso final que se dio a los datos (generación de publicidad segmentada y personalizada en campañas electorales).

Para hacer frente a este tipo de problemáticas, podría contemplarse la posibilidad de profundizar ciertos aspectos del RGPD, haciendo mayor hincapié en la importancia de desarrollar políticas de privacidad más claras y concisas. Es decir, sería aconsejable incentivar a las empresas que utilizan este tipo de contratos, a que los hagan más sencillos, intuitivos y

entiende por "uso secundario y no consentido" de datos personales brindados y consentidos para un fin explícito, y sus posibles riesgos.

[315] European Parliament resolution (2020/C 345/10) of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP)). P. 3.

[316] VERCELLI, A. "Facebook Inc. - Cambridge Analytica: (des)protección de datos personales y campañas globales de desinformación. Grupo de Investigación" *Ciencia, Tecnología, Universidad y Sociedad (CITEUS),* 2019, p. 60.

[317] *Ibidem*, p. 61.

[318] *Ibidem*, p. 59.

atractivos para el interesado, de manera que se incentive, a su vez, el interés del individuo por tener conocimiento e interés por la protección de su información personal[319].

Por otro lado, en relación con la publicidad política, cabe destacar la labor de la UE, en su elaboración del Reglamento 2024/900 sobre transparencia y segmentación en la publicidad política[320]. Así, obliga a incluir una declaración clara, destacada e inequívoca de que el contenido compartido es un anuncio político, así como la identidad del patrocinador[321]. Adicionalmente, prohíbe estrictamente la elaboración de perfiles, y restringe el uso de publicidad segmentada en base a los datos personales, de forma que solo sea aceptable cuando el interesado dé su consentimiento informado y explícito[322]. Con ello se pretende que el individuo pueda reconocer la publicidad política y distinguirla de otro tipo de contenido, como, por ejemplo, opiniones a título personal de otro sujeto, o campañas de desprestigio, de manera que pueda tomar decisiones de forma más consciente e informada[323].

3.3. Transmisión de datos a terceros

En relación con el caso Facebook-Cambridge Analytica, cabe hacer una mención a la relevancia de la transmisión de datos a terceros. Así, en su afán por movilizar y promover el mercado europeo de datos, la UE adoptó el Reglamento 2023/2854[324], que complementa al RGPD y a la Directiva 2002/58/CE[325]. A través de este, se pretende establecer unas normas de interoperabilidad en el mercado de datos, para continuar estimulando la innovación y el intercambio de información dentro de los umbrales de un marco regulador. De esta manera, favorece, entre otros aspectos, el traslado y venta de datos[326] a terceros para su utilización. Este uso está, por supuesto, supeditado al consentimiento del usuario a través de un contrato, que debe incluir una cláusula que recoja el fin específico que el tercero pretende dar a dichos datos[327]. Este contrato puede darse de muchas formas; entre ellas, una política de términos y condiciones de uso en una aplicación, o las políticas de aceptación de *cookies* en una página web.

3.3.1. Términos y condiciones de uso

Esta normativa, aplicada de forma justa, resulta muy enriquecedora, tanto para las empresas que operan con estos datos, como para los usuarios, a los que se les da acceso a servicios y productos más personalizados.

No obstante, también favorece la aparición de nuevos modelos abusivo, en los que el usuario esté obligado a aceptar la transmisión de sus datos a terceros si quiere utilizar un determinado

[319] GIL, E. *op. cit*., p 143-144.
[320] Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo de 13 de marzo de 2024 sobre transparencia y segmentación en la publicidad política (Texto pertinente a efectos del EEE).
[321] *Ibidem*, art. 11, pp. 28-29.
[322] *Ibidem*, art. 18, pp. 35-36.
[323] *Ibidem*, párr. 74, p. 14.
[324] Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).
[325] En tanto que consideradas normativas base para la protección de la privacidad de datos.
[326] En este caso, personales y no personales.
[327] Reglamento (UE) 2023/2854, párr. 25, pp. 8-9.

servicio. Esta situación se ve plasmada en el actual asunto sometido ante el TJUE, *Meta Platforms Inc. c. Bundeskartellsamt*, C-252/21[328]. En este caso, la autoridad alemana de competencia, el *Bundeskartellsamt*, demanda a Meta por obligar al interesado a aceptar en su totalidad sus condiciones y términos de uso, si quiere utilizar sus plataformas; incluyendo esto la remisión de publicidad conductual personalizada y otras cláusulas consideradas abusivas[329]. En este sentido, el usuario no puede elegir si quiere o no aceptar ciertas condiciones, porque ello limitaría su acceso a las redes sociales del complejo de Meta (Facebook, Instagram y WhatsApp, entre otros). Así, se considera que Meta estaría abusando de su posición dominante en el mercado, y forzando una transmisión de datos que, de ser evitable, no se llevaría a cabo[330].

Así todo, para hacer referencia a la transmisión de datos a terceros y la existencia de políticas abusivas, no es necesario remitirse a casos de tal envergadura; pues lo cierto es, que se trata de una realidad a la que el usuario se enfrenta en su día a día, meramente a través del uso de *cookies*.

3.3.2. Las cookies

El consentimiento de las *cookies* presenta grandes paralelismos con respecto a las políticas de condiciones de uso; de hecho, la normativa aplicable a la validez del consentimiento y al tratamiento de datos obtenidos a partir de *cookies* es la misma en ambos casos, es decir el RGPD[331]. Así todo, la aceptación de las *cookies* es, en cierta medida, más compleja, dado que muy pocos entienden realmente en qué consisten, y son aún menos los que leen las opciones disponibles a la hora de rechazarlas o de aceptarlas, total o parcialmente.

De forma resumida, las *cookies* son una tecnología de seguimiento individual que segmenta datos de los usuarios, y que pueden, posteriormente, incluirse en el conjunto de *Big data*. Se trata de paquetes de información, que la página web almacena cuando el usuario la visita[332]. No obstante, estos datos pueden ser recopilados no solo por el sitio web visitado[333], sino también por socios con los que trabaje esa página[334]. Los paquetes de información recopilados por estos asociados se denominan *cookies* de terceros[335].

Al entrar en una página web, la reglamentación europea establece que el usuario debe tener la elección de rechazar todas las *cookies,* o bien de aceptarlas, de forma total o granular, es

[328] Asunto C-252/21. Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023 (petición de decisión prejudicial planteada por el Oberlandesgericht Düsseldorf — Alemania) — Meta Platforms Inc., anteriormente Facebook Inc., Meta Platforms Ireland Limited, anteriormente Facebook Ireland Ltd., Facebook Deutschland GmbH contra Bundeskartellamt, con intervención de Verbraucherzentrale Bundesverband e. V.

[329] Permitían recolectar datos del usuario y de su dispositivo, a través de todas las plataformas de la empresa y otros interfaces en sitios web o aplicaciones de terceros conectados a "Productos de Facebook"; estos datos eran luego combinados en la red de Facebook,com para su tratamiento. Cabe destacar que esto incluiría información referente al número de teléfono del usuario, su ubicación o sus datos de transacción y métodos de pago, entre otros.

[330] GÓRRIZ LÓPEZ, C. "Tratamiento de datos personales y defensa de la competencia (Meta Platforms Inc v Bundeskartellamt)". *Derecho y digitalización empresarial, UAB* (s.f.).

