Universidad de Valladolid

Facultad de **Derecho**

Grado en Derecho

Protección constitucional de la privacidad en internet

Presentado por:

Daniel Puertas Gonzalez

Tutelado por:

Dra. María Eugenia Hernández Peribáñez

Valladolid, 11 de Julio de 2023

ÍNDICE

RESUMEN

La hipótesis planteada en el presente trabajo es la respuesta jurídica a la necesidad de proteger la privacidad en el ámbito de internet. El internauta, en el uso cotidiano de la red, se expone a potenciales agresiones a su privacidad. La mayoría de la ciudadanía cree que las búsquedas que realiza en internet son gratis, pero, aunque no pagamos una contraprestación económica directa, si entregamos nuestros datos, cuyo tratamiento es un incipiente y cotizado mercado. Es necesario comprender cómo el usuario cede estos datos mientras navega por internet, manifestando su consentimiento a través de la aceptación de cookies, muchas veces sin conocer su contenido. La respuesta jurídica para proteger nuestra privacidad en internet se articula en varios niveles: el mandato original de nuestros constitucionalistas en el artículo 18.4 de la Constitución Española, las posteriores leyes orgánicas que lo han desarrollado y el conjunto de normas comunitarias en materia de protección de datos. Toda esta legislación tiene como objetivo salvaguardar la privacidad del usuario durante su navegación por internet.

PALABRAS CLAVE

Internet. Privacidad. Consentimiento. Cookies. Datos. Navegación. Riesgos. Proteger.

ABSTRACT

The hypothesis raised in this paper is the legal response to the need to protect privacy in the realm of the Internet. Internet users, in their daily use of the network, are exposed to potential violations of their privacy. The majority of citizens believe that the searches they perform on the Internet are free, but while we may not pay a direct economic counterpart, we do provide our data, which is a growing and valuable market. It is necessary to understand how users surrender this data while browsing the Internet, expressing their consent through the acceptance of cookies, often without knowing their content. The legal response to protect our privacy on the Internet is structured at various levels: the original mandate of our constitutionalists in Article 18.4 of the Constitution, the subsequent organic laws that have developed it, and the body of community regulations on data protection. All this legislation aims to safeguard the user's privacy while browsing the Internet.

KEY WORDS

Internet. Privacy. Consent. Cookies. Data. Risks. Browse. Protection

1. INTRODUCCIÓN

Nos guste o no, vivimos en un mundo digitalizado, donde internet se ha convertido en una herramienta omnipresente en nuestras vidas. Utilizamos internet para llevar a cabo una amplia gama de actividades diarias, desde buscar información y realizar compras hasta compartir detalles íntimos de nuestra vida a través de publicaciones en redes sociales. También recurrimos a ella para adquirir conocimientos mediante cursos online o para comunicarnos con otras personas a través de videoconferencias, entre otras muchas cosas. Sin embargo, en medio de toda esta interconexión, rara vez nos detenemos a considerar la importancia de proteger nuestra privacidad en línea.

Al tiempo que navegamos por Internet dejamos una huella digital. Cada acción que realizamos en la red contribuye a la formación de nuestro perfil digital, sin que nos percatemos de quien puede acceder a nuestros datos y con qué fines.

El objeto de este trabajo es analizar esta nueva realidad y examinar los desafíos jurídicos que plantea.

En primer lugar, es necesario comprender la dimensión de Internet y cuántos ciudadanos se ven afectados por este problema. A través de cifras y estadísticas, conoceremos el alcance de la digitalización en nuestro país.

En segundo lugar, definiremos la esfera de la privacidad y los términos afines, a fin de establecer una necesaria distinción entre ellos.

En tercer lugar, abordaremos la regulación existente que busca proteger nuestra privacidad en Internet. Para ello analizaremos nuestra Constitución, la evolución de las distintas leyes orgánicas de protección de datos que se han promulgado a lo largo del tiempo, así como el conjunto de normas comunitarias que regulan esta materia.

En cuarto lugar, una vez analizada y comprendida la normativa vigente, nos centraremos en los riesgos que conlleva la navegación en Internet para la privacidad del usuario. Examinaremos detalladamente las amenazas y los peligros a los que nos enfrentamos al compartir información, así como las implicaciones que esto tiene para nuestra vida cotidiana y nuestra capacidad de control sobre nuestros datos personales.

Por último, nos centramos en la jurisprudencia comunitaria en relación con la privacidad en Internet. Para ello, estudiaremos un caso emblemático en el que se aplicó el derecho al olvido en nuestro país, analizando su repercusión e implicaciones legales.

En definitiva, este trabajo tiene como objetivo analizar la realidad digital en la que vivimos, centrándonos en la importancia de proteger nuestra privacidad en Internet. A través de la exploración de la dimensión de Internet, la distinción de términos clave, el examen de la regulación existente, la identificación de riesgos y la revisión de la jurisprudencia, buscamos arrojar luz sobre esta cuestión fundamental en la sociedad actual.

2. PARADIGMA ACTUAL: LA SOCIEDAD DIGITAL

Algunos autores definen Internet como "la red de redes" y otros como "la autopista de la Información"[1]. Ofrecer un concepto sobre Internet es una tarea compleja, por ser una tecnología relativamente nueva y sobre todo en constante evolución, siguiendo a García Mexía "*Internet es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP*[2]*, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial".*

Podemos afirmar que hoy en día existe una disponibilidad de internet a nivel mundial y la diseminación de las Tecnologías de la Información y la Comunicación (TIC) a nivel universal permite que la interacción entre personas y corporaciones de distintos países sea algo sencillo y rápido. A consecuencia de esto actualmente nos encontramos ante un mundo virtual, un "ciberespacio"[3], un lugar sin entidad física que crece de manera imparable[4] y que alberga datos importantes de la vida de millones de personas.

Internet es un milagro tecnológico que nos permite posibilidades de comunicación jamás soñadas. Se constituye como un espacio virtual, una alternativa al mundo real, en

[1] GARCÍA MEXÍA, P., *El derecho de Internet*. Tirant lo Blanch, Valencia: 2005 pág. 99-101

[2] un protocolo de comunicación es el conjunto de reglas que especifican el intercambio de datos u ordenes durante la comunicación entre las entidades que forman internet.

[3] el ciberespacio es un término que proviene de las novelas de ciencia ficción y que define el espacio conceptual en donde palabras, relaciones humanas, datos, son manifestados empleando la tecnología de la comunicación a través de los ordenadores.

[4] En el año 2022 en España un total de 33,5 millones de usuarios según el INE [consulta en línea] https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout [último acceso: 10 jun. 2023]

el que los ciudadanos de todo el mundo realizan actividades comerciales, educacionales, de ocio y también en algunos casos ilícitas.

El acelerado avance de las nuevas tecnologías en los últimos tiempos, y más concretamente desde la irrupción de internet, ha propiciado un progreso sin precedentes que ha resultado en una profunda transformación de nuestra sociedad.

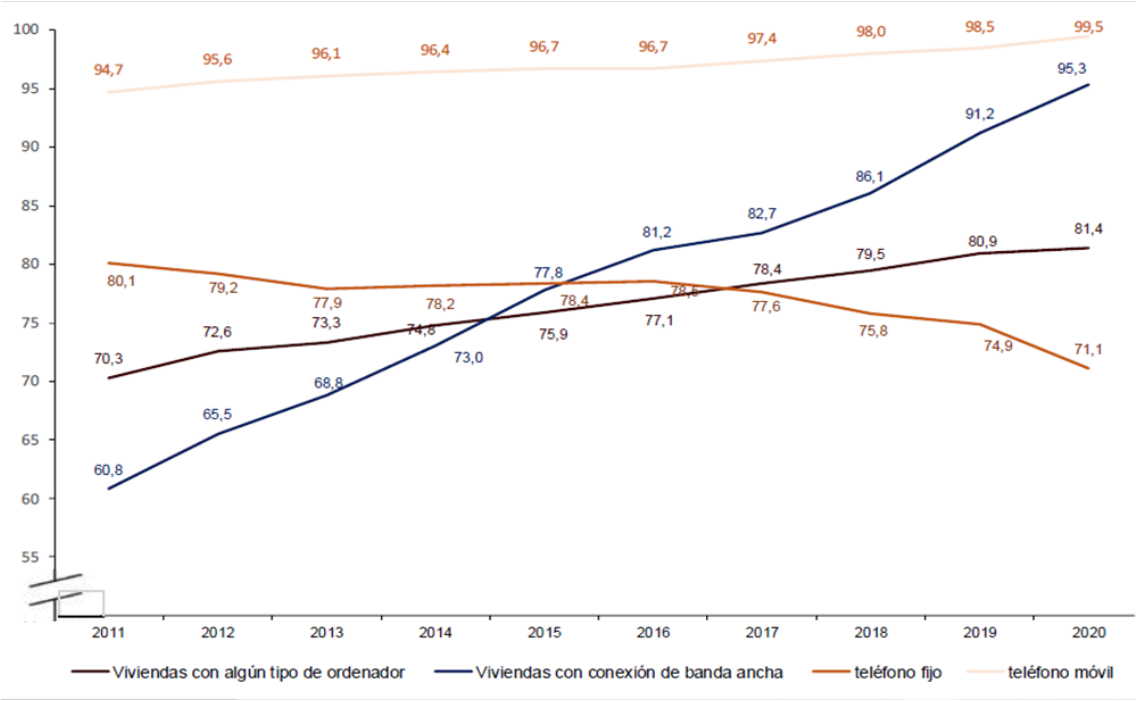
Estos profundos cambios sociales demandan una respuesta jurídica. Así pues, el derecho ha de dar una respuesta y regular esta nueva realidad ya que, como advierte Negroponte[5] *"(…) toda tecnología o dadiva de la ciencia posee su lado oscuro, y la vida digital no constituye una excepción".*

En la misma línea, Eric Schmidt, uno de los CEO de la empresa Google, hacía una advertencia que con el paso del tiempo cobra, cada vez, más relevancia al señalar que *"Internet es la primera cosa que la humanidad ha construido que la humanidad no entiende, el experimento más grande de anarquía que hemos tenido".*

Nunca en la historia de la humanidad tantas personas habían tenido acceso a una cantidad tan ingente de información, a un simple clic y a un coste relativamente accesible. Podemos hablar de una evolución imparable del uso de las TIC, como se muestra en los datos publicados en España por el Instituto Nacional de Estadística (INE) en el año 2022[6], donde se recoge que un total de 16,3 millones de hogares con al menos un miembro de 16 a 74 años (el 96,1% del total) disponen de acceso a Internet por banda ancha fija y/o móvil. En el siguiente gráfico de la misma fuente (INE) se aprecia la evolución que ha tenido el uso de las TIC en España en la última década donde se pone de manifiesto la practica universalidad en el uso de internet en el momento actual en España.

[5] NEGROPONTE, Nicholas. *El mundo digital.* Ediciones B, Barcelona: 1996. Pág. 39

[6] INE, Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los Hogares. Año 2022. [consulta en línea] https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608 [último acceso: 10 jun. 2023]



Respecto al consumo de internet por edad podemos constatar que su uso a diario está muy generalizado entre los jóvenes de 16 a 24 años (el 98,1% lo utiliza). Y va descendiendo conforme aumenta la edad. A partir de los 55 años se sitúa en el 80,0% y en el grupo de 65 a 74 años baja hasta el 59,9%. Los porcentajes de uso aumentan en todos los grupos de edad respecto a 2021. El mayor incremento se produce entre los de 65 a 74 años, podemos intuir que la brecha digital por edad va en descenso.

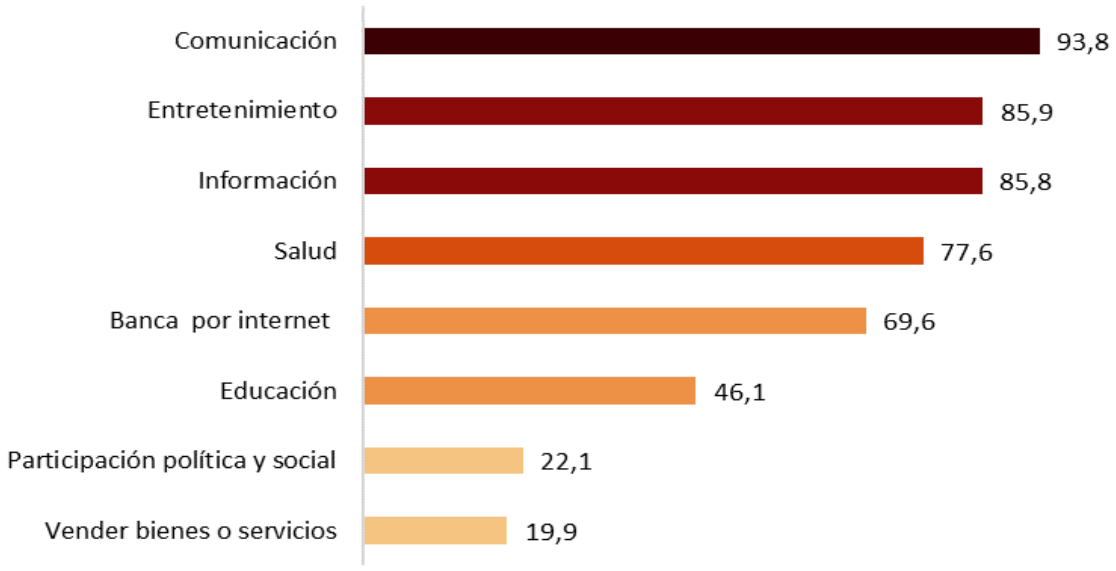
La revolución digital ha hecho posible una nueva forma de interacción social materializada a través de las redes sociales, concebidas como un espacio en el que la gente publica y comparte sus datos sociales, muchas veces personales y bastante íntimos, al tiempo que interacciona con los publicados por los demás. Es tal el uso de las redes sociales que en España hay 40,7 millones de usuarios[7], lo que supone un 87,1% de la población total. La penetración de las redes sociales entre los internautas españoles de 12 a 70 años es de un 88%, alcanzando el 93 % en el tramo de edad de 18 a 24 años. *WhatsApp, Facebook, Instagram, YouTube* y *Twitter* lideran el uso de Redes Sociales en España. *Instagram* (66%) y *TikTok* (25%) son las que más crecen el año 2022. El móvil

[7] IAB ESPAÑA, estudio de redes sociales 2022 [consulta en línea] https://iabspain.es/estudio/estudio-de-redes-sociales-2022/ [último acceso: 10 jun. 2023]

sigue siendo el principal dispositivo para conectarse a las redes sociales, seguido del PC y la Smart TV.

No podemos olvidar que la transición digital que lleva ya 30 años revolucionando sectores enteros (medios de comunicación, industrias culturales, turismo, comercio, logística, educación, salud, administración…) muchos de ellos encuadrados en la tipología de servicios al consumidor, también ha transformado los hábitos de consumo de la mayoría de los ciudadanos del mundo.

Es significativo conocer los datos que publica el INE respecto a la distribución de actividades realizadas por internet entre la población española de 16 a 74 años (véase en el siguiente gráfico[8]).



La llegada de internet no solo ha transformado nuestra forma de relacionarnos si no también nuestro consumo y en consecuencia nuestra economía. En España casi 19,6 millones de personas, el 55,3% de la población ha comprado por internet en los últimos meses. El gasto medio que estima el INE por comprador en 2022 alcanza los 282.8 euros (frente a 273,8 euros en 2021), reflejando una tendencia al alta mantenida en los últimos años.

[8] INE. op. cit.

