universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2020 /2021

EL DERECHO DE AUTODETERMINACIÓN INFORMATIVA ANTE LOS MECANISMOS DE SEGUIMIENTO Y CONTROL PRESENTES EN EL ENTORNO DIGITAL

THE RIGHT TO INFORMATIONAL SELF-DETERMINATION IN THE FACE OF TRACKING AND CONTROL MECHANISMS PRESENT IN THE DIGITAL ENVIRONMENT

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR/A: D. SANTIAGO GRIGERA

TUTOR/A: D. SALVADOR TARODO SORIA

ÍNDICE

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
CCPA	*California Consumer Privacy Act*
CEDH	Carta Europea de Derechos Humanos
CNIL	*Commission Nationale Informatique et Libertés*
EEUU	Estados Unidos de América
e- privacy	Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)
GT 29	Grupo de Trabajo del artículo 29
LSSI/LSSICE	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
ONTSI	Observatorio Nacional de las Telecomunicaciones y de la sociedad de la Información.
TFUE	Tratado de Funcionamiento de la Unión Europea
STC	Sentencia del Tribunal Constitucional

RESUMEN

En la actualidad transitamos una época de avances tecnológicos que superan el nivel de entendimiento y asimilación humana. De esta manera, se pone en evidencia que la demorada respuesta normativa no siempre resulta eficaz ante los vertiginosos cambios generados por la transformación digital.

En este escenario complejo y globalizado, abundan las normas, pero se carece de armonización a nivel internacional. Esta fragmentación normativa presenta desafíos en el control y cumplimiento legal.

El usuario, interactúa con tecnologías que no siempre comprende. Además, tampoco se le informa correctamente acerca de los efectos e implicaciones de la utilización de los dispositivos conectados a Internet y programas de los que se vale en su vida cotidiana.

Ciertas tecnologías pueden tener repercusiones en los derechos y libertades de los usuarios.

Por ello, en el presente trabajo se elabora una sistematización de tecnologías, técnicas y fenómenos presentes en el entorno digital, que tienen injerencias en el derecho fundamental de autodeterminación informativa. Se explicará en lenguaje común de qué se tratan y también se señalarán, algunos aspectos legales que entrañan su utilización.

PALABRAS CLAVE

Libertad informática, autodeterminación informativa, tecnologías de seguimiento y control, privacidad, protección de datos, libertades, derechos fundamentales, principios, protección de datos desde el diseño y por defecto.

ABSTRACT

Nowadays we are going through a time of technological advances that exceed the level of human understanding and assimilation. Thereby, it is evident that the delayed regulatory response is not always effective due to the vertiginous changes generated by the digital transformation.

In this complex and globalized scenario, norms abound but international harmonization is lacking. This regulatory fragmentation presents challenges in legal compliance and enforcement.

The user interacts with technologies that he does not always understand. In addition, it is not properly informed about the effects and implications of using internet connected devices and programs in daily life.

Certain technologies may have an impact on the rights and freedoms of users.

For this reason, the present work elaborates a systematization of technologies, techniques and phenomena existing in the digital environment, which interfere with the fundamental right of informational self determination. It will be explained in common language what they are about and will also point out some legal aspects that their use entails.

KEY WORDS

Computer freedom, informational self determination, monitoring and control technologies, privacy, data protection, freedoms, fundamental rights, principles, data protection by design and by default.

OBJETO DEL TRABAJO

La presente investigación comenzó con el cuestionamiento de las denominadas *cookies.* Surgieron algunas inquietudes al respecto: ¿De qué se tratan estos avisos que no nos permiten navegar libremente por internet? ¿Qué las hace tan especiales? ¿Son programas espías? ¿Qué implicaciones tienen para el usuario, para sus derechos y qué consecuencias tienen para las empresas y para la economía en general? A medida que se avanzó en el estudio del tema se advirtió que, así como las *cookies* no resultan intrascendentes para los derechos de los usuarios, existen otras técnicas, fenómenos y tecnologías que no deben pasar inadvertidas atendiendo a su afectación sobre algunos derechos fundamentales.