[331] KUBICECK, K., *op. cit*., pp. 1-2.

[332] *Ídem*.

[333] Article 29 Data Protection Working Party. "Opinion 04/2012 on Cookie Consent Exemption". Adoptado el 7 de junio de 2012, pp. 4-5.

[334] Pueden ascender fácilmente a los 800 asociados.

[335] Es decir, cookies establecidas por páginas con un dominio diferente al de la página visitada.

decir, aceptar las esenciales, pero rechazar las de terceros. Además, estas opciones deben presentarse de manera clara, de forma que el usuario tenga una elección real, libre y consciente de cómo ejercer sus derechos sobre sus datos y dar su consentimiento expreso[336].

El conflicto más evidente que existe a este respecto es esta última cuestión. Así, puede cuestionarse cómo de claros son los *pop-ups*[337] que presentan las opciones de *cookies*; es muy común que el enlace de "aceptar todas" se muestre en mayúsculas, con un tamaño de fuente grande, y dentro de un cuadro a color; mientras que la opción de "rechazar todas", "elegir configuración", o similar, aparece a menudo en una esquina, en un tono gris y con una letra minúscula de menor tamaño[338]. No obstante, incluso si estos diseños pueden resultar controvertidos, es un aspecto complejo de regular de forma general, pues no es obligatorio el uso de un formato estándar en cada página. Así pues, se trata de una cuestión que debería analizarse caso a caso.

Por otro lado, resulta problemática la falta de una clasificación legal reconocida a nivel internacional sobre los tipos de *cookies* que existen. Tomando como ejemplo la categorización de la *International Chamber of Commerce*[339], Karel Kubicek distingue[340] entre:

(1) Esenciales: estrictamente necesarias para el funcionamiento de la página.
(2) Funcionales: personalizan el contenido de la página, pero no son necesariamente esenciales para su correcto funcionamiento.
(3) Analíticas: estudian el comportamiento del usuario y se utilizan de forma acumulativa, es decir, combinándolas con otras de diferentes bases de datos para construir un perfil completo del usuario.
(4) Publicitarias: son utilizadas para segmentar la publicidad, a partir del seguimiento de la actividad del usuario en diferentes dominios[341].

Dada la falta de una categorización oficial, Kubiceck mantiene que pueden surgir ciertas disconformidades que lleven a lo que él considera una clasificación incorrecta; esto es, por ejemplo, categorizar ciertas *cookies* analíticas – posiblemente, las más invasivas – como esenciales para el funcionamiento de la página visitada; obligando así al usuario a aceptarlas[342]. Ahora bien; se sobreentiende que, de manera general, al visitar una página web, no es un requisito indispensable que un tercero recopile los datos del usuario, puesto que no es necesario para el funcionamiento de la página web en cuestión, sino que suelen estar destinadas a un servicio alternativo[343].

Además, puede surgir una complicación adicional en aquellos casos en los que una misma *cookie* esté destinada a fines múltiples, como, por ejemplo, recordar las preferencias de navegación y realizar un seguimiento de la actividad del usuario. Es necesario que el usuario dé su consentimiento expreso para ambas utilidades, de manera que no se vea obligado a aceptar

[336] Article 29 Data Protection Working Party, 7 de junio de 2012, *op. cit*., p. 5.
[337] Ventanas emergentes.
[338] KUBICECK, K., *op. cit*., p. 16.
[339] Cámara Internacional de Comercio de Reino Unido.
[340] KUBICECK, K., *op. cit*., p. 60.
[341] Direcciones de sitios web.
[342] KUBICECK, K., *op. cit*., pp. 72-74.
[343] *Ídem*.

el seguimiento de su actividad simplemente por querer que se recuerden sus preferencias de navegación[344].

Así, independientemente de que la página web proporcione al usuario una clasificación de los tipos de *cookies* que utiliza y de su finalidad, Kubiceck señala que el 25,4 % de las páginas web analizadas en su investigación recogen *cookies* no clasificadas en ninguna categoría[345]; e incluso, que un 82,5 % de dichas páginas utilizaban *cookies* que ni siquiera estaban declaradas, es decir, no ponían a disposición del usuario información acerca de su finalidad[346].

Por último, existe una fuerte controversia con respecto a la licitud de las conocidas como *cookie walls* o "muros de *cookies*"; estas son, como su nombre indica, barreras a ciertas páginas web, que restringen el acceso del usuario al contenido de las mismas si no aceptan todas las *cookies*. Esta práctica se considera contraria a la normativa europea, concretamente, al principio del consentimiento libre tal y como se define en el considerando 43 del RGPD[347]. Así lo señalaba[348] en 2016 el Grupo de Trabajo del artículo 29[349], que indicaban que esta aproximación, que caracterizaba como "tómalo o déjalo"[350] no cumplían los principios legítimos de consentimiento, puesto que "si las consecuencias del consentimiento menoscaban la libertad de elección de los individuos, el consentimiento no sería libre"[351].

Así pues, se considera que el problema de las *cookie walls* reside en que no ofrecen una opción alternativa al usuario para acceder a la información, producto o servicio de una página web[352]. Tomando esto en consideración, ha comenzado a extenderse una nueva práctica, conocida bajo el nombre de *paywalls*.

3.3.3. Las paywalls como alternativa al tratamiento de datos

El concepto de *paywalls* es aplicable tanto en el contexto de las *cookies* como en otros servicios, por ejemplo, el de las redes sociales. Siguiendo la línea anterior, las *paywalls* se ajustarían a un lema de "págalo, tómalo o déjalo"; es decir, dan al usuario tres opciones. Primero, pagar, y rechazar así el tratamiento de sus datos; segundo, no pagar, pero asumir que todos sus datos van a ser tratados; y tercero, renunciar a los servicios de la página.

---

344 *Ibidem*, p. 65.
345 *Ibidem*, p. 66.
346 *Ídem*.
347 "Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento".
348 Article 29 Data Protection Working Party: "Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)". Adoptado el 19 de julio de 2006, p. 16.
349 Creado por la Directiva 95/46/CE, trataba cuestiones relacionadas con la protección de la privacidad y los datos personales hasta la entrada en aplicación del RGPD en 2018.
350 Traducción propia de: "take it or leave it"
351 Traducción propia de: "if the consequences of consenting undermine individuals' freedom of choice, consent would not be free".
352 Article 29 Data Protection Working Party, 19 de julio de 2006, *op. cit*., p. 17.

Por un lado, parece lógico que las páginas web y las redes sociales implementen esta medida. Hace años que se ha normalizado el acceso a las mismas de forma gratuita, pero la realidad es que son empresas que se financian, en gran medida, a partir de la información que sus usuarios les brindan. Así pues, estos servicios no son gratuitos, sino que los datos se convierten en el instrumento de trueque, que es posteriormente monetizado. Por lo tanto, si estas empresas dejan de tener acceso a los datos de los usuarios, deben encontrar formas alternativas de obtener ingresos; una de estas sería exigir directamente el pago de una cantidad determinada de dinero[353]. Así lo hacen muchos periódicos, por ejemplo, El País.

Es también la intención de Meta, tras el mencionado revuelo causado por su confrontación con el *Bundeskartellsamt*. Así, en el asunto C-252/21, el TJUE determinó que las opciones de pago podrían ser una alternativa válida y ajustada el principio de consentimiento libre.