Los datos estadísticos mostrados nos sirven para constatar cómo el ser humano ha cambiado sus hábitos y costumbres en estos últimos años. La pandemia del covid-19 ha supuesto un punto de inflexión en el proceso de transformación digital de nuestra sociedad, ha propiciado un acelerón de la digitalización en la esfera pública y privada. En mayor o menor medida, durante el confinamiento, una gran parte de los ciudadanos ha recurrido de forma masiva a las redes sociales, al consumo online de bienes y servicios, pero también durante la pandemia se modificó de forma acelerada el modelo tradicional de trabajo presencial propiciando así un aumento sin precedentes del número de empleados teletrabajando en España. En definitiva, la pandemia ha empujado a la digitalización a poblaciones que anteriormente eran menos activas en la red, muchos mayores se han iniciado en las videollamadas, se han integrado en los grupos de WhatsApp y ya no temen a la compra online. Por su parte, muchos negocios y también las Administraciones han acelerado su digitalización en todos los sentidos. Hemos comprobado que todo lo que antes se hacía de forma física, puede tener ahora su versión digital.

La posibilidad de comunicación que nos ofrece el mundo digital nos permite obtener información instantánea de cuanto ocurre en nuestro mundo, interactuar con un número creciente de personas, aprender, enseñar, disponer de todo tipo de productos y servicios y de nuevas oportunidades de negocios, de trabajo y de relaciones.

Por tanto, no se puede concebir la sociedad actual sin la presencia de internet. Su impacto es de tal magnitud, que tal como sostiene Jeffrey D. Sach[9], "la creación de internet ha supuesto el fin de la edad contemporánea y el inicio de una nueva edad digital, en la que todos estamos interconectados de manera instantánea y permanente".

Así mismo, las tecnologías digitales están impactando en cómo se ejercen, protegen y vulneran derechos fundamentales como el derecho a la intimidad, la libertad de expresión y el acceso a la información. Por este motivo, cobran especial relevancia una nueva serie de Derechos Digitales que protegen al usuario de estas nuevas tecnologías y que garantizan el derecho de los ciudadanos a la tutela de su intimidad y la protección de sus datos.

[9] JEFFREY D. Sach, *las edades de la globalización*, DEUSTO S.A. ediciones, Bilbao, 2021.

Precisamente, el foco de este trabajo va a recaer en el estudio de la protección de la privacidad en internet. Para ello, y como punto de partida vamos a distinguir dos conceptos: intimidad y privacidad, que frecuentemente se usan como sinónimos pero que en realidad no lo son, tal como examinaremos seguidamente.

3. LA NECESARIA DISTINCIÓN ENTRE INTIMIDAD Y PRIVACIDAD

Antes de avanzar en el tema de la protección de la privacidad en internet hemos de delimitar el contenido de la privacidad y distinguirlo de vocablos que en la práctica jurídica se utilizan como sinónimos de este derecho fundamental de primera generación. El propio legislador utiliza privacidad e intimidad indistintamente como si se tratasen de sinónimos. Sin embargo, debemos tener presente que no significan lo mismo, aunque guarden una conexión, tal como veremos a continuación.

Lo primero que hemos de tener en cuenta es que el contenido de los conceptos intimidad y privacidad son cambiantes y heterogéneos. Son cambiantes porque se ven afectados por el devenir histórico, el paso del tiempo cambia usos y costumbres sociales y lo que ayer se concebía como íntimo hoy quizás ya no lo sea, y viceversa. Son heterogéneos porque no tenemos el mismo concepto de privacidad en todo el mundo, lo que entendemos por privado en nuestra cultura occidental puede no serlo en otro lugar, en un mundo con tal heterogeneidad cultural como es el nuestro se antoja imposible delimitar un contenido universal de lo que entendemos por privacidad. Lo que percibimos como privacidad e intimidad se ve marcado, en definitiva, por el lugar y momento en que nos encontremos.

Existe un gran debate doctrinal sobre si el termino intimidad es sinónimo de privacidad. En la legislación española no se advierten diferencias y son utilizados indistintamente. Por su parte, los tribunales parecen usar ambos términos como si de sinónimos se tratasen. Sirva de ejemplo el Auto 642/86 del Tribunal Constitucional[10], que en su fundamento jurídico tercero dice que:

[10] ATC 23/86, de 23 de julio de 1986. ECLI:ES:TC:1986: 642ª. [consulta en línea] https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/10662 [último acceso: 10 jun. 2023]

> "el derecho a la intimidad constitucionalmente garantizado por el art. 18 en relación con un área espacial o funcional de la persona precisamente en favor de salvaguardar su privacidad, que ha de quedar inmune a las agresiones exteriores…".

Constatamos, por tanto, que ni la norma ni su interpretación jurisprudencial arrojan luz sobre la diferencia entre estos dos términos. Nos resta, pues, el recurso etimológico y las definiciones que dan los lingüistas para dilucidar qué es privado y qué es íntimo.

El Diccionario de la Lengua Española[11] (DLE en adelante) define la privacidad como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". Respecto a los adjetivos derivados del vocablo privacidad el DLE dice: "que se ejecuta a vista de pocos, familiar o domésticamente, sin formalidad ni ceremonia alguna", "particular y personal de cada individuo" y "que no es propiedad pública o estatal, si no que pertenece a particulares". De estas acepciones podemos deducir que la privacidad es un espacio en el que todo ser humano disfruta del derecho a no ser perturbado por otros, a que nadie se entrometa en su ámbito. Otro matiz que se desprende de estas definiciones es la contraposición de lo privado con lo público, el término "privado" se origina del latín *privatus* que significa privar y está íntimamente relacionado con la propiedad, así pues, decimos que esto es una propiedad privada o algo de uso privado para señalar que es lo contrario a público. Por lo tanto, la privacidad se refiere a un ámbito, a un espacio o a la propiedad sobre algo que se disfruta protegido frente a las intromisiones de terceros.

Por otra parte, el DLE define intimidad como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia". La intimidad es el conjunto de pensamientos y sentimientos mejor guardados en el interior de la persona, tales como su religión, ideología o su orientación sexual. Lo íntimo es un adjetivo que deriva del latín *intimus* y que alude a lo que está en el fondo de algo, a lo recóndito. Por lo tanto, la intimidad hace referencia a la zona espiritual que queremos preservar de los demás y que únicamente confiamos a nosotros mismos y a quienes elegimos.

[11] *Diccionario de la Lengua Española* (DLE) [consulta en línea] 23ªed., 2014 https://dle.rae.es/ [último acceso: 10 jun. 2023]

Hemos de advertir que el DLE es un diccionario descriptivo y no normativo por lo que sigue habiendo un debate doctrinal entre los juristas acerca de si dichos vocablos son sinónimos o no lo son, tal y como se desprende de las definiciones anteriormente expuestas. Hay autores, como Tornabene I., que consideran que el término privacidad debe ser rechazado por tratarse de una traducción del inglés *privacy* y defienden que en su lugar se empleen términos como intimidad o vida privada. Defiende la citada autora que el termino *privacy* utilizado en EE. UU. no puede equipararse con la concepción de la intimidad que tenemos en Europa que tiene un carácter más restringido. No obstante, Tornabene sostiene que el termino privacidad es un neologismo aceptado en los diferentes países de habla hispana y por tanto se aprecia necesaria una distinción entre ambos conceptos (intimidad y privacidad) que estima que es cuestión de una relación género- especie ya que la intimidad pertenece al ámbito de la privacidad porque todo lo íntimo es privado en cambio no toda la información privada es información íntima[12].

En esta línea argumental podemos centrar las diferencias entre ambos conceptos sosteniendo que mientras la intimidad tiene un alcance más restringido, hace referencia a la zona íntima y reservada: el domicilio, las creencias religiosas, las afinidades políticas, las preferencias sexuales, etc. Su protección legal se canaliza a través de los tres primeros párrafos del artículo 18 de la Constitución y de las normas que los desarrollan en aspectos tales como el derecho al honor, a la intimidad personal y la propia imagen, la inviolabilidad de las comunicaciones, etc.

La privacidad, por su parte, tiene un sentido más amplio y de mayor alcance**.** Afecta a aspectos de la persona que de forma aislada pueden no tener excesiva relevancia (hobbies, gustos musicales, libros preferidos, películas más vistas, etc.) pero que tomados en su conjunto arrojan un perfil completo del individuo en cuanto a gustos, aficiones, preocupaciones o necesidades, que, sin lugar a duda, también merecen protección. En este punto los medios de comunicación, la tecnología y la informática permiten cruzar datos y mantenerlos en el tiempo, por lo que se hace necesaria una

[12] TORNABENE, I., "privacidad e intimidad: la protección legal de la información personal en la República Argentina", en Amoroso Fernández, Y., (dir.), *Género, Código de Juventud: construir sociedades mas justas e inclusivas,* Unión Nacional de Juristas de Cuba, 2014 p. 87.

limitación y reglamentación de su uso. A este concreto aspecto, atiende la legislación en materia de tratamiento de información personal y protección de datos**.**

La primera Ley Orgánica que limitó el uso de la informática obedeciendo el mandato constitucional contenido en el artículo 18.4 CE fue la actualmente derogada Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Esta norma diferenciaba claramente entre privacidad e intimidad. Concretamente, en el apartado primero de su exposición de motivos se habla de la privacidad y no de la intimidad:

> "Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado" [13].

En resumen, la intimidad se refiere a la zona más reservada de la persona (creencias religiosas, orientación sexual, etc.) mientras que la privacidad abarca aspectos más amplios de la vida de una persona que, si bien individualmente no son de gran interés, si los tomamos en conjunto pueden reflejar los gustos y necesidades de una persona. Por lo que podemos concluir que todos los asuntos íntimos son privados, pero no todos los asuntos privados son íntimos.

Tanto el derecho a la intimidad como a la privacidad se erigen para proteger información personal. Por ello, es necesario conocer el régimen que ha previsto el legislador para el tratamiento de dicha información en internet. El derecho no ha quedado al margen de esta nueva realidad y ya desde la redacción original de nuestra Carta Magna, se previó la amenaza a la privacidad que en aquel entonces podía suponer el uso de la informática, y que hoy en día se ha materializado en la utilización de internet, el almacenamiento de

[13] Agencia Estatal Boletín Oficial del Estado*, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*. [disponible en línea] https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189 [último acceso: 10 jun. 2023]

datos del usuario y la necesidad de poner límites jurídicos a dicho almacenamiento. Así pues, debemos comenzar examinando tanto el mandato contenido en la CE como el desarrollo legislativo que del mismo se ha llevado a cabo.

4. DESARROLLO LEGAL Y JURISPRUDENCIAL DE LA PROTECCIÓN DE LA PRIVACIDAD EN INTERNET

4.1 Protección constitucional: El artículo 18 CE

El mandato contenido en el 18.4 CE en su momento fue pionero. Nuestros constituyentes como ya hicieron los portugueses dos años antes se mostraban preocupados por como una tecnología incipiente, internet, podría afectar a nuestra privacidad. En los años en los que se redacta nuestra Carta magna el uso de la informática no era algo tan generalizado como actualmente. Pese a ello nuestros constituyentes anticiparon el peligro que supone el archivo y uso de los datos informáticos y previeron como el tráfico ilícito de datos podría ser una amenaza a la intimidad como posteriormente se ha confirmado en los casos de vigilancia masiva.

Hemos de tener presente que, aunque esté ligado con el derecho a la intimidad y la libertad ideológica estamos ante un derecho autónomo, un derecho fundamental a la protección de datos que garantiza al ciudadano el control sobre sus datos y su uso y destino. De esta forma el individuo podrá oponerse a que sus datos se usen para fines distintos de los que legitimaron su obtención. Por lo tanto, este derecho fundamental protege el tráfico ilícito o lesivo para la dignidad de los datos informáticos sensibles (relativos a ideología, creencias, orientación sexual) y también de aquellos que se usan para fin distinto del que fueron recabados. El TC, a través de su jurisprudencia, ha reconocido la existencia de un derecho fundamental autónomo a la protección de datos personales:

"Estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la

persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama la informática" [14].

Además, el TC en su Sentencia de 30 de noviembre de 2000, ha fijado el contenido mínimo de este derecho

> "El derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos"[15].

En definitiva, el derecho fundamental a la protección de datos persigue garantizar a la persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado[16].

La regulación del derecho a la protección de datos se articula a través de un marco normativo multinivel en el que, como analizaremos a continuación, interaccionan normas internacionales, europeas y nacionales.

4.2 Evolución de las distintas leyes orgánicas de protección de datos

La primera ley española que da cumplimiento al mandato del 18.4 CE y a las obligaciones contraídas por España tras la ratificación del Convenio 108 del Consejo de Europa[17] fue la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de

[14] Véase STC 254/93, de 20 de julio ECLI:ES:TC:1993:254 [consulta en línea] https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383 [último acceso: 10 jun. 2023]

[15] Véase STC 290/2000, de 30 de noviembre ECLI:ES:TC:2000:290 [consulta en línea] https://hj.tribunalconstitucional.es/HJ/es-ES/Resolucion/Show/SENTENCIA/2000/290 [último acceso: 10 jun. 2023]

[16] En este sentido véase STC 292/2000, de 30 de noviembre ECLI:ES:TC:2000:292 [consulta en línea] https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276 [último acceso: 10 jun. 2023]

[17] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 [consulta en línea] https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447 [último acceso: 10 jun. 2023]

Carácter Personal (LORTAD[18]). Con el Convenio 108, los Estados miembros del Consejo de Europa tomaron en cuenta la intensificación de la circulación a través de las fronteras de los datos personales y la necesidad de conciliar el respeto a la privacidad y la libre circulación de estos. El objetivo y la finalidad de este convenio, tal y como señala el artículo 1, es garantizar, en el territorio de la Unión, a cualquier persona física el respeto a sus derechos y libertades fundamentales, específicamente, su derecho a la vida privada con relación a la protección de sus datos de carácter personal.

La incorporación de la Directiva 95/46/CE[19] al ordenamiento jurídico español supuso un cambio en la regulación del tratamiento de los datos de carácter personal. El título de la misma "Directiva relativa a protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" resulta en si mismo revelador. Tomando como base la libertad de circulación del mercado interior, la directiva buscaba la eliminación de cualquier obstáculo que impidiera dicho fin. Por lo que, el flujo transfronterizo de datos personales debía ser regulado de forma coherente y homogénea para no obstaculizar la libre circulación de estos.

En definitiva, la protección de datos debe servir a un fin principal: preservar el correcto funcionamiento del mercado interior de la Unión Europea. La adecuación normativa de esta Directiva se materializo en nuestro país a través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD[20]).

La Directiva 95/46/CE había demostrado un éxito sin precedentes generalizando un sistema común de protección de datos en el conjunto de los Estados miembros. Pero a su vez, adolecía de las limitaciones inherentes a su naturaleza, ya que pese a su vocación armonizadora no impidió notables divergencias entre las legislaciones nacionales, que provocaban disfunciones en el mercado interior y en la garantía uniforme de la protección de datos. La deficiente transposición de la directiva puso de manifiesto que

[18] LORTAD [Consulta en línea] https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189 [último acceso: 10 jun. 2023]

[19] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos [en línea] https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678 [último acceso: 10 jun. 2023]

[20] LOPD [Consulta en línea] https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750 [último acceso: 10 jun. 2023]

el instrumento jurídico idóneo para lograr la homogeneidad, dado su alcance general y su aplicabilidad directa, era el reglamento.

El Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD[21]) junto con La Ley Orgánica 2/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD[22]) ponen fin al proceso legislativo del derecho a la protección de datos y alumbran el nuevo marco normativo, derogando la Directiva 95/46/CE y la LOPD.