> "Así pues, en el marco del proceso contractual, esos usuarios deben disponer de la libertad de negarse individualmente a prestar su consentimiento a operaciones particulares de tratamiento de datos que no sean necesarias para la ejecución del contrato, sin verse por ello obligados a renunciar íntegramente a la utilización del servicio ofrecido por el operador de la red social en línea, lo que implica que se ofrezca a dichos usuarios, *en su caso a cambio de una remuneración adecuada*[354], una alternativa equivalente no acompañada de tales operaciones de tratamiento de datos".[355]

No obstante, los problemas de estas *paywalls* son varios, si bien en esta ocasión se señalarán cinco. En primer lugar, como se ha mencionado anteriormente, los usuarios no están al tanto de lo que implica compartir su información; por lo tanto, ante la posibilidad de obtener un servicio "gratuito", no dudarán en aceptar el tratamiento de todos sus datos. Adicionalmente, la posibilidad de elegir entre "gratuito" o "de pago", desincentivará todavía más el interés de los usuarios por leer las condiciones de tratamiento[356], lo que además aumenta las probabilidades de que este método sea utilizado en páginas web con intereses poco legítimos para exigir la aceptación de un tratamiento desproporcionado de los datos o bien realizar un pago[357].

En segundo lugar, existe otro problema evidente, y es que los datos de los usuarios ya están, irremediablemente, en el ciberespacio. Es cierto que algunos de ellos están sujetos a contratos que se comprometen con la eliminación de tales datos después de un tiempo determinado. Pero el hecho de que ya existan perfiles de los usuarios implica que, incluso si estos dejan de estar alimentados con tanta información de forma constante, podrían seguir en uso y actualizándose de forma más moderada, por ejemplo, a partir de la recopilación de *cookies* o de otros datos esenciales para el disfrute de un servicio[358].

---

[353] MOREL, V. et al. "Your Consent Is Worth 75 Euros A Year – Measurement and Lawfulness of Cookie Paywalls". *Association for Computing Machinery*, 2022, p. 213.
[354] Cursiva añadida.
[355] Asunto C-252/21*, op. cit*, párr. 150.
[356] D'AMICO, A. et al. "Meta's pay-or-okay model: an analysis under eu data protection, consumer and competition law". *Utrecht Centre for Regulation and Enforcement in Europe Working Papers*, 8 de abril de 2024, p. 10.
[357] *Ibidem*, p. 21.
[358] *Ibidem*, p. 7.

En tercer lugar, cabe destacar que, en muchas ocasiones, la conservación de privacidad ni siquiera depende de los datos que proporcione el usuario. Así, Elena Gil señala que es posible acceder a información no expuesta de un individuo, tomando la proporcionada por un contacto en una red social[359]. Según explica a partir de un estudio realizado por Alan Misolve[360], basándose en los datos que algunos usuarios exponen acerca de su grado universitario, año de graduación y dormitorio en residencias universitarias, se puede obtener esa misma información de estudiantes que no la habían revelado. Por lo tanto, el hecho de que un usuario trate de salvaguardar su privacidad y restringir el tratamiento de sus datos, a partir de un pago o de cualquier otro método, no le da ninguna garantía de que su información esté realmente protegida[361].

El cuarto problema identificable se da al respecto del concepto de "remuneración adecuada", tal y como se indica en la sentencia del TJUE del 4 de julio de 2023. En este sentido, cabría preguntarse cuánto cuestan los datos de los usuarios y cuánto se debería exigir en compensación. Y es que Meta estudia la posibilidad de establecer tarifas de hasta 13 € mensuales por el uso de Facebook e Instagram, para respetar la decisión del TJUE en el asunto C-252/21. Por supuesto, cada empresa es libre de establecer su modelo de negocio, así como sus precios; no obstante, si se compara con otras plataformas, estas tarifas pueden parecer excesivas[362]. Así, Netflix, cobra también 13 € mensuales a sus suscriptores por su tarifa estándar, pero ofrece un contenido cuyo coste es mucho mayor que el que se encuentra normalmente en las redes sociales, alimentadas básicamente por los propios usuarios.

El quinto y último problema sería, de nuevo, la posibilidad de que esta herramienta fuera utilizada de manera abusiva, en el sentido de que la opción sea "todo o nada"; es decir, que no se le dé al usuario la posibilidad de escoger una opción intermedia, pagando una tarifa más reducida, y aceptando unas determinadas opciones para el tratamiento de sus datos[363]. En este sentido, sería más viable ofrecer modelos de suscripción con diferentes niveles de acceso y precios, de manera que el usuario tuviera la libertad de dar o retirar su consentimiento en operaciones particulares, sin que ello implicara la renuncia íntegra del servicio[364].

Así pues, si bien es cierto que las *paywalls* pueden ser una opción legítima para asegurar la supervivencia económica de algunas empresas, y una alternativa lícita al tratamiento de datos, no implican una garantía absoluta de la intimidad y la protección general del usuario. Por lo tanto, su implementación no debería ser aceptada sin una regulación adicional, pues podrían suponer un detrimento para la privacidad de los usuarios e incentivar prácticas abusivas por parte de las empresas[365].

[359] GIL, E. *op. cit*., p. 75.
[360] MISOLVE, A. et al. "You are who you know: inferring users profiles in online social networks". *Conferencia WSDM* 2010, 4-6 de febrero de 2010, Nueva York, p. 2.
[361] GIL, E. *op. cit*., p. 76.
[362] D'AMICO, *op. cit*., p. 21.
[363] *Ibidem*, p. 18.
[364] GÓRRIZ LÓPEZ, C., *op. cit.*
[365] D'AMICO, *op. cit*., p. 4.

3.4. La IA y los peligros de la elaboración de perfiles

En los apartados anteriores se han señalado una serie de problemáticas en la normativa europea para la protección de los datos personales del individuo, con aproximaciones que corresponden tanto al RGPD como a la regulación en torno al uso de las cookies[366]. Se ha resaltado en varias ocasiones la falta de concienciación de los ciudadanos con respecto a su privacidad; y es que, de manera generalizada, el ciudadano promedio considera que dar acceso a ciertos datos no puede causarle ningún tipo de daño.

Es cierto que permitir el tratamiento de datos personales no acarrea necesariamente perjuicios; no obstante, cuanto menos se protege la información personal, más aumenta el riesgo de exposición a un daño. Así, al navegar sin consciencia, se alimenta al Big data con nuestros gustos, nuestros miedos, nuestros trabajos, nuestros familiares y, lo que más preocupaciones parece despertar; nuestra cuenta bancaria. La herramienta encargada de asociar toda esa información a un individuo es la IA.

3.4.1. Re-identificación del individuo

La IA es una herramienta destinada al análisis y procesamiento de *Big data*. Así, tratará los datos que se recopilen en la red y los procesará para darles una utilidad, estableciendo correlaciones entre individuos, intereses, tendencias u otras cuestiones que tengan un potencial social o económico de valor[367].

El operar con datos y analizarlos no conlleva *directamente*[368] la exposición de la identidad del interesado. De hecho, según un testimonio de un ingeniero de Google, citado en el libro *Big data, privacidad y protección de datos*, la identidad del usuario ni siquiera resulta interesante – o al menos, no *en la mayoría de los casos*[369]; puesto que aquello que se considera realmente útil son los atributos de comportamiento, que permiten encontrar una correlación de patrones comunes[370].

Así pues, el interés primario de las tecnologías de análisis de datos no es la identificación del individuo. Sin embargo, no debe descartarse esta posibilidad, y la regulación europea exige la aplicación de técnicas y medidas que garanticen un compromiso con la preservación de la privacidad del usuario[371].

Una de las opciones propuestas es la *pseudonimización*[372], es decir, omitir los datos que hagan al individuo identificable directamente – como el nombre o apellidos – y sustituirlos por

[366] Tomando en consideración tanto la Directiva 2002/58/CE como la propuesta de reglamento.
[367] SARTOR, G. "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence". *Scientific Foresight Unit (STOA).* Junio 2020, p. 1.
[368] Cursiva añadida
[369] Cursiva añadida
[370] GIL, E. *op. cit*., p. 101.
[371] European Parliamentary Research Service, op. cit., pp. 69-70.
[372] Definida en el art. 4(5) del RGPD como "tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

otra variable. Durante un tiempo, se utilizaba, por ejemplo, el número de la Seguridad Social; no obstante, este ha pasado a considerarse un dato personal que permite la identificación del individuo[373]. Así pues, actualmente, para llevar a cabo una *pseudonimización*, se utiliza un código de valor generalizado o aleatorio[374].

Por otra parte, cabe la posibilidad de utilizar técnicas de *anonimización*, es decir, omitiendo directamente todas las variables de datos que hagan al usuario identificable. No obstante, una vez *anonimizados*, el RGPD no sería aplicable[375], puesto que esta normativa solo afecta a aquellos datos que permitan la identificación directa o indirecta del usuario[376].

En principio, utilizando estas técnicas, el usuario debería tener la libertad para operar en el ciberespacio, registrarse en redes sociales, suscribirse a plataformas, realizar compras o descargarse aplicaciones con la seguridad de que el almacenamiento de sus datos podrá ser accesible tan solo de forma parcial y por lo tanto no debería comprometer su intimidad. Sin embargo, el problema reside en que, hoy en día, gracias a la existencia del *Big Data* y a su explotación mediante la IA, cabe la posibilidad de poner en común los datos parciales – ya sean *pseudonimizados* o *anonimizados* –, de diferentes bases de datos, y averiguar, a través de su combinación, la identidad de un individuo[377].

Así, en 2008, dos investigadores de la Universidad de Texas, Narayanan y Shmatikov, demostraron poder identificar a usuarios de Netflix a partir de datos no personales, a saber; la calificación que le daban a una serie de películas, y la fecha en la que se realizó tal calificación[378]. A través de la comparación de esos datos con los recopilados en IMDb[379], los investigadores pudieron revelar la identidad de los usuarios[380].

No obstante, como los propios Narayanan y Shmatikov explican en su estudio del caso sobre el Premio Netflix, la cuestión no es que el hecho de que suscribirse a una plataforma audiovisual de este tipo suponga directamente un riesgo a la privacidad del usuario; sino que lo que tratan de demostrar es que incluso información que parece nimia puede ser utilizada de forma injusta, o bien para acceder a datos personales muy valiosos gracias a las tecnologías *Big data*, incluyendo datos sensibles[381].

[373] GIL, E., *op. cit*., p. 90-91.
[374] *Ibidem*, p. 89.
[375] *Ibidem*, p. 51.
[376] Reglamento aplicable, según su artículo 4(1), a un individuo identificable, directa o indirectamente.
[377] European Data Protection Supervisor, *op. cit*., p. 15
[378] Expuesta con motivo de un concurso para mejorar el algoritmo de recomendación; no proporcionaba más información que la indicada, y además, agregaba ruido para proteger aún más la privacidad de sus usuarios.
[379] Base de datos de película donde los usuarios pueden registrarse para publicar sus votaciones y valoraciones.
[380] NARAYANAN, A. & SHMATIKOV, V. "Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)". *Universidad de Texas*, 5 de febrero de 2008, p. 11.
[381] *Ídem*.

3.4.2. Inferencia de información sensible

Disponer de este tipo de información puede causar grandes estragos en la intimidad del usuario. Así, puede, por ejemplo, causar prejuicios de tipo moral, sacando a la luz cuestiones que el interesado puede preferir mantener en privado. Esta fue una de las polémicas más destacadas en la investigación de Narayanan y Shmatikov, pues permitió inferir otro tipo de datos personales, tal como la orientación sexual de los usuarios. Este tipo de información, que debería ser intrascendente, puede ser utilizada contra el individuo, en contextos comunes como una preselección para conseguir un trabajo[382]; o en situaciones más extremas, como en un viaje a un país donde la homosexualidad esté penada[383].

Aún más, la sobreexposición del individuo y de su información sensible lo convierte en un blanco más fácil a ataques de suplantación de identidad o de ingeniería social, y lo hace más vulnerable ante posibles manipulaciones[384], como, por ejemplo, en asuntos de naturaleza política[385].

Volviendo al ejemplo de Cambridge Analytica, lo que convirtió a este caso en una noticia escandalosa y ampliamente extendida, fueron las acusaciones de que los datos personales recopilados habían sido utilizados en campañas electorales, concretamente en la campaña del Brexit y en la de Trump. Así, según las alegaciones, se elaboraba un perfil de cada usuario a través del análisis de dichos datos, y se segmentaba la publicidad electoral[386]. A los afines al partido promocionado se les dirigía publicidad que reforzara esta afinidad; a los que distaban mucho de la posición de tal partido, se les dirigía publicidad disuasoria del grupo contrario; no obstante, los usuarios que marcaban una diferencia realmente en esta campaña publicitaria eran aquellos con ideas poco definidas o intermediarias. Estas personas se incluían en un grupo denominado "persuasible". A partir de la creación de un análisis de sus gustos, intereses o miedos, se les compartía publicidad personalizada para influir en su voto; de esta manera, el grupo de los, digamos, "indecisos", pasaron a posicionarse. Según testimonios de empleados de la compañía "veían en el mundo tal y como queríamos que lo vieran"[387], sin importar si para ello les hacían ver noticias verdaderas o falsas[388].

Asimismo, se puede facilitar, por ejemplo, la categorización del individuo, que puede favorecer, entre otras cuestiones, la aplicación de discriminación de precios. Por ejemplo, en el marco sanitario, a una persona que presente un cuadro médico con ciertas complicaciones se le podrá asignar un seguro médico de mayor coste[389]. O, en un contexto comercial, si se identifica

[382] Se sobreentiende, en una empresa donde impere un pensamiento homófobo y discriminatorio
[383] XENIDIS, R. "Tuning EU equality law to algorithmic discrimination: Three pathways to resilience". *Maastricht Journal of European and Comparative Law*. Vol. 27(6) 736–758, p. 744.
[384] EBERS, M. et al. "The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)". *J – Multidisciplinary Scientific Journal*, núm. 4, 8 de octubre de 2021, p. 592.
[385] Por ejemplo, identificando potenciales votantes a un partido político en función de sus conexiones en redes sociales y sus "amigos" o "me gustas".
[386] La UE está trabajando para prohibir esta práctica, con una propuesta de la Comisión (Reglamento sobre la transparencia y la segmentación de la publicidad política el 25 de noviembre de 2021).
[387] Traducción propia. Original: "they saw the world the way we wanted them to".
[388] AMER, K. & NOUJAIM, J. (2019). El gran hackeo. [Documental]. Netflix.
[389] EBERS, M. et al., *op. cit.,* p. 594.

al individuo como un comprador con interés especial en un producto – por ejemplo, cuando visita un anuncio en repetidas ocasiones – se aumenta el precio del producto[390].