En este nuevo marco, que podemos calificar de multinivel, interaccionan normas europeas y nacionales configurando un nuevo derecho de protección de datos. Con base en el derecho consagrado en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea[23] (CDFUE) el legislador pretende homogeneizar la legislación de los Estados miembros. Así el RGPD, de aplicación directa, garantiza la subsidiariedad legislativa de los Estados miembros, pero mantiene instrumentos supranacionales de coordinación con el fin de lograr esa libre circulación de datos, ya que las diferencias entre los niveles de protección de la intimidad podrían constituir un obstáculo para las actividades económicas a escala comunitaria. Por lo que podemos afirmar que el nuevo modelo de protección de datos, sustentado en un RGPD de alcance general y aplicación directa sin necesidad de medidas de incorporación al derecho nacional, es un modelo esencialmente comunitario en detrimento del activismo legislativo nacional. En consecuencia, el derecho de protección de datos queda garantizado por el RGPD y protegido por la jurisdicción europea sin que las instituciones legislativas nacionales puedan modificar este derecho europeo. Teniendo en cuenta esto el margen del legislador nacional es, aparentemente, mínimo. Los 99 artículos y los 174 considerandos del RGPD conforman un marco normativo bastante exhaustivo, por lo que podemos afirmar que es el RGPD y no la ley orgánica la norma llamada a desarrollar el derecho

[21] RGPD [Consulta en línea] https://www.boe.es/doue/2016/119/L00001-00088.pdf [último acceso: 10 jun. 2023]

[22] LOPDGDD [Consulta en línea] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673 [último acceso: 10 jun. 2023]

[23] CDFUE [consulta en línea] https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003 [último acceso: 10 jun. 2023]

fundamental de protección de datos contenido en el mandato del 18.4 CE y consagrado en el artículo 8 de la CDFUE. El legislador nacional debe limitarse a adoptar las previsiones a las que obligue el RGPD para su aplicación y adaptarlo a las tradiciones jurídicas propias, teniendo siempre en cuenta el objetivo final: fortalecer la seguridad jurídica y la vocación de uniformidad de la protección de datos en toda la UE.

Teniendo en cuenta la evolución legislativa anteriormente expuesta, podemos concluir que el marco normativo de protección de datos es el resultado de una construcción vertical. Operada en origen por instrumentos internacionales como el Convenio 108 del Consejo de Europa de 1981 o las directrices de la OCDE de 1980. En las últimas décadas, este marco legislativo ha sido conformado por la legislación comunitaria a través de la Directiva 95/46 y posteriormente con el fin de homogeneizar la protección de datos en todos los países miembros por el RGPD. Este reglamento ha devaluado la posición del legislador orgánico, que ha quedado relegada a garantizar la aplicabilidad de este, complementándolo y adaptándolo a la tradición jurídica de cada país, en el caso de España a través de la LOPDGDD.

4.3 El derecho fundamental a la protección de datos: contenido

Una vez analizada la regulación, podemos concluir que, actualmente, el derecho fundamental a la protección de datos se encuentra protegido en instrumentos nacionales, comunitarios e internacionales. Los preceptos mas relevantes que recogen este derecho son: el artículo 18.4 de la Constitución (CE), el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE[24]) y el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE[25]). El RGPD y la LOPDGDD pretenden dar

[24] Artículo 8 Protección de datos de carácter personal:
1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

[25] Artículo 16 Tratado de Funcionamiento de la Unión Europea:
1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros

respuesta a las constantes amenazas a nuestra privacidad que suponen los constantes avances tecnológicos y en concreto el Internet.

Debemos conocer el contenido de esta normativa para saber cómo se configura actualmente la protección de datos a través de la autodeterminación informativa y como la jurisprudencia ha venido desarrollando este concepto.

Por lo tanto, debemos analizar como se refleja este derecho en la práctica, como operan estas herramientas jurídicas a la hora de proteger nuestros datos, pasar de un marco teórico de protección de datos a un marco práctico para ver que datos son los que se protegen y como se refleja el consentimiento del titular en dicha protección.

A la hora de realizar dicho análisis nos hemos de fijar en la evolución de la protección de datos en nuestro país. Conocer como a través de la interpretación de nuestro Alto Tribunal se ha creado un derecho fundamental autónomo y se le ha dotado de contenido propio. Por último, estudiaremos cómo afecta el consentimiento del titular en materia de protección de datos.

4.3.1. Evolución de la protección de datos en nuestra jurisprudencia

Como ya hemos mencionado, en la redacción originaria de la Constitución ya se contemplo el potencial riesgo que tendría la informática sobre nuestra privacidad en el artículo 18.4[26].

Sin embargo, este artículo 18 no definió que se entendía por intimidad ni tampoco lo hizo la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[27]. De manera que fue el TC quien definió el concepto de intimidad, otorgándole una doble vertiente. Distinguiendo un

en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos.
El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

[26] "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos." art. 18.4 CE.

[27] Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen39. [consulta en línea] https://boe.es/buscar/act.php?id=BOE-A-1982-11196 [último acceso: 10 jun. 2023]

primer ámbito objetivo de intimidad[28](se incluyen aquí: la intimidad corporal, orientación e identidad sexual, estado de salud, filiación, etc.).

Y un ámbito subjetivo de la intimidad, que fue configurada en el denominado caso Sara Montiel, donde el TC señalo que:

> "*el art. 18 de la CE no garantiza una intimidad determinada sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicación de la información relativa a su persona y a su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público"* [29].

Esta vertiente subjetiva de la intimidad es relevante de cara a comprender la importancia del consentimiento. El interesado tiene un poder de control sobre los datos que desea compartir y los que no, de manera que el titular tiene la libertad de decidir lo que considera íntimo y lo que desea hacer público.

En lo que nos ocupa, que es la protección de datos, inicialmente[30] el TC consideraba la protección de datos como una especificación del derecho de intimidad del art. 18.1 CE. Posteriormente en el año 1993[31] lo califica como un derecho fundamental autónomo con base en el artículo 18.4 CE e introduce el concepto de libertad informática. Así pues, el TC expresó en su doctrina que el derecho a la protección de datos y la libertad informática:

> "*no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, (...) sino que, además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad-, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos"* [32] .

---

[28] En la construcción de este ámbito objetivo, destacamos las SSTC:
STC 37/1988, de 15 de febrero, FJ 7º.
STC 89/1987, de 3 de junio, FJ 2º.
STC 99/2019, de 18 de julio de 2019, FJ 4º.

[29] STC 134/1999, de 15 de julio, FJ 5º.

[30] LUCAS MURILLO DE LA CUEVA, P. (2003). *La primera jurisprudencia sobre el derecho a la autodeterminación informativa.* Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, n.º 1.

[31] STC 254/1993, de 20 de julio.

[32] STC 11/1998, de 13 de enero, FJ 5º, y STC 94/1998, de 4 de mayo, FJ 4º.

En el año 2000, el TC[33] reitera que el derecho a la protección de datos es un derecho autónomo dotándole de un contenido esencial, que a parte de proteger datos íntimos también protege los que no lo son, sino solamente quedarían amparados por el derecho a la protección de datos aquellos datos de carácter personal que tuviesen una estrecha relación con la intimidad y vida personal quedando excluidos los que no tuvieran esa relación.

Podemos, por tanto, diferenciar un derecho fundamental a la intimidad y un derecho fundamental a la protección de datos. El derecho a la intimidad se concreta en la práctica en un deber de abstención por parte de las autoridades y del resto de ciudadanos, la función de este derecho es proteger de intromisiones de terceros no deseadas en nuestra vida personal y familiar. En cambio, el derecho a la protección de datos personales se configura como un deber de prestación, el Estado debe dar a las personas las herramientas necesarias para poder ejercer la facultad de control sobre sus datos personales, por lo tanto, impone una conducta activa.

Aunque la protección de datos sea un derecho autónomo no puede ni debe separarse del derecho a la intimidad, por eso ambos se regulan en el artículo 18 CE. Esto se debe a que ambos tienen en común que quieren proteger datos que sirvan para identificar a una persona. Es decir, la información, el dato en si mismo tomándolo de manera aislada no afecta a la intimidad, pero cuando se relaciona este con una persona, se utiliza para identificar a una persona, ahí si entra en juego la intimidad. Por ejemplo, en este sentido se ha pronunciado la jurisprudencia del Tribunal Superior de Justicia de Madrid[34], anulando un despido disciplinario basado en unos incumplimientos apoyados en la localización y seguimiento de un trabajador. Este despido fue anulado porque vulneraba el derecho fundamental a la protección de datos y al mismo tiempo el derecho a la intimidad personal. Sirva esta sentencia para observar como en nuestro ordenamiento jurídico, si bien estamos ante dos derechos fundamentales autónomos, estos están

[33] STC 292/2000, de 30 de noviembre, FJ 5º.

[34] STSJ Madrid 739/2014, de 29 de septiembre, rec. n.º 1993/2013, FFJJ 3º, 4º y 5º. «[...] todos los datos que se refieren a su utilización, localización y desplazamientos [...] [permiten] conocer en todo momento durante su uso determinadas parcelas de la vida de la misma por muy relacionadas [...] que inciden en la esfera de su derecho a la intimidad personal, asistiéndole el derecho de protección de datos de tal carácter».

íntimamente relacionados, y que existen datos, como el de localización, que vulneran ambos derechos.

4.3.2. La libertad informática, autodeterminación informática y protección de datos

Analizando la jurisprudencia del TC que ha ido caracterizando el derecho de protección de datos como un derecho fundamental autónomo hemos mencionado el término "libertad informática" (empleado por primera vez en 1993[35]). La conjunción de ambos consiste en el derecho del ciudadano a:

> "*controlar el uso de los mismos datos insertos en un programa informático (habeas data) y que comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención*" [36].

Tal y como señala el TC el fin que persigue el derecho a la protección de datos es:

> "*garantizar a la persona un poder de disposición sobre el uso y destino de sus datos con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, garantizando a los individuos un poder de disposición sobre esos datos"* [37].

De manera que el derecho a la protección de datos confiere a su titular un poder de disposición sobre sus datos personales. Esta concepción se asemeja a lo que la jurisprudencia del Tribunal Constitucional Federal Alemán denominó en 1983[38] "derecho a la autodeterminación informativa" [39], como el derecho que tiene el titular a controlar sus datos.

Debemos tener en cuenta que el derecho a la protección de datos se ha europeizado, no solo hemos de centrarnos en el artículo 18.4 CE si no también en el derecho comunitario; el artículo 8 de la CDFUE y el artículo 16 del TFUE. Como ya se ha mencionado en este trabajo, actualmente la normativa en esta materia tiene origen

[35] STC 254/1993, de 20 de julio
[36] STC 96/2012, de 7 de mayo, FJ 6º
[37] STC 17/2013, de 31 de enero, FJ 4º.
[38] *Bundesverfassungsgericht* (*BVerfG*), sentencia de 15 de diciembre de 1983 sobre la Ley del Censo y de Población, BVerfGE 65, 1; 1 BvR 209/83; *Gründe*, C, II (ap. n.º 147).
[39] "*Recht auf informationelle Selbstbestimmung*", en alemán.

mayoritario en la Unión, dejando poco margen al legislador nacional que se limita a regular especialidades en su ámbito.

4.3.3. ¿Qué son los datos personales?

La respuesta a esta pregunta se encuentra en la regulación que ha desarrollado la protección de datos, desde la Directiva 95/46/CE de 24 de octubre de 1995, hasta el actual RGPD.

La Directiva 95/46/CE y la LOPD que la traspuso, definieron los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables"[40]. El RLOPD amplio la definición "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"[41].

De las definiciones anteriormente expuestas se nos plantea la duda de que diferencia hay entre una persona física "identificada" o "identificable". Pues bien, la mencionada Directiva[42] estableció que "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social". Por lo tanto, es identificada cuando la información indica directamente la identidad de una persona (DNI, pasaporte, etc.). En cambio, será identificable cuando su identidad pueda determinarse mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social, es decir, cuando la información no indique la identidad directamente, pero si sea un aporte suficiente para poder averiguarla (huella dactilar, ADN, dentadura, iris del ojo, etc.).

El RGPD sigue estas definiciones anteriores y dice que serán datos personales "toda información sobre una persona física identificada o identificable. Información que será cualquiera que sea numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo"[43].

[40] Art. 3, apartado a), de la LOPD y art. 2, letra a), de la Directiva 95/46/CE.
[41] Art. 5.1, apartado f), del RLOPD.
[42] Directiva 95/46/CE en su artículo 2, apartado a).
[43] Art. 4, apartado 1, del RGPD.

De manera que los datos personales son información que puede vincularse a una persona física.

Mas allá de las definiciones legales, atendiendo a la jurisprudencia comunitaria vemos que el concepto de dato personal es muy amplio. Según el TJUE, tienen la consideración de datos personales, entre otros: el nombre y número de teléfono o información sobre condiciones de trabajo y/o aficiones[44], datos bancarios (ingresos, etc.)[45], datos personales que obran en poder del municipio[46], perfiles de usuario de las redes sociales[47], datos conseguidos por un detective privado[48], datos del registro de trabajo (periodos de trabajo, descanso, etc.)[49], la imagen de una persona grabada por una cámara[50], los datos fiscales[51], las respuestas escritas de un examen y las anotaciones del examinador[52], los que figuran en una minuta (nombre, fecha de nacimiento, nacionalidad, sexo, etnia, religión e idioma)[53],las comunicaciones escritas o habladas e imágenes[54], las filmaciones[55] o sonidos[56]de circuito cerrado de televisión, etc.

A la vista de la normativa y jurisprudencia comunitaria, los datos personales serán aquellos datos sobre una persona identificada o identificable, es decir, aquellos que identifican o permitan identificar a cualquier persona[57].

---

[44] STJUE (Gran Sala), de 6 de noviembre de 2003, asunto C-101/01, asunto Göta hovrät (Suecia) c. Lindqvist, ap. 24.
[45] STJUE (Gran Sala), de 20 de mayo de 2003, asunto C-465/00, caso Österreichischer Rundfunk y otros, ap. 64.
[46] STJUE (Sala Tercera), de 7 de mayo de 2009, asunto C-553/07, caso Rijkeboer, ap. 42.
[47] STJUE (Sala Tercera), de 16 de febrero de 2012, asunto C-360/10, caso SABAM, ap. 49.
[48] STJUE (Sala Tercera), de 7 de noviembre de 2013, asunto C-473/12, caso IPI, ap. 26
[49] STJUE (Sala Tercera), de 30 de mayo de 2013, asunto C-342/12, caso Worten y ACT, ap. 19.
[50] STJUE (Sala Cuarta), de 11 de diciembre de 2014, asunto C-212/13, caso František Ryneš y Úřad pro ochranu osobních údajů, ap. 22.
[51] STJUE (Sala Segunda), de 27 de septiembre de 2017, asunto C-73/16, caso Peter Puškár y otros, ap. 41 y STJUE (Sala Tercera), de 1 de octubre de 2015, asunto C-201/14, caso Bara y otros, ap. 29
[52] STJUE (Sala Segunda), de 20 de diciembre de 2017, asunto C-434/16, Peter Nowak y Data Protection Commissioner, ap. 37.
[53] STJUE (Sala Tercera), de 17 de julio de 2014, asuntos acumulados C-141/12 y C-372/12, caso YS (C-141/12) c. Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel (C-372/12) contra M y S, ap. 38.
[54] STEDH (Sección Tercera), de 24 de junio de 2004, asunto Von Hannover c. Alemania; STEDH (Sección Cuarta), de 11 de enero de 2005, asunto Sciacca c. Italia.
[55] STEDH (Sección Cuarta), de 28 de enero de 2003, asunto Peck c. el Reino Unido; STEDH (Sección Quinta), de 5 de octubre de 2010, asunto Köpke c. Alemania.
[56] TEDH (Sección Tercera), de 25 de septiembre de 2001, asunto P.G. y J.H. c. el Reino Unido, ap. 59 y 60; STEDH (Sección Segunda), de 20 de diciembre de 2005, asunto Wisse c. Francia.
[57] STEDH 27798/1995, de 16 de febrero de 2000, Amann contra Suiza, ap. 65; y STC 292/2000, de 30 de noviembre, FJ 6º.

4.3.4. El consentimiento del interesado

Como ya hemos dicho, el derecho fundamental a la protección de datos confiere al titular una facultad de disposición sobe sus datos, que ha de garantizar el Estado a través de la ley[58]. El ejercicio práctico de este derecho no se limita a proteger los datos si no que también comporta un control y un poder de disposición sobre los mismos.

Por lo tanto, el contenido de este derecho se manifiesta a través del consentimiento del interesado y los derechos ARSLOP[59] que podrá ejercer para controlar los datos.

El consentimiento es la facultad del individuo para decidir acerca de sus datos, es la capacidad de autodeterminación del individuo, su capacidad de decisión en el mundo tecnológico.

El consentimiento junto con los mencionados derechos ARSLOP, tal y como se refleja en el RGPD y en la LOPDGDD, son la piedra angular de la protección y tratamiento de datos, son el contenido esencial de este derecho. El consentimiento es una de las bases que legitima el tratamiento de datos[60]. Cuando el titular consiente esta celebrando un contrato[61], cuya ejecución consiste en el tratamiento de datos.

Debemos pues analizar en profundidad que interpretamos por consentimiento, como se ha de formaliza, cual es su estructura y sus requisitos básicos.

El consentimiento es una manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen[62].

Respecto a la forma debe darse mediante un acto afirmativo claro como una declaración por escrito, inclusive por medios electrónicos, una declaración verbal u otros medios como incluir marcar una casilla de un sitio web en internet (siempre que se haga a través

[58] STC 292/2000, de 30 de noviembre, FJ 5º

[59] Los «derechos ARSLOP»: derecho de acceso (art. 15 RGPD y art. 13 LOPDGDD), derecho de rectificación (art. 16 RGPD y art. 14 LOPDGDD), derecho de supresión (art. 17. RGPD y art. 15 LOPDGDD), derecho de limitación (art. 18. RGPD y art. 16 LOPDGDD), derecho de oposición (art. 21. RGPD y 18 LOPDGDD) y derecho de portabilidad (art. 20 RGPD y art. 17 LOPDGDD). Derechos que superan y actualizan los antiguos 'derechos ARCO': derecho de acceso, derecho de rectificación, derecho de cancelación y derecho de oposición.

[60] Art. 6.1, letra a), del RGPD y art. 6 de la LOPDGDD.

[61] Art. 6.1, letra b), del RGPD.

[62] Art. 4.11 del RGPD y art. 6.1 de la LOPDGDD.

de casillas no premarcardas), escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique que el interesado acepta la propuesta de tratamiento de sus datos personales[63].

El Comité Europeo de Protección de Datos (CEPD[64]), que sustituye al anterior Grupo sobre Protección de Datos del artículo 29 (GT29[65]), interpretó como debe ser un consentimiento válido, exigiendo para ello que se preste de manera "libre", "específica", "informada" e "inequívoca". A continuación, analizaremos estos requisitos.

a) "libre". El sujeto debe ser libre a la hora de prestar el consentimiento, no puede sentirse obligado a dar su consentimiento ni sentir que sufrirá consecuencias negativas si no lo presta. Si no es libre, el consentimiento no será válido. Para ello el RGPD ofrece información para valorar si se ha dado el consentimiento libre[66], recayendo la carga de la prueba sobre el responsable del tratamiento[67].

b) "específica". Se debe garantizar al interesado el control y la transparencia[68], dando opción a elegir los fines de los datos[69], evitando así la desviación en el uso de estos.

c) "Informada". Para que sea un consentimiento válido se exige que facilite información previa. El interesado, antes de dar su consentimiento, debe estar informado, para que así sea, según el GT29, se requiere como mínimo la siguiente información[70]: identidad del responsable del tratamiento, fin de cada tratamiento, tipo de datos que van a recogerse y utilizarse, el derecho a retirar el consentimiento,

[63] Considerando n.º 32 del RGPD.
[64] Comité Europeo de Protección de Datos. El RGPD (art. 68-76) ha creado el Comité Europeo de Protección de Datos (CEPD), un organismo europeo independiente que ha venido a sustituir al GT29 y en el que también se ha incluido el Supervisor Europeo de Protección de Datos (SEPD)
[65] El Grupo sobre Protección de Datos del artículo 29 (GT29) fue creado por la Directiva 95/46/ CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, en su artículo 29 (de ahí el nombre).
[66] Art. 7.4 RGPD y Considerando n.º 43 del RGPD.
[67] Art. 7.1 del RGPD.
[68] Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, del Grupo de Protección de Datos del artículo 29, adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, p. 12
[69] Dictamen 3/2013 sobre la limitación de la finalidad, del Grupo de Protección de Datos del artículo 29, adoptado el 3 de abril de 2013
[70] Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, del Grupo de Protección de Datos del artículo 29, adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, p. 14.

información sobre el uso de los datos para decisiones automatizadas e información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas.

d) "inequívoca". Esto implica que el consentimiento se preste a través de una declaración afirmativa, siempre deberá haber una acción o declaración afirmativa[71].

Como hemos mencionado anteriormente, la protección de datos se sustenta sobre dos piedras angulares: el consentimiento del interesado y los derechos ARSLOP. Estos segundos son un compendio de derechos que el RGPD[72] y la LOPDGDD[73] reconocen a todo internauta sobre el tratamiento de sus datos. Especial atención requiere el estudio de dos de ellos, el derecho de rectificación y el de supresión, que se conocen conjuntamente como derecho al olvido en internet.

El artículo 85.1 LOPDGDD posibilita la depuración reactiva (no preventiva) de datos personales o no, que contravienen la veracidad y la exactitud. Este articulo extiende los requisitos y procedimientos de la LO 2/1984[74] a cualquier usuario de redes que publique o difunda hechos inexactos que pudieran causar un perjuicio. Asimismo, debemos de tener en cuenta que este precepto no otorga a los proveedores de servicios de internet ninguna facultad de censura preventiva o reactiva, la facultad la tiene el usuario.

Respecto de la actualización de informaciones en medios de comunicación digitales, el artículo 86 LOPDGDD proclama que toda persona tiene derecho a solicitar de los medios de comunicación digitales la inclusión de un aviso de actualización, que ha de ser suficientemente visible e ir junto a las noticias que le afecten. Esto siempre y cuando la información contenida en la noticia original no refleje su situación actual, que se ha visto

[71] Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, del Grupo de Protección de Datos del artículo 29, adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, p. 17
[72] artículos 15 a 22
[73] Enumerados en los artículos 13 al 18
[74] Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación [consulta en línea] https://www.boe.es/buscar/act.php?id=BOE-A-1984-7248 [último acceso: 10 jun. 2023]

alterada a consecuencia de circunstancias que acontecieron después de la publicación, ocasionándole un perjuicio.

El artículo 94 LOPDGDD contiene el derecho al olvido en servicios de redes sociales y servicios similares en virtud del cual toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y equivalentes.

Como todo derecho, el derecho al olvido tiene limites, supuestos en los que tras una ponderación cede ante un interés mayor. En este caso, estos límites se encuentran citados en el artículo 17.3 RGPD, a saber: a) derecho de libertad de expresión e información, b) el cumplimiento de una obligación legal o de una misión de interés publico, c) la salud pública, d) el archivo público por razones de investigación científica, histórica o fines estadísticos, y e) la defensa de reclamaciones. Hemos de advertir que en casos de minoría de edad el derecho al olvido se manifiesta de manera incondicionada.

5. LA NAVEGACIÓN POR INTERNET: RIESGOS PARA NUESTRA PRIVACIDAD

En una etapa anterior, sin el desarrollo tecnológico actual, el respeto a la privacidad e intimidad se centraba en poner limites al uso de los sentidos, tales como la vista o el oído. De tal manera que los muros de nuestra casa eran suficientes para asegurar la protección de la privacidad y para excluir la difusión de los actos que sucedían en nuestra esfera mas íntima. Por lo que podemos afirmar que antes de la irrupción de las TIC, las injerencias en la vida privada encontraban limitadas por el espacio y por el tiempo.

Como hemos visto a lo largo de este trabajo el advenimiento de la era tecnológica, mas concretamente el uso masivo de internet y de las redes sociales, ha dinamitado estas limitaciones exponiendo al ciudadano a una situación de vigilancia sin precedentes. Actualmente es posible escuchar y observar a distancia, sin límites de tiempo o de espacio. Por ejemplo, conocer los datos fiscales aportados por los ciudadanos en los procesos informatizados de recaudación de impuestos (declaración del IRPF a través de internet), controlar los documentos de identificación digitalizados (DNI electrónico o

firmas digitales), datos bancarios facilitados al realizar pagos en internet, acceder al historial de búsquedas realizadas en la red, etc. cuestiones que ponen de manifiesto la omnipresente vigilancia informática a la que se encuentra sometida la sociedad actual.

Cada ciudadano, cuando navega por internet, queda registrado en un banco de datos. Generamos una descomunal cantidad de información digital que queda almacenada en servidores en poder de terceros o en la memoria de nuestros dispositivos. Esta información es muy relevante ya que puede revelar datos que afecten a los aspectos mas sensibles de nuestra vida privada, otorgando a quien los conozca un profundo conocimiento de nuestra personalidad, gustos, intereses, orientación sexual, afinidad política, creencias religiosas, etc. En definitiva, creamos una huella digital que contiene datos cuyo conocimiento permite identificar al usuario.

El desarrollo de las tecnologías permite un almacenamiento masivo de esta información. Entidades y personas, tanto públicas como privadas, tienen la posibilidad de acumular estos datos digitales para fines muy diversos y no siempre perfectamente identificados de manera que el ciudadano pierde el control sobre estas informaciones, sobre su tratamiento y posible alteración o cesión a terceros.

En consecuencia, el tratamiento de datos personales supone un potencial peligro para nuestra intimidad y privacidad, dando lugar a nuevas maneras de injerencia en este ámbito protegido, que se pueden llevar a cabo de una manera prolongada en el tiempo, sin necesidad de estar próximos en el espacio e incluso sin que la persona afectada se dé cuenta de ello.

En síntesis, la protección de datos se constituye como uno de los grandes desafíos jurídicos de nuestro siglo. Es una prioridad comprender esta compleja realidad online para solucionar los diferentes problemas legales que nacen de la inclusión tecnológica en nuestro día a día. Hemos de examinar los riesgos y crear construcciones jurídicas modernas para responder ante las nuevas amenazas tecnológicas que vulneran nuestros derechos fundamentales.

5.1 Los datos personales como moneda de cambio: El Big Data

Realizar una búsqueda en internet es gratuito, los internautas no pagamos contraprestación económica ninguna, pero si damos algo a cambio. Cuando navegamos

nos identificamos, revelamos nuestros deseos y preferencias, damos una información que tiene un valor comercial extraordinario porque gracias a ella la publicidad se personaliza. El anunciante se dirige a un sujeto concreto del que conoce sus intereses comerciales lo que multiplica la eficiencia del mensaje.

Crearse una cuenta en redes sociales también es gratuito. En estas, el usuario crea un perfil a través del cual vuelca una considerable cantidad de datos personales. Inclusive aun cuando se mantenga en una actitud pasiva, es decir, no publique contenido (fotos, videos, mensajes, etc.), los círculos con los que interactúa, las personas a las que sigue revelan información que potencialmente puede lesionar nuestra privacidad.

De manera que los usuarios de internet se convierten en "prosumidores"[75], consumidores de información y también productores, son sujetos que depositan información en un espacio virtual que ellos mismos construyen.

Internet es un entorno que fluye en dos direcciones en el que el usuario es consumidor y al mismo tiempo generador de contenido[76] consolidándose así un diálogo entre receptores y emisores en el que se intercambian informaciones sensibles. Internet se configura como un nuevo espacio virtual donde se celebran negocios jurídicos y se ejercitan distintos derechos en la red, creando constantemente relaciones jurídicas que se firman con un "clic".

Cada vez que navegamos por internet, revelamos de forma consentida o no, datos de nuestra personalidad, ideología, creencias, etc., y son estos datos los que posibilitan las agresiones al derecho a la intimidad.

En efecto, la red permite nuevas y mas ágiles formas de comunicación, pero también, y como contrapartida, la posibilidad de injerencias técnicas en las mismas. Internet presenta un potencial para agredir la intimidad sin precedentes[77]. Estas amenazas

---

[75] Conforme a Francisca Ramón Fernández "los consumidores de información se convierten en prosumidores, ya que producen información que ellos mismos consumen (…) se fomenta, pues, la colaboración y el intercambio de producción entre los usuarios". *La red social como ejemplo de participación: casos y cuestiones.* [In: AA.VV. *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías.* Lorenzo Cotino Hueso (Editor), PUV (Publicaciones de la Universidad de Valencia) Valencia: 2011, p.16]

[76] COTINO HUESO, Lorenzo. *Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los "blogs"). [in: AA.VV. Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías.* Lorenzo Cotino Hueso (Dir.), PUV (Publicaciones Universidad de Valencia) Valencia: 2011.

[77] Así lo afirma la jurisprudencia en la STC 110/1984, de 26 de noviembre, fundamento jurídico 3º.

provienen tanto del Estado como de particulares y empresas privadas. Desde el ámbito jurídico constitucional se ha de dar una respuesta urgente más no es un reto sencillo ya que los ataques que se pueden producir en internet son casi ilimitados[78], de proveniencia transfronteriza y, en consecuencia, difíciles de rastrear y perseguir por las autoridades.

El volumen de datos que se generan en internet es inmenso, cada día 2,5 quintillones de bytes de datos, para hacernos una idea de lo que esto supone "Si estuvieran impresos en libros, cubrirían la superficie entera de Estados Unidos, formando cincuenta y dos capas y si esta inmensa cantidad de datos estuvieran grabados en CD-ROMs apilados, tocarían la Luna formando cinco pilas separadas"[79]

Recopilar, tabular y acceder a estos datos es una nueva fuente de poder a la que se accede a través del Big Data. La expresión Big Data, traducida como "datos a gran escala" o "datos masivos", es un término que designa el tratamiento de grandes volúmenes de datos mediante algoritmos matemáticos con el fin de establecer correlaciones entre ellos, predecir tendencias y tomar decisiones[80]. Los usuarios de internet ceden sus datos para fines concretos, por ejemplo, en las redes sociales a cambio de una comunicación, pero desconocen sus usos posteriores, que tratamiento se dan a esos datos, que en ocasiones son comprados por terceros para finalidades distintas de las que han sido autorizadas, poniendo en entredicho la privacidad del usuario.