Además, no debe obviarse la existencia de otros actores maliciosos, cuyo objetivo se limita al beneficio personal en perjuicio del usuario[391]. En este sentido, el hecho de que los datos estén presentes en un número incontable de bases de datos implica una sobreexposición del interesado y una mayor posibilidad de que estos agentes logren tener un acceso a su información[392].

De esta manera, el problema reside en que ciertos datos pueden utilizarse para exponer al usuario a comportamientos discriminatorios, denigrantes e incluso peligrosos en determinados contextos. Así pues, si bien es cierto que el reglamento de IA hace referencia a la importancia de que "las personas físicas sean debidamente informadas y puedan decidir libremente no ser sometidas a la elaboración de perfiles u otras prácticas que puedan afectar a su conducta"[393], la elaboración de perfiles es, hoy en día, intrínseca a la utilización de la red, y, por lo tanto, no supone ninguna garantía de protección para el individuo ante los peligros mencionados[394].

Más allá de este tipo de respuestas sociales intencionadas, cabría considerar que las tecnologías de IA tienen un cierto margen de error. Por lo tanto, la toma de decisiones en base a los análisis de *Big data* presenta un cierto riesgo en la medida en que los resultados automatizados no siempre serán los correctos, pues si bien muchas correlaciones se establecen por *causalidad*, otras tantas se darán por *casualidad*[395].

3.5. Reflexiones sobre el capítulo 3

La actividad de los usuarios en la red lleva a la acumulación de sus datos mediante tecnologías *Big data*[396], que se valen de instrumentos como las *cookies* para recopilar información individualizada de cada usuario[397]; y, posteriormente utilizan herramientas de IA para crear una suerte de perfil del individuo[398], permitiendo recopilar e inferir todo tipo de información, tanto del propio usuario como de su círculo.

El uso de este tipo de tecnologías es inherentemente contrario al principio de minimización de datos[399]. No obstante, debe tenerse en cuenta que sus beneficios para la investigación, la economía y, en general, la innovación, son cuanto menos notables, y desaprovecharlos ralentizaría a la UE y la posicionaría en una situación muy desventajosa con respecto a otros actores internacionales[400]. Así pues, teniendo en cuenta que la prohibición de

[390] XENIDIS, R., *op. cit*., p. 749.
[391] Como los mencionados en el capítulo 1: secuestro de datos, denegación de servicio o suplantación de identidad, entre otros.
[392] GIL, E., *op. cit*., p. 118.
[393] Propuesta de Reglamento 2021/0106, *op. cit*., p. 15
[394] EBERS, M. et al., *op. cit.,* p. 594.
[395] GIL, E., *op. cit*., p. 33.
[396] *Ibidem*, p. 17.
[397] KUBICECK, K., *op. cit*., pp. 1-2.
[398] EBERS, M. et al., *op. cit.,* p. 594.
[399] GIL. E., *op. cit,* p. 52.
[400] European Data Protection Supervisor, *op. cit*., p. 7.

estas tecnologías es improbable, parece necesario estudiar la normativa para precisar ciertos aspectos.

Por un lado, es esencial incentivar una mayor concienciación de los usuarios[401]. En este sentido, es necesario mantener informados a los ciudadanos, e incluso plantear alguna reforma educativa que incluyera este tipo de cuestiones, ya que están absolutamente implantadas en la sociedad actual.

Por otro lado, el uso de *cookies*, que parece completamente irrelevante, parece estar insuficientemente regulado; el hecho de que no haya siquiera una categorización oficial dificulta la tarea de proporcionar la debida información al usuario para que este pueda tomar una decisión ajustada[402].

A este respecto, la reglamentación en transmisión de datos a terceros parece también demasiado laxa, y favorece más a las empresas que operan con estos datos que a los propios usuarios. Esto es especialmente notable con la legalización de *paywalls*, que, si bien son, en esencia, legítimas, deberían contar con una cierta regulación para evitar la imposición de cláusulas abusivas o de una *pseudo-obligación* de aceptar un tratamiento desproporcionado de los datos, siendo la alternativa el pago de tarifas excesivas[403].

Adicionalmente, es crucial que el usuario tenga conocimiento de las implicaciones de compartir sus datos, tanto al aceptar cookies como al brindar su consentimiento para el tratamiento de datos por parte de una empresa o de terceros[404].

Así pues, debe recalcarse el problema no es la proliferación de los mercados de datos, cuyos beneficios económicos y sociales son notables; sino que el peligro reside en el hecho de que (1) el usuario no es consciente de hasta qué punto sus datos están recogidos en innumerables bases de datos (2), teniendo esto en cuenta, no puede ejercer su derecho al olvido o a la rectificación y (3) dichos datos son más susceptibles de ser atacados o de ser utilizados de manera injusta y dañina, cuanto más extendidos, y por ende, más accesibles sean.

Por último, cabe resaltar que la protección de los datos *personales*[405] no parece ser suficiente para salvaguardar la privacidad del individuo, puesto que cualquier tipo de información, incluidos los datos considerados *no personales*[406], han demostrado poner en riesgo la privacidad y la intimidad de los ciudadanos[407]. En este sentido, podría considerarse la posibilidad de incluir la protección de todo tipo de datos en la regulación europea, en la medida en que cualquier dato puede hacer a una persona identificable; y, con ello, cabría incorporar, asimismo, ciertas técnicas de *anonimización* perfeccionadas.

[401] GIL, E. *op. cit*., p 143-144.
[402] KUBICECK, K., *op. cit*., p. 60.
[403] D'AMICO, *op. cit*., p. 18.
[404] European Data Protection Supervisor, 19 de diciembre de 2015, *op. cit*., p.4.
[405] Cursiva añadida
[406] Cursiva añadida
[407] NARAYANAN, A. & SHMATIKOV, V., *op. cit*., p. 11.

CONCLUSIONES

Tras haber realizado un análisis de las vulnerabilidades de la navegación en la red, la regulación existente para tratar de confrontarlas, y la efectividad de dicha legislación en un contexto práctico, parece más importante que nunca prestar atención a las diferentes conclusiones extraídas de este estudio, a saber:

Primera. La evolución de la tecnología ha transformado por completo la manera en la que nuestras relaciones sociales, laborales y comerciales funcionan. La regulación de esta actividad digital es sumamente compleja, dada su reciente creación y constante evolución; la falta de una jurisdicción clara, que delimite la competencia de cada Estado; y la multiplicidad de actores participantes en estas interacciones, cuya identidad no siempre es identificable. No obstante, se trata de una cuestión que atañe a todos aquellos que interactúan en la red – es decir, el mundo entero – y, por lo tanto, es necesario extender una concienciación general de la peligrosidad de esta nueva realidad digital, que sirva como incentivo para crear una normativa sólida, alineada con otras a nivel internacional.

Segunda. Las interacciones en la red se basan en el intercambio de datos, gestionados por compañías privadas. Por este motivo, la regulación vigente presta una atención especial a la actividad empresarial. En este sentido, cabe destacar que la transformación digital de las empresas ha llevado al desarrollo de un mercado de datos, cuyo valor en la economía mundial está en constante aumento, lo que ha fomentado a su vez el avance de nuevas tecnologías para el tratamiento masivo de datos, como las tecnologías *Big data*, o herramientas para su recopilación incesante, como las *cookies*.

Tercera. El ordenamiento jurídico de la Unión Europea, y así como el del Espacio Económico Europeo, es uno de los más robustos en materia ciberseguridad y transformación digital. Destaca su compromiso con el objetivo de transformación digital, pero siempre bajo la premisa de que esta digitalización sea accesible y garantice la protección del ciudadano, en línea con sus reconocidos derechos fundamentales y su privacidad, situándolos en el centro de la normativa en materia de protección de datos.

Cuarta. Si bien todas las disposiciones normativas desarrolladas por la Unión pretenden adquirir el estatus de reglamento – y no de directiva – con el fin de lograr una armonización interestatal en el plano europeo, es importante destacar que la aplicación de la legislación y la imposición de sanciones administrativas corresponde a las "autoridades de control" independientes de cada Estado, por lo que esta uniformidad es todavía relativa, y depende en gran medida de la colaboración entre tales autoridades.

Quinta. La legislación europea en protección del usuario en la red se desarrolla en torno al Reglamento General de Protección de Datos. Así, toda regulación adicional, sean reglamentos, directivas o directrices, debe tomar en consideración los principios básicos recogidos en el Reglamento 2016/679 (resumidos a grandes rasgos en: trato lícito, real y transparente; limitación de propósito; minimización de datos; exactitud y actualización; limitación temporal necesaria). Este patrón se puede identificar en las normativas estudiadas, a saber, la Directiva 2002/58/CE, la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, y el Reglamento de Inteligencia Artificial.

Sexta. Las regulaciones que hacen referencia a cuestiones de nuevas tecnologías encuentran grandes dificultades en su implementación, por dos motivos. Por un lado, la complejidad de dar con una definición clara, completa, inequívoca y uniforme de determinados conceptos esenciales para desarrollar el texto jurídico pertinente; así, el margen de

interpretación puede ser peligrosamente elevado, dando lugar a una normativa ineficaz. Por otro lado, la necesidad de conceder un periodo considerable para la propia implementación de la normativa, con el objetivo de permitir una adaptación a la nueva realidad tecnológico-jurídica; la problemática de este planteamiento es que, cuando por fin se adoptan las disposiciones de la regulación en su totalidad, pueden resultar obsoletas, dado el ininterrumpido avance tecnológico desarrollado en ese tiempo. Ambas dificultades pueden ser aplicables al Reglamento de Inteligencia Artificial.

Séptima. En línea con la *Tercera* conclusión, la superioridad del marco normativo del Espacio Económico Europeo con respecto a otras legislaciones se basa en una mayor preocupación por la seguridad del individuo. Esto puede verse reflejado en comparaciones con la normativa estadounidense respecto a la protección de datos personales, cuyo alcance es mucho más limitado, y, por lo tanto, la seguridad del individuo se ve manifiestamente mermada. Esto tiene un impacto directo en sus relaciones comerciales con otros Estados, en la medida en la que su actividad empresarial puede no estar permitida en el marco de la jurisdicción europea, pero sí en otros Estados.

Octava. A pesar de sus múltiples aspectos positivos, la regulación europea no está exenta de vulnerabilidades. Así, los intereses por el desarrollo económico, social y tecnológico son a menudo incompatibles con la legislación estudiada. En este sentido, el uso de tecnologías *Big data* resulta incompatible con el principio de minimización de datos, lo cual abre un debate sobre si debe priorizarse una por encima de otra, o si debe reformarse el texto normativo para dar cabida a nuevas tecnologías, sin por ello menoscabar los derechos del individuo.

Novena. La implementación de legislación carece prácticamente de utilidad, si no viene acompañada por una mayor consciencia del individuo. A este respecto, es especialmente destacable la aceptación indiscriminada de *cookies*, de términos y condiciones de uso de datos, o de transmisión de estos datos a terceros. Así, es tan importante desarrollar una regulación sólida, como incentivar al usuario a proteger sus datos personales, a través de la transmisión de información de forma más clara, sencilla e inteligible. Adicionalmente, la proliferación de *paywalls*, si bien legítimas, no constituye más que un nuevo elemento para desincentivar el interés del individuo, y debería desarrollarse cierta regulación adicional para evitar el establecimiento de precios descompensados.

Décima. El pensamiento generalizado es que los datos de un individuo común no son importantes, y nadie puede utilizarlos contra él, por lo que la única preocupación al utilizar Internet gira en torno a cuestiones económicas, tales como extracciones de su cuenta bancaria, o subidas de precios en productos o servicios de interés. Sin embargo, a través del tratamiento masivo de datos, se pueden elaborar perfiles completos de cada usuario que permiten reconocer rápidamente de su identidad, además de inferir información sensible, que incluye cuestiones como el estado de salud, la orientación sexual, la ideología política y las creencias religiosas. Todo ello puede convertir al individuo en un blanco fácil para manipulaciones, y, asimismo, puede acarrear consecuencias en situaciones como una preselección para conseguir un trabajo o incluso en una visita a un país donde la homosexualidad esté penada. Por lo tanto, es esencial tener conocimiento sobre la relevancia de la protección de datos, así como ser consciente de los potenciales peligros de la navegación inconsciente por la red.

BIBLIOGRAFÍA

Referencias académicas

ALONSO LECUIT Javier. "Privacidad, confidencialidad e interceptación de las comunicaciones". *Real Instituto Elcano*. ARI 92/2018, 24 de julio de 2018. Disponible en: <https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari92-2018-alonsolecuit-privacidad-confidencialidad-interceptacion-comunicaciones.pdf>

ARNAL, Judith & JORGE RICAT, Raquel. "Inteligencia artificial: el 'efecto Bruselas', en juego", *Real Instituto Elcano*, 3 de octubre del 2023. Disponible en: <https://www.realinstitutoelcano.org/analisis/inteligencia-artificial-parte-1-el-menor-efecto-bruselas/>

CANDO-SEGOVIA, M. R., y MEDINA-CHICAIZA, P. "Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica". *Cuadernos de desarrollo aplicados a las TIC*, 2021. <https://doi.org/10.17993/3ctic.2021.101.17-41>

CHHETRI, B. & KUJUR, P. "Evolution of World Wide Web: Journey From Web 1.0 to Web 4.0". *International Journal of Computer Science Trends and Technology*, junio-marzo 2015. Disponible en: <https://www.researchgate.net/publication/28094>

COLOMINA Carme et. al, "The World in 2024: ten issues that will shape the international agenda", *CIDOB notes internacionals*, ISSN 2013-4428, 2023.