Las bases de datos y su tratamiento han supuesto un cambio de paradigma, los algoritmos utilizados hoy en día permiten encontrar patrones comunes en los datos para

---

[78] Existen múltiples herramientas para agredir nuestra intimidad, algunas de las más habituales: 1.*Sniffers:* programas diseñados para captar los paquetes que viajan por las redes con el fin de conocer el *username* y la contraseña para acceder a nuestras cuentas. 2.*Crackers:* software pensado para averiguar que usuarios han elegido contraseñas débiles para proteger sus cuentas. 3.*Xwatchwin:* software pensado para fines de docentes que permite capturar sesiones de Windows de un nodo concreto y observar que es lo que el usuario realiza. En las manos incorrectas puede ser una herramienta muy dañina pues permite observar que es lo que realiza el usuario sin que este note esta vigilancia. 4. *Hijacking:* técnica que consiste en tomar el control de una conexión ya establecida de forma que se suplanta al usuario que realmente establece la conexión, el cual queda "colgado" y acaba retirándose, dejando al hacker trabajando en el sistema desde el anonimato.
Todas estas definiciones han sido extraídas de: GONZÁLEZ, José Luis y SÁNCHEZ, Marisol. *Autopistas de la información e internet (Tecnología, Servicios, Peajes y normas de navegación).* Universidad de Extremadura, Cáceres: 1998, pp. 411-413.

[79] CABALLERO R, MARTÍN E. *Las bases de Big Data*. Catarata, Madrid 2015.

[80] SOTO, Yasmina. *Datos masivos con privacidad y no contra privacidad.* Revista de Bioética y Derecho. [consulta en línea] https://scielo.isciii.es/pdf/bioetica/n40/1886-5887-bioetica-40-00101.pdf [último acceso: 10 jun. 2023]

conocer la información que se desea. Saber sobre sus relaciones, conexiones e interacciones a través del Big Data supone claramente una amenaza a la privacidad y además permite la posibilidad de prever su futuro comportamiento[81].

La capacidad actual para almacenar y procesar datos supone un enorme riesgo para la intimidad y privacidad del usuario, de la mano del Big Data se ha creado régimen de control masivo, una sociedad de control sometida a una vigilancia ininterrumpida. Este control se realiza bajo una aparente libertad de los ciudadanos, que no somos conscientes de la vigilancia electrónica permanente que se lleva a cabo con bienes que adquirimos libremente: ordenadores, teléfonos móviles, tabletas, tarjetas bancarias inteligentes, relojes smartwatch, GPS, etc. Los ciudadanos facilitamos miles de datos sin tener conocimiento sobre el uso que se puede hacer de ellos, por ejemplo "Google, dispone de un impresionante número de sensores para espiar el comportamiento de cada usuario: el motor *Google Search* le permite saber dónde se encuentra el internauta, qué busca y en qué momento. El navegador Google Chrome envía directamente a *Alphabet*, la empresa matriz de Google, todo lo que hace el usuario en materia de navegación. *Google Analytics* elabora estadísticas muy precisas de las consultas de los internautas en la Red. Google Plus recoge información complementaria y la cruza. *Gmail* analiza la correspondencia intercambiada, lo cual dice mucho sobre el emisor y sus contactos. El servicio DNS (*Domain Name System*) de *Google* analiza los sitios visitados; YouTube, el servicio de vídeos más visitado del mundo que pertenece también a *Google*, y por tanto también a *Alphabet,* registra todo lo que los usuarios hacen en él. *Google Maps* identifica el lugar en el que se encuentra el internauta, adónde va, cuándo y con qué itinerario. Pero aún hay más: *AdWords* sabe lo que el empresario quiere vender o promocionar. Y desde el momento en que la gente enciende un *smartphone* con Android, *Google* sabe inmediatamente dónde está el usuario y qué está haciendo. Obviamente nadie obliga a recurrir a *Google*, pero cuando se requiere, *Google* lo sabe todo sobre los usuarios"[82]

[81] MATÉ-JIMENEZ C*. Big Data. Un nuevo paradigma de análisis de datos.* Anales de mecánica y electricidad, Vol. 91, Fascículo 6, 2014, pág. 10-16.
[82] RAMONET I. *Google lo sabe todo de ti*. LE MONDE Diplomatique, año XX N.º 224, febrero 2016. [consulta en línea] http://www.ignaciodarnaude.com/textos_diversos/Filpo,Google%20lo%20sabe%20todo%20de%20ti.pdf [último acceso: 10 jun. 2023]

Con cada clic que hacemos, con cada pago a través de la tarjeta de crédito, con cada búsqueda navegando por internet, suministramos magníficas informaciones sobre cada uno de nosotros. Datos de gran interés que, con mucha rapidez, serán analizados por corporaciones comerciales, empresas publicitarias, entidades financieras incluso por autoridades gubernamentales.[83].

Nuestros datos tienen interés para sectores tanto públicos como privados[84], como vemos en los siguientes ejemplos:

En el ámbito privado "MasterCard tiene una división llamada *MasterCard Advisors* que agrega y analiza 65.000 millones de transacciones de 1.500 millones de titulares de tarjetas en doscientos diez países con la finalidad de definir tendencias de negocio y consumo. Luego vende esa información a otros. Entre otras cosas, descubrió que cuando la gente llena de gasolina el depósito del coche alrededor de las cuatro de la tarde existe la probabilidad de que, a lo largo de la hora siguiente, gasten de treinta y cinco a cincuenta dólares en una tienda de comestibles o en un restaurante. Un publicista podría hacer uso de esa información para imprimir cupones de oferta de los negocios vecinos al dorso de los recibos de la gasolinera alrededor de esa hora del día. Como empresa intermediaria de los flujos de información, MasterCard se halla en una posición privilegiada para recopilar datos y capturar su valor. Se puede imaginar un futuro en el que las entidades emisoras de tarjetas de crédito renuncien a sus comisiones sobre las transacciones y las procesen gratuitamente a cambio de acceder a más datos, y perciban ingresos de la venta de analíticas cada vez más sofisticadas basadas en estos mismos datos[85]".

Otro ejemplo en el sector privado de esta situación de almacenamiento masivo de datos realizada por la empresa Vizio[86], fabricante de televisores inteligentes en USA y número

---

[83] RAMONET I. *El imperio de la vigilancia*. Clave Intelectual, 2016 [consulta en línea] https://www.eldiplo.org/wp-content/uploads/2018/files/7114/6040/1796/INTRODUCCION.pdf [último acceso: 10 jun. 2023]

[84] SALAS J. *¿Dónde acaban los datos privados que recogen las "apps" de salud?* El País, Ciencia. 8 de marzo de 2016. [consulta en línea] http://elpais.com/elpais/2016/03/07/ciencia/1457369646_082762.html [último acceso: 10 jun. 2023]

[85] MAYER-SCHÖNBERGER, V y CUKIER, K. *Big Data. La revolución de los datos masivos*. Turnen Noema, Madrid, 2015. Cap. VI, pág. 155-186.

[86] POZZI, S., "Cuando el televisor espía" en *El País,* 28 de julio de 2015, [consulta en línea], http://economia.elpais.com/economia/2015/07/27/actualidad/1438001658_976873.html [último acceso: 10 jun. 2023]

uno en ventas, que recolecto mas de 100 billones de datos de forma diaria a través de mas de 8 millones de televisores. Esta información era analizada y cedida a terceros para que conociesen cual eran los contenidos audiovisuales mas demandados por la población norteamericana.

En el ámbito público, en España existe el proyecto PADRIS[87], que según la AQUAS[88] ES un programa público de analítica de datos para la investigación y la innovación en salud. PADRIS tiene la misión de poner a disposición de la comunidad científica los datos sanitarios relacionados para impulsar la investigación, la innovación y la evaluación en salud mediante el acceso a la reutilización y cruce de los datos sanitarios generados por el SISCAT[89]. Este proyecto recopila datos sanitarios para ponerlos a disposición de los centros de investigación, con la finalidad de mejorar los servicios de salud, tal como indica el Observatorio de Bioética y Derecho en su documento sobre Bioética y Big Data[90]. Pero, estos datos también se ponen a disposición de terceras partes una gran cantidad de datos sobre la salud de la ciudadanía catalana, empresas que reutilizarían los datos para fines distintos que el usuario desconoce, probablemente venderlos y obtener un beneficio económico.

Por lo que el valor de los datos no reside únicamente en recopilarlos si no en su potencial reutilización, es decir, el valor no esta en su posesión si no en su uso. Por lo tanto, las empresas desean obtener más información sobre sus usuarios, para analizarlos, y posteriormente venderlos o alquilarlos, creándose una nueva economía en torno al análisis y compraventa o alquiler de estos datos, con la finalidad de conocer mejor a los usuarios para ofrecer productos que se adecúen a sus necesidades[91]. Las páginas web recomiendan productos que es muy probable que consumamos ya que conocen nuestras preferencias y saben que nos interesa ese bien o servicio. La utilización de nuestros datos permite a las empresas realizar una oferta personalizada que se adecua al interés del cliente, todo ello vulnerando nuestra intimidad y privacidad.

---

[87] OBSERVATORIO DE BIOÉTICA Y DERECHO, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Universidad de Barcelona, 2015. [consulta en línea] http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf [último acceso: 10 jun. 2023]

[88] Agència de Qualitat i Avaluació Sanitària de Catalunya

[89] sistema sanitario integral de utilización pública de Cataluña

[90] Ibid.

[91] CABALLERO. R; MARTÍN. E. *Las bases de Big Data*. Catarata, Madrid 2015.

Tal como nos ilustra Rafael Caballero:

> "Inditex, tiene su propio centro de datos en A Coruña. Emplean técnicas de Big Data y gracias a la gestión eficiente de los datos, cuando un cliente no encuentra una talla de una prenda, Inditex garantiza que repondrá el producto en menos de 48 horas. Para hacerlo, el sistema informático primero mira si la prenda existe en el stock de una tienda o centro de distribución cercano, y en caso de que no sea así, es el propio sistema informático el que solicita la fabricación de nuevas prendas. Pero no todo es gestión del stock. Inditex también aplica técnicas de minería de datos para averiguar qué prendas son compradas a la vez de forma habitual"[92].

Conociendo y analizando los datos de sus ventas, Inditex adapta su fabricación de prendas a los gustos demandados por sus clientes. En principio este es un uso legítimo ya que responde a un fin consentido por el usuario que compra online productos de Inditex, pero a estos datos sobre las ventas en tiendas hay que añadirle la información extraída de forma automática por programas que examinan nuestras búsquedas en internet y en redes sociales. De manera que el acopio de información sobre el usuario proviene de diversas fuentes que almacenan los datos y la usan directamente o la licencian para que otros extraigan su valor.

Estos ejemplos evidencian que los datos se han convertido en un elemento esencial de nuestra sociedad y que tienen un alto valor de mercado. Estos datos revelan información que, en la mayoría de los casos, afecta a nuestra privacidad e intimidad. Los datos pueden ofrecer un sinfín de mejoras en los servicios, pero muchas veces a cambio de esas mejoras se vulneran nuestros derechos.

El avance de las tecnologías ha reducido nuestro ámbito de vida privada. Empresas como *Facebook, Twitter o Instagram* tienen perfiles de sus usuarios que reflejan patrones de nuestra vida diaria. A través de lo que "posteamos", nuestros comentarios, "*likes*", seguidores, etc., las redes sociales lo conocen todo sobre nuestras opiniones y gustos personales, manejan un patrón del usuario que pueden comercializar, y comercializan, a empresas publicitarias que están deseosas de adquirir dicha información ya que, gracias al análisis de estos datos acopiados, conocerán al consumidor y estarán en una

[92] Ibid.

mejor posición para ofrecer una publicidad especifica y adaptada personalmente a estos datos.

No solo volcamos nuestros datos a través de redes sociales, las fuentes, y en consecuencia los detectores de nuestros actos, abundan por todas partes: tarjetas de fidelidad que ofrecen la mayoría de comercios (Eroski, Alcampo, FNAC, El Corte Inglés, Costco…) que registran los productos favoritos de sus clientes para conocer sus gustos, escáneres de reconocimiento facial o de huella digital que crean bases de datos biométricas de cada ciudadano, apps como *Google Maps, Wikiloc o Waze* que registran nuestra ubicación GPS y conocen nuestros desplazamientos, apps para gestionar nuestros ahorros como *Fintonic, Money Manager, Honeydue o Mint* que manejan información dineraria de sus usuarios o incluso dentro del ámbito sanitario aplicaciones conocidas como *apps Mhealth*[93]que conectan a las personas con dispositivos médicos o sensores, recordatorios de medicación e información de salud a través de mensajes y servicios de telemedicina.

Estas informaciones que son analizadas por un imperio en la sombra al servicio de corporaciones comerciales, de empresas publicitarias, de entidades financieras, de partidos políticos o de autoridades gubernamentales[94]. Se han creado nuevas economías alrededor de estos datos y nuevos actores se benefician de ello, "los datos son una plataforma" afirma Tim O'Reilly, editor de tecnología y voz autorizada de Silicon Valley, ya que se trata de bloques de construcción para fabricar nuevos bienes y modelos de negocio[95].

Estos datos masivos, si se manejan de una forma responsable, son una herramienta útil para facilitar los actos de los usuarios como en el caso de Oren Etzioni[96]: En 2003, el Sr. Etzioni voló de Seattle a Los Ángeles. Creyendo que cuanto antes comprase el billete menor precio pagaría, reservo el suyo con meses de antelación. Una vez ya embarcado en el avión se sorprendió al saber que la mayoría de los pasajeros habían pagado menos

[93] Mas información sobre estas apps disponible en https://www.ehcos.com/la-revolucion-del-mhealth-en-salud/. [último acceso: 10 jun. 2023]

[94] RAMONET, I. op. cit.

[95] MAYER-SCHÖNBERGER, V y CUKIER, K. op. cit.

[96] Caso de Oren Etzioni, sobre un uso de los datos masivos de forma positiva para el usuario. Consulta op. cit. Cap. I, pág. 11-32

que él, aún cuando lo habían comprado mas tarde. En ese momento Etzioni se decidió a buscar la forma de que la gente pudiese saber si lo que pagaba por su billete de avión era un buen precio o no. Para ello, Etzioni creó un modelo predictivo que, mediante la recopilación y el análisis de datos, ofrecía a los futuros pasajeros un ahorro prediciendo si el billete iba a subir o bajar de precio, ofreciendo al usuario la posibilidad de comprar en el momento óptimo. Este proyecto evoluciono hasta convertirse en la empresa *Farecast* adquirida por Microsoft en 2008. Este ejemplo nos permite observar dos cosas, la primera que el análisis de datos es una materia prima de un nuevo negocio con un gran valor económico, y la segunda, que, con una utilización correcta, el Big Data puede ofrecer nuevos servicios de gran utilidad al ciudadano.

Pero si a los datos masivos se les da un mal uso tienen consecuencias especialmente graves contra nuestra privacidad e intimidad. Por ejemplo, los datos que volcamos en las *Mhealth apps* tienen un carácter sensible y privado, sin embargo, lo mas habitual es que el usuario desconozca lo que comparte ni con quien lo comprarte. Esta falta de información tiene consecuencias, la revista medica JAMA[97] ha publicado un estudio para dar a conocer este incipiente problema, en el que advierte que "los pacientes pueden creen por error que la información que vuelcan en una *app* es privada, sobre todo si tiene política de privacidad, pero generalmente no es así".

Si bien no debemos obviar los beneficios de estas apps para nuestra salud (ayudarnos a perder peso y mantenernos en forma, vigilar enfermedades como la diabetes, monitorizar nuestro ritmo cardiaco para prever cardiopatías, conocer el estado anímico del usuario y cuidar de nuestra salud mental, recordarnos la pauta de ingesta de medicamentos, etc.) se ha de informar al ciudadano de la importancia de ceder los datos personales, en el ámbito de estas apps especialmente sensibles porque hemos de conocer su tratamiento, y que terceros están interesados en adquirir estos datos y con que fines.