D'AMICO, A. et al. "Meta's pay-or-okay model: an analysis under eu data protection, consumer and competition law". *Utrecht Centre for Regulation and Enforcement in Europe Working Papers*, 8 de abril de 2024. Disponible en: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4787609>

DANDAURA, S. & MBANSO, U. "The Cyberspace: Redifining a New World". *IOSR Journal of Computer Engineering*, mayo-junio 2015. Disponible en: <https://www.researchgate.net/publication/280101879_The_Cyberspace_Redefining_A_New_World>

EBERS, M. et al. "The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)". *J – Multidisciplinary Scientific Journal*, núm. 4, 8 de octubre de 2021. Disponible en: <https://www.mdpi.com/2571-8800/4/4/43>

FINNEMORE, M. & HOLLIS, D. "Constructing norms for global cybersecurity". *The American Journal of International Law*, vol. 110:425, 2016. Disponible en: <https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf>

GIL, E. "Big Data, privacidad y protección de datos". *Imprenta Nacional de la Agencia Estatal*. Boletín del Estado: Madrid, España, 2016. Disponible en: <https://www.aepd.es/sites/default/files/2019-10/big-data.pdf>

HOLLIS, B. D. "A Brief Primer On International Law and Cyberspace". *Carnegie Endowment for International Peace*. Junio, 2021. Disponible en: <https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763>

IMBROGNO, A. "Internet: camino hacia un derecho globalizado". *Cartapacio Universidad Nacional del Centro*, núm. 7, 2004. Disponible en: <https://dialnet.unirioja.es/ejemplar/393142>

KOBRIN, J. S. "Territoriality and the Governance of Cyberspace". *Journal of International Business Studies*, vol. 32, núm. 4, 2001. Disponible en <https://link.springer.com/article/10.1057/palgrave.jibs.8490990>

KRAUS, S. et al. "Digital Transformation: An Overview of the Current State of the Art of Research". *SAGE Open*, julio-septiembre 2021. Disponible en: <https://journals.sagepub.com/doi/full/10.1177/21582440211047576>

KRUSE, O. et al. "Digital Writing Technologies in Higher Education". *Springer Nature Switzerland AG*, Cham, Suiza: 2023. *Capítulo 4. Hypertexts, Hyperlinks, and the World Wide Web,* Disponible en: <https://link.springer.com/chapter/10.1007/978-3-031-36033-6_4>

KUBICECK, K. (2024). *Automated analysis and enforcement of consent compliance* [Tesis de doctorado, Universidad Masaryk]. Disponible en: <https://www.research-collection.ethz.ch/handle/20.500.11850/662039>

LEINER, B.M. et al. "A Brief History of the Internet". *Internet Society*, 1997. Disponible en: <https://doi.org/10.1145/1629607.1629613>

MATTLI, W. & WOODs. "The Politics of Global Regulation". *Capítulo 2. The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State*. Princeton University Press, New Jersey, 2009. Disponible en: <https://www.jstor.org/stable/j.ctt7rgmj>

MAZÓN CALPENA, C. & PEREIRA, P. (2000), "Las tecnologías de Internet y las empresas: riesgos y oportunidades". *Navarra y la sociedad del conocimiento: actas del congreso*, Gobierno de Navarra, 2000. Disponible en: <https://www.navarra.es/nr/rdonlyres/a9e2f1dc-194f-42ce-a9f5-c8af054d34ad/79802/cristina.pdf>

MISOLVE, A. et al. "You are who you know: inferring users profiles in online social networks". *Conferencia WSDM* 2010, 4-6 de febrero de 2010, Nueva York. Disponible en: <https://www.researchgate.net/publication/221520166_You_are_who_you_know_Inferring_user_profiles_in_online_social_networks>

MOREL, V. et al. "Your Consent Is Worth 75 Euros A Year – Measurement and Lawfulness of Cookie Paywalls". *Association for Computing Machinery*, 2022. Disponible en: <https://doi.org/10.1145/3559613.3563205>

MUELLER, M. L., "Ruling the Root. Internet governance and the taming of cyberspace". *MIT Press*, Cambridge, Massachussetts, 2002. Disponible en: <https://mitpress.mit.edu/9780262632980/ruling-the-root/>

NARAYANAN, A. & SHMATIKOV, V. "Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)". *Universidad de Texas*, 5 de febrero de 2008. Disponible en: <https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>

PÉREZ DE LAS HERAS Beatriz. "Hacia el Mercado Único Digital en la Unión Europea: retos y potencialidades para los entes subestatales", *Ekonomiaz,* núm. 98, 2020. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=7694315>

POPESCUL, D. "The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation", en Khalid S. Soliman (ed.) *Innovation and Knowledge Management: A Global Competitive Advantage* [Recurso electrónico]. Proceedings of The 16th International Business Information Management Association Conference. Kuala Lumpur, 29-30 junio 2011. Disponible en: <https://www.researchgate.net/publication/257985911_The_Confidentiality_-_Integrity_-_Accessibility_Triad_into_the_Knowledge_Security_A_Reassessment_from_the_Point_of_View_of_the_Knowledge_Contribution_to_Innovation>

RAYMOND, M. & DENARDIS, L. "Multi-stakeholderism: anatomy of an inchoate global institution". *International Theory*, 2015. Disponible en: <https://www.cambridge.org/core/journals/international-theory/article/multistakeholderism-anatomy-of-an-inchoate-global-institution/B69E6361B5965C98CFD400F75AA8DC53>

ROSELLÓ MALLOL, V. "Marketing y Protección de Datos (VI): comunicación de datos a terceros y encargo del tratamiento de datos. Transferencias internacionales de datos". *Noticias Jurídicas*. Disponible en: <https://noticias.juridicas.com/conocimiento/articulos-doctrinales/4516-marketing-y-proteccion-de-datos-vi:-comunicacion-de-datos-a-terceros-y-encargo-del-tratamiento-de-datos-transferencias-internacionales-de-datos-/>

SARTOR, G. "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence". *Scientific Foresight Unit (STOA).* Junio 2020. Disponible en: <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>

THEOHARY, C. *Defense Primer:* Cyberspace Operations. *Congressional Research Service*. Diciembre, 2023. Disponible en: <https://sgp.fas.org/crs/natsec/IF10537.pdf>

VERCELLI, A. "Facebook Inc. - Cambridge Analytica: (des)protección de datos personales y campañas globales de desinformación. Grupo de Investigación" *Ciencia, Tecnología, Universidad y Sociedad (CITEUS),* 2019. Disponible en: <https://sedici.unlp.edu.ar/handle/10915/135072>

WENSHENG GAN, V. et al. (2023). "Web 3.0: The Future of Internet". *In Companion Proceedings of the ACM Web Conference 2023 (WWW '23 Companion),* 30 abril - 4 mayo 2023. Disponible en: <https://doi.org/10.1145/3543873.3587583>

XENIDIS, R. "Tuning EU equality law to algorithmic discrimination: Three pathways to resilience". *Maastricht Journal of European and Comparative Law*. Vol. 27(6) 736–758. Disponible en: <https://doi.org/10.1177/1023263X20982173>

Textos normativos y otros documentos nacionales e internacionales

Agencia Española de Protección de Datos: 325/2004. "Comunicación de datos entre empresas de un mismo grupo", 28 de julio de 2004. Disponible en: <https://www.aepd.es/documento/2004-0325.pdf>

Anexos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021. COM (2021) 206. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206>