No existe, ni se facilita que exista, una cultura social sobre la privacidad en materia de datos personales, es necesario informar a la ciudadanía sobre los usos de sus datos,

[97] BLENNER, S. *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*. March 8: Vol 315, No. 10, 2016. [consulta en línea] http://jama.jamanetwork.com/article.aspx?articleid=2499265. [último acceso: 10 jun. 2023]

advertir sobre las posteriores reutilizaciones de estos. Cada vez que descargamos una App o nos registramos en una red social, o accedemos a una pagina web que nos interesa consultar aceptamos los términos y condiciones de privacidad y las cookies, damos nuestro consentimiento, firmamos un contrato. La mayoría de la población ni se molesta en leer estas reglas que imponen al usuario ya que requiere demasiado tiempo y esfuerzo dada la complejidad con las que se redactan[98]. Los textos donde explican a los usuarios sus términos son muy extensos, se valen de un lenguaje muy técnico lleno de especificaciones legales y cláusulas de difícil comprensión. Todo ello provoca que los usuarios de estas herramientas digitales acepten los términos sin detenerse a leerlos, haciendo *scroll*[99] para llegar cuanto antes a la casilla de aceptar y poder disfrutar de los servicios.

Como hemos referido a lo largo de este trabajo, nuestra privacidad queda vulnerada por el contenido de los datos personales. Estos datos dicen mucho de los usuarios y es necesario que la ciudadanía tome consciencia de porqué y para qué deben protegerse. Bajo la premisa de un consentimiento dado por el usuario, las empresas comercializan estos datos con terceros, obtienen rendimientos económicos de nuestros datos al venderlos o cederlos a un tercero que, a su vez, se beneficia porque estructura y categoriza sus productos según las necesidades de compra de sus clientes.

En definitiva, el Big Data es una revolución que, en palabras de Mayer-Schönberger y Cukier, "no estriba en las máquinas que calculan los datos, sino en los datos mismos y en cómo los usamos y usaremos en el futuro[100]".

5.2 La cesión de nuestros datos personales: el consentimiento y las cookies

Es el titular del derecho a la intimidad y privacidad quien delimita el ámbito de lo que considera como lo íntimo y lo privado. Si bien la jurisprudencia[101] ha reconocido una serie de temas (orientación sexual, intimidad corporal, ideología política, estado de

[98] PARRA, Sergio. *Términos y condiciones web*. Yorokobu. 30 de septiembre de 2016. Blog accesible en: www.yorokobu.es/terminos-y-condiciones/18/?offset=29.

[99] Anglicismo referido al desplazamiento, generalmente de arriba hacia abajo, de los contenidos que forman una página web, una app, etc.

[100] MAYER-SCHÖNBERGER, V y CUKIER, K. op. cit.

[101] SSTC 156/2001, de 2 de julio; 196/2004 de 15 de noviembre; 25/2005, de 14 de febrero; 70/2009, de 23 de marzo; 159/2009, de 29 de junio; 136/2001, de 18 de junio, entre otras [in: Medina Guerrero, Manuel. *La protección Constitucional de la intimidad frente a los medios de comunicación.* Tirant lo Blanch, Valencia: 2005, pág. 24-29]

salud, relaciones matrimoniales, etc.) que por su contenido se consideran como íntimos y por ende protegidos constitucionalmente, en última instancia el ciudadano tiene la capacidad de renunciar a esta intimidad y hacer dichos temas públicos.

Configurada así, la vulnerabilidad de la intimidad y privacidad en internet es enorme. En numerosas ocasiones el titular, es víctima de su propio poder de decisión sobre lo que considera íntimo o no. Por lo que, es necesario que el consentimiento sea legitimo, para ello se ha de prestar de manera libre, específica, informada e inequívoca.

En la navegación por la red el usuario se ve forzado a comprometer su propia privacidad cuando consiente cookies impuestas por el operador de la pagina web o por terceros. Cookies que el usuario acepta con un simple clic, haciendo *scroll* sin detenerse informarse de lo que implica realmente su declaración de voluntad para el tratamiento de los datos recabados. Teniendo en cuenta esto, cabe preguntarse ¿estamos ante un consentimiento válido? Es interesante conocer la postura del TJUE sobre el consentimiento en materia de cookies en el caso 673/17[102].

Pero antes de adentrarnos a analizar la jurisprudencia comunitaria se antoja esencial en este punto referirnos a las cookies, conocer qué son y qué conlleva su utilización.

Las cookies son pequeños archivos que se guardan en los ordenadores de los usuarios para almacenar preferencias y otros datos utilizados en las páginas web que visitan[103].

Por lo tanto, el concepto de cookies se refiere a la información guardada en el equipo de un usuario con el fin de facilitar el acceso a páginas web, aunque también se utilizan para el seguimiento o rastreo de las actividades de los usuarios[104]. No todas las cookies

[102] Asunto C-673/17 resuelto en la Sentencia de Gran Sala EU:C:2019:801

[103] Definición de Google Ads [consulta en línea] https://support.google.com/google-ads/answer/2407785?hl=es&sjid=10920011215786164 20-EU

[104] Existen varias categorías de cookies, la Agencia Española de Protección de Datos (en adelante AEPD) las clasifica de la siguiente forma: a) según la entidad que las gestione; b) según el plazo de tiempo que permanecen activadas; y, c) según su finalidad.

a) según la entidad que las gestione:

Se distinguen dos tipos de cookies; las propias y las de terceros. Las propias son las enviadas al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el cual se presta el servicio solicitado por el usuario. Las de terceros son las enviadas al equipo terminal del usuario desde un equipo o dominio el cual no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las *cookies*.

son utilizadas de forma ilegítima, pero es común encontrar abusos, ya que pueden revelar los hábitos de navegación de los usuarios en línea e indudablemente, plantean preocupaciones en cuanto a la privacidad de las personas.

En principio las cookies brindan beneficios significativos en el ámbito de la navegación por Internet. Por ejemplo, permiten a los usuarios acceder de manera rápida a sitios web frecuentemente visitados, evitando la necesidad de volver a ingresar contraseñas. Además, las cookies son capaces de almacenar y rastrear las preferencias de los usuarios, lo que posibilita la presentación de contenido web personalizado y relevante.

No obstante, es importante considerar los aspectos negativos asociados a las cookies. En términos de seguridad, las cookies pueden ser objeto de ataques por parte de hackers que buscan obtener acceso no autorizado a cuentas de usuario. Estos actores

b) según el plazo de tiempo que permanecen activadas:

se distinguen dos tipos de cookies; las de sesión y las persistentes. Las de sesión están diseñadas para obtener y almacenar los datos del usuario para acceder a una página web, se recaban para almacenar para almacenar información que solo interesa conservar para la prestación de un servicio solicitado por el usuario en una ocasión. Por el contrario, las cookies permanentes son aquellas en las cuales los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo de tiempo definido por el responsable de la cookie (este plazo puede ser de unos minutos a varios años).

c)según su finalidad:

atendiendo a la finalidad para la cual se utilizan los datos obtenidos a través de las cookies podemos distinguir entre las técnicas, de personalización, de análisis y las publicitarias.

Las cookies técnicas son las que facilitan al usuario la navegación a través de la página web y la utilización de los servicios que en ella existan (por ejemplo, identificar el ID y la contraseña de un usuario. Otro ejemplo, en las redes sociales las cookies que permiten el almacenar contenido audiovisual para compartirlo).

Las cookies de personalización son aquellas que permiten al usuario caracterizar el servicio en función de una serie de criterios del terminal con el que el usuario accede (por ejemplo, el idioma en función del lugar desde donde se accede).

Las cookies de análisis son las que permiten al proveedor conocer y seguir el comportamiento de los usuarios. Esta información recopilada se utiliza para elaborar un perfil de navegación del usuario de dicho sitio web con el fin de introducir mejoras en el servicio. Estas cookies no representan una amenaza a la privacidad si tan solo tienen fines estadísticos, siempre y cuando se facilite información sobre su uso y el usuario tenga la facultad de negar su utilización.

Las cookies publicitarias son las que permiten la gestión de los espacios publicitarios que el editor haya incluido en la pagina web, aplicación o plataforma. Estas cookies “observan” el comportamiento del usuario, sus hábitos de navegación, para mostrar publicidad que se ajuste a sus intereses.

maliciosos pueden aprovechar la información almacenada en las cookies, incluyendo nombres de usuario y contraseñas, para acceder a datos personales del usuario.

Adicionalmente, desde el punto de vista de la monetización en línea, muchas plataformas web gratuitas dependen de la publicidad como fuente de ingresos. Las cookies desempeñan un papel crucial en la entrega de anuncios personalizados, basados en los intereses y comportamientos de los usuarios. Sin embargo, esta práctica puede resultar intrusiva y afectar negativamente la experiencia de navegación, al generar interrupciones o ralentizar la carga de las páginas.

Si bien las cookies ofrecen ventajas en términos de accesibilidad y personalización de contenido, también conllevan riesgos de seguridad y posibles inconvenientes relacionados con la publicidad en línea. Es fundamental encontrar un equilibrio entre la comodidad y la protección de la privacidad del usuario.

Una parte considerable de la inversión en el ámbito de Internet se destina a la publicidad en línea. En este sentido, las cookies desempeñan un rol central en la ejecución de estrategias publicitarias en Internet. Su función principal radica en facilitar la navegación del usuario y ofrecer publicidad altamente personalizada, basada en ocasiones en los patrones de navegación registrados mediante las cookies[105].

Uno de los problemas que planteaba el uso de las cookies era que no se informaba al usuario sobre la implementación de estas en las páginas web. El Parlamento Europeo y el Consejo Europeo advirtieron de esta situación en la Directiva 2009/136/CE[106] ,que en su considerando 66 señala lo siguiente:

> "*Puede que haya terceros que deseen almacenar información sobre el equipo de un usuario o acceder a información ya almacenada, con distintos fines, que van desde los fines legítimos (como algunos tipos de cookies) hasta aquellos que suponen una intrusión injustificada en la esfera privada (como los programas espía o los virus). Resulta, por tanto,*

[105] Agencia Española de Protección de Datos (AEPD), "Guía sobre el uso de cookies", [consulta en línea] https://www.aepd.es/es/documento/guia-cookies.pdf [último acceso: 10 jun. 2023]
[106] Directiva 2009/136/CE del parlamento europeo y del consejo de 25 de noviembre de 2009 [consulta en línea] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:Es:PDF [último acceso: 10 jun. 2023]

capital que los usuarios reciban una información clara y completa cuando realicen una acción que pueda dar lugar a dicho almacenamiento u obtención de acceso"

También, la mencionada Directiva advierte sobre la grave amenaza que suponen los programas informáticos (spyware o programas espía) que controlan subrepticiamente las acciones de los usuarios e incluso pueden llegar a tomar el control del funcionamiento de los terminales. La Directiva encomienda a los Estados miembros que informen a sus ciudadanos acerca de esta amenaza para que puedan tomar las precauciones necesarias para proteger sus terminales contra estos virus espía.

Por lo visto hasta ahora, sabemos que las cookies son archivos que almacenan datos, información acerca de las acciones que realiza en la web el internauta, y que se utilizan para ofrecer ventajas de accesibilidad (recordar contraseñas) y también para fines comerciales (elaboración de un perfil comercial para adecuar la publicidad a los intereses del usuario). De manera que, las cookies contienen información muy sensible sobre la persona que utiliza un servicio de la sociedad de la información. Esto nos lleva a realizarnos la siguiente pregunta ¿Cómo puede el usuario controlar el tratamiento de los datos?

La respuesta jurídica a esta cuestión la da la Ley de servicios de la sociedad de la información y de comercio electrónico[107] (en adelante LSSI). Concretamente, en el artículo 22.2 dispone:

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

Por lo que podemos afirmar que el consentimiento informado es el elemento clave, la llave que permite al usuario saber que datos envía, quien conoce estos datos y con que

[107] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [consulta en línea] https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758 [último acceso: 10 jun. 2023]

fin. Pero ¿cómo ha de ser este consentimiento para que el tratamiento de la información recabada por las cookies sea válido? Para resolver esta cuestión hemos de analizar la jurisprudencia comunitaria que mencionábamos al comienzo de este subepígrafe.

El caso 673/17 tiene por objeto resolver una cuestión prejudicial planteada por el Tribunal Supremo alemán, que pide al TJUE que interprete el derecho comunitario en relación con la protección de la intimidad en el sector de las comunicaciones electrónicas.

La cuestión se suscita en el contexto de un litigio entre la Federación de Organizaciones de Consumidores de Alemania y la sociedad mercantil "planet49" que desarrolla juegos online. Los participantes en estos juegos, a través de la aceptación de las cookies, autorizaban la transmisión de sus datos personales a patrocinadores y empresas colaboradoras de la mercantil "planet49". En 2013 esta empresa alemana organizo un juego a través de una página en internet. Los participantes que deseasen participar debían introducir su código postal, tras lo cual accedían a un sitio web en el que debían incluir su nombre y dirección postal. En este sitio web, debajo de los espacios reservados para adjuntar dicha información, acompañaban dos casillas cuyo contenido era el siguiente.

En una primera casilla, que no estaba marcada por defecto, se estipulaba:

> *"Presto mi consentimiento para que determinados patrocinadores y empresas colaboradoras puedan informarme por correo, teléfono, correo electrónico o SMS sobre ofertas de su respectivo ámbito de actividad. Yo mismo puedo determinarlos aquí, en caso contrario serán elegidos por el organizador. Puedo revocar mi consentimiento en cualquier momento. Aquí puede obtener más información al respecto"*

La segunda casilla, marcada por defecto, contenía lo siguiente:

> *"Presto mi consentimiento para el uso del servicio de análisis de páginas web Remintrex. En consecuencia, el organizador del juego con fines promocionales, [Planet49], instalará cookies una vez me haya registrado para en el juego, lo que le permitirá analizar mi comportamiento de navegación y uso de páginas web de socios publicitarios y enviarme*

publicidad específica conforme a mis intereses a través de Remintrex. Puedo cancelar las cookies en cualquier momento. Aquí puede obtener más información al respecto".

La participación en el juego era únicamente posible si se marcaba, al menos, la primera casilla. La organización de consumidores alemana alegó que las declaraciones consentimiento solicitadas por "Planet49" eran ilegales, y presento una demanda ante el Tribunal Regional de lo Civil y Penal de Fráncfort solicitando que se condenase a "Planet49" a dejar de recabar dichos consentimientos y a pagar una indemnización a los afectados.

Tras un recurso de apelación contra la resolución de primera instancia y otro de casación contra la sentencia de segunda instancia, el asunto llega al Alto Tribunal alemán que suspende le procedimiento y plantea una cuestión prejudicial al TJUE, para que interprete el derecho comunitario en materia de prestación de consentimiento válido. Concretamente si el consentimiento prestado en este caso es válido a la luz de las disposiciones de los artículos 5, apartado 3, y 2, letra f), de la Directiva 2002/58, del artículo 2, letra h), de la Directiva 95/46, y del artículo 6, apartado 1, letra a), del Reglamento 2016/679.

El TJUE se enfoca en examinar el manejo de los datos recopilados de un usuario mediante el uso de cookies, y limita su alcance a una declaración de voluntad válidamente otorgada.

El artículo 1261 del Código Civil establece que los contratos se componen de tres elementos esenciales: el consentimiento, el objeto y la causa. Entre estos elementos, el consentimiento es el más relevante, ya que la obligatoriedad del contrato y las obligaciones que se derivan de él se basan en el acuerdo de voluntades[108]. Para que el consentimiento sea válido es requisito necesario que las voluntades se hayan conformado libremente y de modo consciente y deliberado. Si no ocurre así, estaremos ante un consentimiento viciado, que puede incluso conllevar la anulabilidad del contrato.

[108] SÁNCHEZ CALERO, F.J. (2016). *Curso de derecho civil II. Derecho de obligaciones, contratos y responsabilidad por hechos ilícitos*. Valencia: Tirant lo Blanch, 145

La declaración de voluntad es el acto mediante el cual el sujeto exterioriza lo querido. Es un acto positivo que precisa de la voluntad encaminada a realizar la conducta externa, el comportamiento material, en el que tal declaración consiste. Así pues, quien hace involuntariamente un signo que en el tráfico significa aceptación de una oferta, no manifiesta aceptar esta[109].

En este sentido se posiciona el TJUE en la sentencia comentada cuando en su considerando 59 afirma que:

> "en contra de lo que aduce *Planet49*, el hecho de que un usuario active el botón de participación en el juego con fines promocionales organizado por dicha sociedad no basta para considerar que el usuario ha dado de manera válida su consentimiento para la colocación de *cookies"*

Para que sea licito, conforme al RGPD, recopilar y almacenar información a través de las cookies de los terminales de los usuarios es necesario que estos sean informados de manera clara de que datos se recopilan, con que finalidad y quien es el responsable de dicho tratamiento para que el interesado pueda oponerse al mismo.

Para el TJUE, el artículo 5.3 de la Directiva 2002/58 impone la obligación al operador de una página web que coloca una cookie en el ordenador de un usuario de obtener el previo consentimiento de este, lo cual implica: a) un deber de información al afectado sobre la colocación y fines de las cookies que acepta, b) conocida esta información, el usuario debe consentirla antes de que se coloque la cookie y nunca después o de manera simultánea y c) el interesado a la hora de prestar un consentimiento o no debe hacerlo de manera proactiva.

Es este último punto, la actitud proactiva, el que genera mas debate doctrinal. Muchas veces el internauta no ve la información que acompaña la casilla, se limita a simplemente marcarla, a aceptarla, sin conocer su contenido. Un sector doctrinal considera que a la hora de prestar consentimiento ha de exigirse al usuario la diligencia contenida en el artículo 1104 del Código Civil. Si bien existen voces doctrinales que abogan por una reforma del derecho contractual como medida inmediata para acabar con la incertidumbre que generan las cláusulas mediante las cuales los proveedores de

[109] ALBADALEJO, M. (2013). *Derecho civil I. Introducción y parte general*. Madrid: Edisofer,545.

servicios se reservan el derecho de almacenar datos por ellos mismos o por terceros en otros países[110].

Para la mayoría de la doctrina, el consentimiento informado otorgado mediante una casilla premarcada es un consentimiento viciado, producido por un error, que afecta a la declaración de la voluntad cuando el usuario queriendo declarar una cosa, acaba declarando equívocamente otra[111].

Tras caracterizar el como debe ser el consentimiento para que sea válido, el TJUE trata otras dos cuestiones: a) si se ha de informar al usuario del tiempo de duración de las cookies, es decir, cuanto tiempo estarán activas y b) la posibilidad de acceso de terceros a ellas.

Para el TJUE, las cookies instaladas por la empresa Planet49 tienen fines publicitarios, es decir, la información a la que se accede se utilizara por las empresas colaboradoras para adecuar sus ofertas publicitarias a los intereses del internauta. El TJUE afirma que en virtud del deber de información contenido en el artículo 5.3 de la Directiva 2002/58, debe darse a conocer al usuario tanto el tiempo durante el cual las cookies estarán activas tanto como la posibilidad de acceso de los terceros a la información obtenida. Para el TJUE:

> "debe considerarse que la información relativa al tiempo durante el cual las *cookies* estarán activas responde a la exigencia, establecida en dicho artículo, de que el tratamiento de los datos sea leal, puesto que, en una situación como la controvertida en el litigio principal, un periodo de tiempo largo, o incluso ilimitado, implica la recogida de numerosos datos sobre los hábitos de navegación y la frecuencia de las eventuales visitas del usuario a los sitios de los socios publicitarios del organizador del juego con fines promocionales"[112]

Continua el TJUE, afirmando que:

> "para garantizar un tratamiento de datos leal y transparente, el responsable del tratamiento debe facilitar al interesado información, entre otras cosas, sobre el plazo

[110] REBOLLO DELGADO, L. (2017). *Contratación electrónica y protección de los consumidores —una visión panorámica—*. Madrid: Reus, 282

[111] DÍEZ-PICAZO, L. (2007). *Fundamentos del derecho civil patrimonial I. Introducción. Teoría del contrato*. Pamplona: Aranzadi, Thomson Reuters, Civitas, 149 y 172-183.

[112] Asunto *C-673/17* (Sentencia de Gran Sala EU:C:2019:801), apdo. 78

> durante el cual se conservarán los datos personales o, cuando no sea posible, sobre los criterios utilizados para determinar este plazo"[113]

Por lo que este deber de información por parte de los proveedores, del objeto, del fin y del tiempo durante el cual las *cookies* permanecerán activas, se fundamenta tanto por la complejidad de la naturaleza técnica de aquellas como por la situación de partida de desequilibrio subjetivo, por lo que deviene necesario tutelar la confianza legítima que una parte deposita en la otra, al objeto de corregirlo[114].

Podemos concluir que para el TJUE el consentimiento ofrecido por un internauta para considerarse válido ha de ser activo, es decir, que sea consecuencia de una acción libre, clara, específica, informada e inequívoca. En el asunto "Planet49" el TJUE confirma que las casillas preseleccionadas no son una forma de consentimiento valido por no cumplir con los requisitos legales del RGPD, porque no puede verificarse que el usuario "no haya leído la información que acompaña a la casilla marcada por defecto, o que ni tan siquiera la haya visto, antes de proseguir con su actividad en el sitio de Internet que visita"[115]. Además, el TJUE afirma que para que la información suministrada al usuario pueda considerarse "clara y completa" ha de incluir "información acerca del tiempo durante el cual las cookies estarán activas y la posibilidad de que terceros tengan acceso a ellas[116].

Esta sentencia que hemos decidido comentar es de suma importancia puesto que consolida la doctrina jurisprudencial europea sobre como debe ser el consentimiento en materia de cookies y se erige como un referente hermenéutico para la interpretación del articulo 5.3 de la Directiva 2002/58. Asimismo, supone un paso más en la armonización en el sector de las comunicaciones electrónicas en Europa y que contribuye a proteger la privacidad en Internet.

[113] Asunto *C-673/17* (Sentencia de Gran Sala EU:C:2019:801), apdo. 79
[114] CORRIPIO GIL-DELGADO, M.R. (1999). *Los contratos informáticos. El deber de información precontractual*. Madrid: Publicaciones de la Universidad Pontificia Comillas, 278.
[115] Asunto *C-673/17* (Sentencia de Gran Sala EU:C:2019:801), apdo. 55
[116] Asunto *C-673/17* (Sentencia de Gran Sala EU:C:2019:801), apdo. 75.

6. ESTUDIO DEL CASO GOOGLE SPAIN Y GOOGLE INC. VS MARIO COSTEJA Y LA AEPD

El caso Mario Costeja vs Google adquiere una relevancia significativa en el análisis de la protección de la privacidad en internet, ya que ejemplifica la aplicación del derecho al olvido como una manifestación del derecho a la protección de datos. El Sr. Costeja, como protagonista de un largo proceso judicial, se convirtió involuntariamente en un impulsor del llamado derecho al olvido digital, tanto en España como en otros países miembros de la Unión Europea. Su demanda buscaba que sus datos personales desaparecieran de los resultados de búsqueda en el motor de búsqueda Google, lo que a su vez planteó cuestiones sobre la responsabilidad de las empresas que ofrecen estos servicios en el tratamiento de los datos personales resultantes de las búsquedas.

A lo largo de este trabajo, hemos subrayado que la protección de datos se configura como un derecho fundamental autónomo, aunque estrechamente relacionado con nuestra privacidad y nuestra intimidad. En la práctica, los datos personales a menudo afectan estas tres esferas jurídicas de manera interrelacionada. En este contexto, analizaremos los hechos que dieron lugar a este litigio ante la jurisprudencia española, el cual finalmente llevó a una consulta prejudicial y examinaremos cómo el Tribunal de Justicia de la Unión Europea resolvió dicha cuestión.

6.1 Antecedentes del caso

El 19 de enero de 1998, se difundió a través del periódico La Vanguardia la noticia sobre la subasta de propiedades embargadas por la Tesorería de la Seguridad Social. Entre estos bienes se encontraba una propiedad perteneciente al señor Mario Costeja y su esposa. Esta información fue inicialmente publicada en la edición impresa del periódico y posteriormente, en el año 2008, se volvió a difundir a través de su versión electrónica.

En el año 2010, el Sr. Costeja solicita al periódico que elimine ambas publicaciones, a lo cual La Vanguardia se opuso argumentando que la publicación era perfectamente legal y se encuentra amparada por su libertad de expresión.

Ante esto, el Sr. Costeja se dirige a la AEPD, presentando una reclamación contra este medio y contra Google Spain y Google Inc, solicitando que se eliminen o se modifiquen las publicaciones.

El Sr Costeja argumenta que el embargo realizado por la Seguridad Social ya estaba totalmente solucionado y su deuda satisfecha desde hacía años y que, actualmente, la noticia carecía de relevancia. La reclamación se basaba en el hecho de que, al realizar una búsqueda con su nombre en el motor de búsqueda de Google, se obtenían como resultados enlaces hacia dos páginas del periódico La Vanguardia que contenían un anuncio sobre una subasta de inmuebles relacionada con un embargo de deudas a la Seguridad Social, y mencionaban el nombre completo del afectado. Además, el Sr Costeja defendía que el embargo al que fue sometido en su momento estaba completamente resuelto, la deuda satisfecha y la noticia carecía de relevancia en la actualidad.

La AEPD resuelve, por un lado, desestimando la reclamación en la medida que se refería a La Vanguardia, dado que la publicación en edición impresa que este medio había llevado a cabo estaba legalmente justificada y tenia por objeto dar máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores. Por otro lado, la AEPD estimó la reclamación contra Google Spain y Google Inc. al considerar que los gestores de motores de búsqueda están sometidos a la normativa en materia de protección de datos, ya que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información.

Contra esta resolución Google Spain y Google Inc. interponen recurso ante la Audiencia Nacional, que planteó una consulta de prejudicialidad ante el TJUE.

6.2 La consulta de prejudicialidad

En la consulta la Audiencia Nacional plantea tres temas a través de varias preguntas.

En primer lugar, se cuestiona que normativa es la aplicable, si la de la UE o la normativa estadounidense por ser el domicilio legal de la empresa Google Inc. EE. UU.

En segundo lugar, se plantea es si los motores de búsqueda que indexan información legítima deben tutelar y atender a los derechos de cancelación, rectificación u oposición de las personas titulares de los datos[117].

[117] formulan las siguientes preguntas:

1. En relación con la actividad del buscador de la empresa "Google" en internet, como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros,

Por último, se cuestiona el alcance del derecho al olvido y las facultades del afectado para impedir que la información sea indexada por un motor de búsqueda[118].

6.3 Respuesta del TJUE: Sentencia del Tribunal de Justicia de 13 de mayo de 2014[119]

Con relación a la pregunta sobre normativa aplicable, el TJUE estimó que bastaba que la empresa en cuestión tuviese una sucursal o una empresa filial (como es el caso con Google Spain) en alguno de los Estados Miembros para aplicarse la normativa comunitaria.

Respecto al segundo tema, el TJUE determinó que las autoridades administrativas (AEPD en este caso) o judiciales tienen poder de control y competencias para ordenar a las empresas gestoras de los motores de búsqueda eliminar información de las listas de resultados obtenidos al buscar el nombre de una persona.

Los motores de búsqueda tienen la obligación de eliminar de sus resultados a partir del nombre de una persona los enlaces a páginas de terceros que contengan información relacionada con dicha persona. En este sentido, el TJUE sostiene que las obligaciones

---

indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos" contenido en el art. 2.b de la Directiva 95/46/CE?.

2. ¿Debe interpretarse el artículo 2.d) de la Directiva 95/46/CE, en el sentido de considerar que la empresa que gestiona el buscador "Google" es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?
3. ¿Puede la autoridad nacional de control de datos (en este caso la Agencia Española de Protección de Datos), tutelando los derechos contenidos en el art. 12.b) y14.a) de la Directiva 95/46/CE, requerir directamente al buscador de la empresa "Google" para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información?
4. ¿se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene los datos personales se haya publicado lícitamente por terceros y se mantenga en la página web de origen?

[118] ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la [Directiva 95/46] comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?

[119] Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014. Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. [consulta en línea] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62012CJ0131 [último acceso: 10 jun. 2023]

comunitarias[120] relacionadas con la protección y el tratamiento de datos suponen otorgar una serie de derechos a las personas titulares de estos datos, en particular en este caso, derecho a solicitar su rectificación o incluso oponerse a su publicación.

A razón del tercer tema planteado, sobre de la posibilidad de que el afectado exija al gestor de un motor de búsqueda la eliminación de enlaces a paginas web que contengan información verídica sobre su persona, el TJUE dictaminó que es necesario estudiar si el interesado tiene derecho a que dicha información ya no este vinculada a su nombre en la lista de resultados obtenida mediante búsquedas con su nombre.

En virtud de los derechos reconocidos en los artículos 7 y 8 de la CDFUE, el interesado puede solicitar que la información en cuestión no este disponible para el público en general cuando realiza una búsqueda por su nombre. Estos derechos prevalecen sobre el interés económico del motor de búsqueda y también sobre el interés del público en acceder a dicha información al realizar búsquedas en internet con el nombre de la persona en cuestión. Sin embargo, existen supuestos en los que la injerencia a estos derechos podría estar justificada por el interés predominante del público en acceder a la información tratada, especialmente si el interesado desempeña un papel relevante en la vida pública. Es decir, si hay razones específicas que justifiquen la importancia del acceso a dicha información por parte del público, la protección de los derechos del interesado puede ceder ante ese interés preponderante.

6.4 Conclusiones sobre el fallo del TJUE

De la respuesta a la consulta jurisdiccional podemos concluir lo siguiente:

1. Las empresas que establezcan una filial o sucursal, como Google Spain, se encuentran sometidas a la normativa comunitaria con independencia de su domicilio legal.
2. Los motores de búsqueda llevan a cabo una labor consistente en hallar información publicada en internet por terceros. Esta información es indexada y puesta disposición de los usuarios de internet. Por lo tanto, los motores de búsqueda como Google llevan a cabo un tratamiento de datos y son responsables de los datos que indexan y exponen al público.

[120] según lo establecido en el artículo 25 de la Directiva 95/46/CE.

3. Hilando con lo anterior, los motores de búsqueda son responsables y están obligados a eliminar los vínculos a paginas publicadas por terceros que contengan información perjudicial sobre una persona o la misma no se corresponda con la situación actual. Por lo que los ciudadanos tenemos derecho a controlar los resultados que un buscador ofrece a partir de nuestro nombre, puesto que estos afectan directamente a nuestra privacidad.
4. Si bien el afectado tiene este derecho, se ha de examinar cada caso concreto, pues el derecho al olvido cederá ante la existencia de un interés predominante por parte de público como ocurre en los supuestos en los que el interesado participe o haya participado en la vida pública. Es decir, el derecho al olvido tiene como contra la libertad de expresión y el interés público, y, por tanto, deberá ponderarse en cada caso concreto.
5. El fallo del TJUE da la razón al Sr. Costeja obligando a Google a retirar las referencias al embargo de sus bienes, el cual se ya realizó y en consecuencia su deuda con la Seguridad Social ya estaba satisfecha.