Article 29 Data Protection Working Party: "Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)". Adoptado el 19 de julio de 2006. Disponible en: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf>

Article 29 Data Protection Working Party. "Opinion 04/2012 on Cookie Consent Exemption". Adoptado el 7 de junio de 2012. Disponible en: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf>

Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), del 18 de diciembre del 2000. Disponible en: <https://www.europarl.europa.eu/charter/pdf/text_es.pdf>

Comisión Europea (11 de julio de 2023). *Hacia la próxima transición tecnológica: la Comisión presenta la estrategia de la UE para liderar la web 4.0 y los mundos virtuales* [Comunicado de prensa]. Disponible en https://ec.europa.eu/commission/presscorner/detail/es/ip_23_3718

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Plan coordinado sobre la inteligencia artificial*. Bruselas, 07.12.2018. COM (2018) 795. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=COM%3A2018%3A795%3AFIN>

Comunicación de la Comisión Europea 2020. *Una estrategia para un crecimiento inteligente, sostenible e integrador*. Bruselas, COM (2010) 2020 final, del 3.3.2010. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52010DC2020>

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, 28 de enero de 1981, Serie de Tratados Europeos núm. 108 del Consejo de Europa. Disponible en: <https://rm.coe.int/16806c1abd>

Council of the European Union. *EU Cyber Defence Policy, 15585/14*. Bruselas, 18 de noviembre, 2014. Disponible en: https://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/es/pdf

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) núm. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto

pertinente a efectos del EEE). *DOUE*, L 333/80, de 27 de diciembre de 2022. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022L2555>

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, *DOCE*, L 201/37, de 31 de julio de 2002. Disponible en: <https://eur-lex.europa.eu/eli/dir/2002/58/oj>

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 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, *DOCE*, L 281/31, de 23 de noviembre de 1995. Disponible en: <https://eur-lex.europa.eu/eli/dir/1995/46/oj>

European Data Protection Supervisor. "Opinion 7/2015 on Meeting the challenges of big data", del 19 de diciembre de 2015. Disponible en: <https://www.edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_en>

European Parliament resolution (2020/C 345/10) of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP)). Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018IP0433>

High-Level Expert Group on Artificial Intelligence, "A definition of AI: Main capabilities and scientific disciplines", *Directorate-General for Communication, European Commission*, 18 de diciembre de 2023. Disponible en: <https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf>

International Working Group on Data Protection in Telecommunications: 675.57.14, "Working Paper on Privacy and Artificial Intelligence", 64ª reunión, Nueva Zelanda, 29-30 de noviembre de 2018. Disponible en: <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/berlin-group/2018/2018-IWGDPT-Working_Paper_Artificial_Intelligence.pdf>

Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, *BOE*, núm. 294, de 06 de diciembre de 2018. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

Madiega, T. *Artificial intelligence act* [Legislative Briefing]. European Parliamentary Research Service, marzo, 2024. Disponible en: <https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI(2021)698792>

Propuesta de Reglamento 2017/0003 (COD) del Parlamento Europeo y del Consejo, de 10 de enero de 2017, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=LV>

Propuesta de Reglamento 2021/0106 (COD) del Parlamento Europeo y del Consejo, de 21 abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley

de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206>

Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023R2854>

Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo de 13 de marzo de 2024 sobre transparencia y segmentación en la publicidad política (Texto pertinente a efectos del EEE). Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R0900>

Reglamento (UE) núm. 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *DOUE*, L 119/46, de 4 de mayo de 2016. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679>

Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación (2020/2717(RSP)). Disponible en: <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_ES.html>

Versión consolidada del Tratado de Funcionamiento de la Unión Europea, del 26 de octubre de 2012. Disponible en: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:es:PDF>

Jurisprudencia

Asunto C-252/21. Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023 (petición de decisión prejudicial planteada por el Oberlandesgericht Düsseldorf — Alemania) — Meta Platforms Inc., anteriormente Facebook Inc., Meta Platforms Ireland Limited, anteriormente Facebook Ireland Ltd., Facebook Deutschland GmbH contra Bundeskartellamt, con intervención de Verbraucherzentrale Bundesverband e. V.

Recursos audiovisuales y sitios web

AMER, K. & NOUJAIM, J. (2019). El gran hackeo. [Documental]. Netflix.

CERN (s.f.). *A short history of the Web*. Disponible en: <https://home.cern/science/computing/birth-web/short-history-web>

Comisión Europea. *¿Qué son los datos personales?* Disponible en: <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es>

Comisión Europea. "Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI2)". *Configurar el futuro digital de Europa,* 14 de septiembre de 2023. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/nis2-directive>

Comisión Europea. "Ley de IA". *Configurar el futuro digital de Europa*, 2024. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai>

Comisión Europea. "Paquete de la Ley de Servicios Digitales". *Configurar el futuro digital de Europa*, 16 de febrero de 2024. Disponible en: <https://digital-strategy.ec.europa.eu/es/policies/digital-services-act-package>

Consejo Europeo & Consejo de la Unión Europea. *Un futuro digital para Europa.* 7 de febrero de 2024. Disponible en: <https://www.consilium.europa.eu/es/policies/a-digital-future-for-europe/>

European Commission. *Infographic - Top cyber threats in the EU*. Febrero, 2023. Disponible en : <https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/>

Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. Final Report: A study prepared for the European Commission DG Communications Networks, Content & Technology by Deloitte, 2017. Disponible en: <https://digital-strategy.ec.europa.eu/en/library/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector>

Fieldfisher [Fieldfisher Data & Privacy Team] (1 de febrero de 2024). *Debunking the EU AI Act: an overview of the new legal framework* [Video]. YouTube. Disponible en: <https://www.youtube.com/watch?v=iO0nfxxeYjE>

GÓRRIZ LÓPEZ, C. "Tratamiento de datos personales y defensa de la competencia (Meta Platforms Inc v Bundeskartellamt)". *Derecho y digitalización empresarial, UAB.* Disponible en <https://webs.uab.cat/derecho-y-digitalizacion-empresarial/2023/07/31/tratamiento-de-datos-personales-y-defensa-de-la-competencia-meta-platforms-inc-v-bundeskartellamt/>

North Atlantic Treaty Organization. *Cyber defence*. Septiembre, 2023. <https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=In%20July%202016%2C%20Allies%20reaffirmed,and%20consider%20possible%20collective%20responses.>

OECD/LEGAL/0449, "Recommendation of the Council on Artificial Intelligence", del 22 de mayo de 2019. Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText

Parlamento Europeo. "Una Agenda Digital para Europa". *Fichas temáticas sobre la Unión Europea*, 30 de noviembre de 2023. Disponible en: <https://www.europarl.europa.eu/factsheets/es/sheet/64/una-agenda-digital-para-europa>

SRI International. "75 years of innovation: Internetworking". *SRI International,* 19 noviembre 2020. Disponible en: <https://www.sri.com/press/story/75-years-of-innovation-internetworking/>

Statista. "Número de usuarios de Internet en el mundo entre 2005 hasta 2022", 2023. Disponible en: <https://es.statista.com/estadisticas/541434/numero-mundial-de-usuarios-de-internet/>

Unión Europea. *Tipos de legislación.* Disponible en: <https://european-union.europa.eu/institutions-law-budget/law/types-legislation_es>