6.5 Efecto adverso del derecho al olvido

En el presente caso el Sr. Costeja pretendía que al introducir su nombre en un buscador en internet no apareciese información agravante hacia su persona, no quería que se diera a conocer al público que tuvo una deuda con la Seguridad Social y que para satisfacerla sus bienes fueron objeto de un embargo.

Si bien el TJUE le otorgó la razón, luego de la publicación de la sentencia las búsquedas de su nombre se multiplicaron, el caso se volvió mediático y aún mas gente conocía su condición de moroso. El Sr. Costeja trataba de evitar que se conociese su condición de moroso y el efecto de la sentencia fue el contrario, el caso gano popularidad y mayor atención del público.

Esta consecuencia se conoce como El efecto Streisand[121] y hace referencia a las repercusiones de publicidad que surgen en Internet cuando se intenta eliminar o

[121] El nombre se debe a un incidente ocurrido en 2003 con la actriz y cantante Barbara Streinsad, quien denunció al fotógrafo Kenneth Adelman y la página de fotografías pictopia.com por unas fotografías publicadas de su la casa de la actriz. El efecto fue contraproducente, la noticia se volvió viral y lo que en principio fue un intento de encubrir su casa, termino por convertirse en una de las casas mas conocidas de EE. UU.

suprimir cierto contenido o datos, pero en lugar de lograrlo, se genera un efecto contrario a la censura. En consecuencia, la información en cuestión recibe una mayor atención y difusión de la que hubiera tenido si no se hubiera intentado ocultar o eliminar.

En el caso del Sr. Costeja, basta con escribir su nombre en Google para darnos cuenta de este efecto. El buscador nos arroja 42.200 resultados, siendo uno de los primeros un articulo de un blog titulado "la inolvidable historia del embargo al moroso Mario Costeja González"[122], que para mas inri está disponible en múltiples idiomas.

Pareciera pues que el esfuerzo del Sr. Costeja ha sido en vano, que no existe realmente un derecho al olvido en internet y que todo cede ante afirmaciones altisonantes del tipo "internet nunca olvida" o "todo queda en la nube". Sin embargo, esto no es así.

La sentencia del TJUE es un hito jurídico de gran relevancia en el ámbito de la privacidad y la protección de datos, que marca el inicio del derecho al olvido en el viejo continente. Supuso un antes y un después, pues hace a los motores de búsqueda responsables de la información que indexan y otorga a los ciudadanos un procedimiento de solicitud de retirada de resultados. Cualquier persona puede solicitar la retirada de determinados resultados de búsqueda a través de un formulario que deben facilitar las empresas de motores de búsqueda[123]. Además, la sentencia supuso que el GT29 elaborase unas directrices sobre la ejecución de la sentencia[124].

Por lo que podemos concluir que desde 2014 los ciudadanos pueden acogerse al Derecho al Olvido para desindexar enlaces de los motores de búsqueda. Esta resolución del TJUE ha servido de punto de partida para otros casos[125] de publicaciones con

[122] Disponible en línea en https://derechoaleer.org/blog/2014/05/la-inolvidable-historia-del-embargo-al-moroso-mario-costeja-gonzalez-ocurrida-en-1998.html [último acceso: 10 jun. 2023]

[123] En el caso de Google se puede consultar como funciona este procedimiento de retirada de información en el siguiente enlace https://support.google.com/transparencyreport/answer/7347822?hl=es#zippy= [último acceso: 10 jun. 2023]

[124] Disponibles en https://ec.europa.eu/newsroom/article29/items/667236/en [último acceso: 10 jun. 2023]

[125] Como por ejemplo el enfrentamiento entre el pianista Dejan Lazić vs. *The Washington Post*. Un resumen de este caso disponible en https://derechodeolvido.com/lazic-vs-the-washington-post/ [último acceso: 10 jun. 2023]

contenido, difamatorio, obsoleto y no relevante. Si bien el indeseado efecto Streinsad sigue presente, la colaboración de las empresas responsables de los motores de búsqueda y el número de procesos administrativos y jurisdiccionales se encargarán de reducir la cantidad de noticias y publicaciones, dando lugar a un verdadero derecho al olvido y, en definitiva, otorgando al ciudadano una verdadera protección de sus datos.

7. CONCLUSIONES

I. La irrupción de internet ha generado una profunda transformación en nuestra sociedad, alterando nuestros patrones de consumo y nuestras formas de interacción. Internet ha revolucionado la forma en que accedemos a la información, consumimos bienes y servicios, y nos comunicamos con los demás. Esta revolución digital ha derribado las barreras geográficas y ha facilitado la conexión global, permitiendo un intercambio de ideas y conocimientos sin precedentes. No obstante, también ha planteado nuevos desafíos jurídicos relacionados con la privacidad, la seguridad de los datos y la protección de los derechos individuales de los usuarios. Es esencial que el marco jurídico se adapte a los cambios y desafíos que presenta la era digital. Las leyes deben abordar de manera efectiva los problemas asociados con el uso indebido de datos personales y la difusión de contenido ilegal o dañino en la red. Además, es necesario concienciar a la ciudadanía sobre los riesgos que conlleva el uso de internet.

II. Para aprovechar plenamente los beneficios de esta tecnología y mitigar sus impactos negativos, es imprescindible establecer un marco jurídico adecuado que aborde los desafíos emergentes y proteja la privacidad de los individuos en el entorno digital. El mandato del artículo 18.4 de la Constitución Española revela la visión anticipatoria de nuestros constitucionalistas en relación con estas amenazas. La evolución normativa en materia de protección de datos en España, impulsada por el mandato constitucional y los compromisos comunitarios, ha culminado en la legislación actual: el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). El RGPD, como

marco legal de la Unión Europea, establece principios y normas para la protección de los datos personales, promoviendo la privacidad y el control sobre la información personal. Por su parte, la LOPDGDD complementa y desarrolla el RGPD en el ámbito nacional, estableciendo disposiciones específicas para garantizar los derechos digitales de los ciudadanos españoles.

Estas normativas se basan en dos pilares fundamentales: el consentimiento del usuario y los derechos ARSLOP (Acceso, Rectificación, Supresión, Limitación, Oposición y Portabilidad) que brindan a las personas el control sobre sus datos y les permiten ejercer sus derechos en relación con su privacidad y protección de datos.

III. El consentimiento del usuario desempeña un papel crucial en el ámbito de la protección de datos, especialmente en lo que respecta a la aceptación de cookies en los sitios web. Las cookies son pequeños archivos de texto que se almacenan en los dispositivos de los usuarios y recopilan información sobre su actividad en línea. Pueden ser utilizadas para diversos fines, como el seguimiento de preferencias, personalización de contenido y publicidad dirigida. El RGPD establece que la recopilación y el uso de datos personales a través de cookies requieren otorgar el consentimiento de manera libre, específica, informada e inequívoca. Esto implica que los usuarios deben ser plenamente conscientes de qué cookies se utilizarán, con qué fines y por quién, antes de dar su consentimiento. Además, deben tener la opción de aceptar o rechazar las cookies de forma granular, es decir, seleccionando qué tipos de cookies desean permitir. Los sitios web deben proporcionar una clara y comprensible política de cookies que detalle la información relevante sobre las cookies utilizadas y brinde instrucciones claras sobre cómo administrar las preferencias de cookies. El RGPD también destaca que el consentimiento debe ser revocable en cualquier momento, lo que significa que los usuarios deben tener la posibilidad de retirar su consentimiento de manera fácil y accesible.

IV. Pese a que la legislación vigente mencione la claridad y la accesibilidad como puntos clave a la hora de consentir cookies, a menudo, las políticas de privacidad y las notificaciones de cookies son extensas, complejas y redactadas en un lenguaje técnico y legal que resulta difícil de entender para la mayoría de los usuarios.

Esta falta de comprensión puede llevar a que los usuarios acepten cookies sin un conocimiento adecuado de qué datos se recopilan, cómo se utilizan y con qué fines.

Además, a menudo se presentan en ventanas emergentes o banners que los usuarios, abrumados, tienden a aceptar rápidamente sin leer detenidamente el contenido. Esta falta de comprensión resulta problemática, ya que los usuarios pueden estar cediendo involuntariamente su privacidad y permitiendo el uso de sus datos personales de formas que no desean o comprenden completamente. Existe un desequilibrio en el poder y el conocimiento entre los usuarios y las empresas que recopilan los datos. La falta de opciones claras y sencillas para administrar las preferencias de cookies también contribuye a esta situación. A menudo, los usuarios solo se enfrentan a la opción de aceptar todas las cookies o rechazarlas por completo, sin la capacidad de seleccionar qué tipos de cookies desean permitir. Esto puede generar una sensación de falta de control y llevar a los usuarios a aceptar todas las cookies por conveniencia o porque desconocen las implicaciones reales.

Es fundamental que las políticas de privacidad y las notificaciones de cookies sean redactadas de manera clara y comprensible, utilizando un lenguaje sencillo y evitando el uso de terminología técnica y legal compleja. Además, los sitios web deberían ofrecer opciones de consentimiento granular y proporcionar información más concisa y fácil de digerir sobre las cookies utilizadas, los datos recopilados y los fines específicos de su uso.

V. En relación con los derechos ARSLOP, particularmente los derechos de supresión y rectificación conocidos como el derecho al olvido, analizados en este trabajo a través del caso Mario Costeja vs Google, podemos concluir que los ciudadanos de la Unión Europea tienen la posibilidad de ejercer este derecho para solicitar la desindexación de enlaces en los resultados de los motores de búsqueda. Es importante destacar que el derecho al olvido no es absoluto y debe equilibrarse con otros derechos fundamentales, como la libertad de expresión y el acceso a la información. Los motores de búsqueda deben evaluar cuidadosamente cada solicitud y considerar los intereses en juego para tomar decisiones equilibradas y proporcionadas. De esta manera, el derecho al olvido se aplica específicamente a publicaciones que contengan contenido difamatorio, obsoleto o no relevante.

Aunque el efecto Streisand aún persiste, es decir, la posibilidad de que la atención se amplifique a raíz de los intentos de ocultar información, la colaboración entre las autoridades y las empresas responsables de los motores de búsqueda puede

contribuir a reducir este efecto. Esta colaboración debe conducir a la eliminación de noticias y publicaciones indeseadas, lo que permitirá a los ciudadanos ejercer su derecho al olvido de manera más efectiva.

BIBLIOGRAFÍA

ALBADALEJO, M. (2013). *Derecho civil I. Introducción y parte general*. Madrid: Edisofer.

BARRANCO FRAGOSOM, Ricardo, *¿Qué es Big Data?*, México, 2012, [en línea] http://www.criiasupr.org/multimedia/documents/Que%20es%20Big%20Data.pdf

BLENNER, S. *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*. March 8: Vol 315, No. 10, 2016. Disponible en*:* http://jama.jamanetwork.com/article.aspx?articleid=2499265.

CABALLERO R, MARTÍN E. *Las bases de Big Data*. Catarata, Madrid 2015

CORRIPIO GIL-DELGADO, M.R. (1999). *Los contratos informáticos. El deber de información precontractual.* Madrid: Publicaciones de la Universidad Pontificia Comillas

COTINO HUESO, Lorenzo. *Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los "blogs"). [in: AA.VV. Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías.* Lorenzo Cotino Hueso (Dir.), PUV (Publicaciones Universidad de Valencia) Valencia: 2011.

DÍEZ-PICAZO, L. *Fundamentos del derecho civil patrimonial I. Introducción. Teoría del contrato*. Pamplona: Aranzadi, Thomson Reuters, Civitas, 2007.

GARCÍA MEXÍA, P. *El Derecho de Internet.* Tirant lo Blanch, Valencia: 2005.

GARCÍA MEXÍA, P., "Internet y protección de datos. Los desafíos de la evolución digital", *Diario La Ley*, año XXXII, No. 7577, 25 de febrero de 2011

GONZÁLEZ, José Luis y SÁNCHEZ, Marisol. *Autopistas de la información e internet (Tecnología, Servicios, Peajes y normas de navegación).* Universidad de Extremadura, Cáceres: 1998

IAB ESPAÑA, estudio de redes sociales 2022 [consulta en línea] https://iabspain.es/estudio/estudio-de-redes-sociales-2022/

INE, Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los Hogares. Año 2022. [consulta en línea] https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608

JEFFREY D. Sach, *las edades de la globalización*, DEUSTO S.A. ediciones, Bilbao, 2021

LUCAS MURILLO DE LA CUEVA, P. *La primera jurisprudencia sobre el derecho a la autodeterminación informativa.* Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, n.º 1, 2003.

MATÉ-JIMENEZ C*. Big Data. Un nuevo paradigma de análisis de datos.* Anales de mecánica y electricidad, Vol. 91, Fascículo 6, 2014

MAYER-SCHÖNBERGER, V y CUKIER, K. *Big Data. La revolución de los datos masivos*. Madrid: Turnen Noema, 2015.

NEGROPONTE, Nicholas. *El mundo digital.* Ediciones B, Barcelona: 1996

OBSERVATORIO DE BIOÉTICA Y DERECHO, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Universidad de Barcelona, 2015. Disponible

en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

PARRA, Sergio. *Términos y condiciones web*. Yorokobu. 30 de septiembre de 2016. Blog accesible en: www.yorokobu.es/terminos-y-condiciones/18/?offset=29.

POZZI, S., "Cuando el televisor espía" en *El País,* 28 de julio de 2015, [en línea], http://economia.elpais.com/economia/2015/07/27/actualidad/1438001658_976873.html

RAMÓN FERNÁNDEZ, F. *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías.* Lorenzo Cotino Hueso (Editor), PUV (Publicaciones de la Universidad de Valencia) Valencia: 2011

RAMONET I. *El imperio de la vigilancia*. Clave Intelectual, 2016 [disponible en] https://www.eldiplo.org/wpcontent/uploads/2018/files/7114/6040/1796/INTRODUCCION.pdf

RAMONET I. *Google lo sabe todo de ti*. LE MONDE Diplomatique, año XX N.º 224, febrero 2016. [disponible en] http://www.ignaciodarnaude.com/textos_diversos/Filpo,Google%20lo%20sabe%20todo%20de%20ti.pdf

RAMONET, I. *Google lo sabe todo de ti.* LE MONDE Diplomatique, año XX N.º 224, febrero 2016 y MOUZO, J. *La medicina montada en una app. Las aplicaciones móviles de salud transforman la relación médico-paciente.* El País, domingo 15 de noviembre de 2015.

REBOLLO DELGADO, L. (2017). *Contratación electrónica y protección de los consumidores —una visión panorámica—*. Madrid: Reus.

SALAS J. *¿Dónde acaban los datos privados que recogen las "apps" de salud?* El País, Ciencia. 8 de marzo de 2016. Disponible online: http://elpais.com/elpais/2016/03/07/ciencia/1457369646_082762.html

SÁNCHEZ CALERO, F.J. (2016). *Curso de derecho civil II. Derecho de obligaciones, contratos y responsabilidad por hechos ilícitos*. Valencia: Tirant lo Blanch, 145

SOTO, Yasmina. *Datos masivos con privacidad y no contra privacidad.* Revista de Bioética y Derecho. [disponible en línea en] https://scielo.isciii.es/pdf/bioetica/n40/1886-5887-bioetica-40-00101.pdf

TORNABENE, I., "privacidad e intimidad: la protección legal de la información personal en la República Argentina", en Amoroso Fernández, Y., (dir.), *Género, Código de Juventud: construir sociedades mas justas e inclusivas,* Unión Nacional de Juristas de Cuba, 2014.