El objeto del presente estudio consiste en analizar algunas de esas diversas tecnologías, fenómenos y técnicas que se encuentran presentes en el entorno digital actual, darlas a conocer, describirlas y determinar si pueden afectar el derecho de libertad informática. Se propone buscar si ostentan patrones y características similares entre sí, identificarlos y en su caso, explicar si incide en el libre ejercicio del derecho fundamental mencionado. Se describirán diversas características para dar a conocer de su existencia y que sirva al lector para identificar circunstancias análogas. Para ello, se procederá a sistematizarlas, analizarlas desde un punto de vista técnico para después determinar sus implicaciones jurídicas desde un enfoque del derecho de protección de datos personales.

Además, se efectuarán distintas referencias normativas, doctrinales, artículos académicos y antecedentes jurisprudenciales que abordan las distintas temáticas, que ayudarán a entender las posturas, opiniones, criterios y el derecho que las regula.

El presente estudio surge porque la transformación digital que atraviesa la realidad supone avances sobre dimensiones que se encuentran legalmente protegidas, pero no todos son conscientes de ello. Por eso, los usuarios y ciudadanos deben estar preparados para discernir si las tecnologías de las que se valen en su vida cotidiana pueden interferir en sus derechos y libertades y tomar decisiones informadas, razonadas y conscientes sobre ellas. Se espera que el presente estudio valga como punto de partida a los fines de que el lector pueda analizar críticamente otras tecnologías actuales, emergentes y aquellas que se desarrollen en el futuro. Por último, se invita al cuestionamiento del diseño, funcionamiento e implicaciones en los derechos fundamentales de las tecnologías que se utilizan. La concientización acerca del

desarrollo y uso de tecnologías que garanticen el respeto a la dignidad, derechos y libertades humanas, contribuirán al progreso tecnológico adecuado y sostenible en favor y no en perjuicio de las futuras generaciones.

METODOLOGÍA

El trabajo presenta una metodología mixta y compleja.

Se aborda el objeto de la investigación desde un enfoque técnico y jurídico. Ello ha denotado un esfuerzo por realizar un estudio descriptivo y explicativo en lenguaje común de cuestiones técnicas con el cometido de efectuar un análisis jurídico de diversas implicaciones partiendo de dos perspectivas metodológicas diferentes.

Se han tomado cuestiones de la ingeniería aplicada y asimismo, se ha adoptado dogmática jurídica. Se han tenido en cuenta diversas fuentes normativas, algunas vigentes y otras no, jurisprudencia nacional e internacional, doctrina jurídica y bibliografía especializada.

Luego de la lectura de diversos libros y artículos relacionados con la privacidad y protección de datos, mientras que se anunciaban cambios y novedades en diversos institutos y normas, se identificaron algunos fenómenos y tecnologías que presentaban similitudes con relevancia en los derechos y libertades. Como se encontraban diseminados en distintas fuentes bibliográficas, se decidió sistematizarlas en el presente trabajo.

Después de definir el área de estudio y los temas se procedió a identificar el instituto jurídico más comprometido, siendo este el derecho fundamental de libertad informática.

Se procedió a elegir al tutor y ante el planteo de la problemática, luego del visto bueno, se consultó bibliografía recomendada y se recolectó información de distintas fuentes Se consultaron manuales jurídicos, compendios de artículos monográficos académicos, libros, revistas jurídicas, trabajos finales de Máster, y diversos recursos electrónicos de carácter jurídico como *dialnet*, aprovechando los libros de las distintas bibliotecas de las facultades de la Universidad de León, como también libros disponibles en línea.

Tras una dedicada lectura de las diversas fuentes bibliográficas, se formó una opinión propia y crítica del objeto de estudio. Tuvieron lugar reuniones e intercambios de correos electrónicos con el tutor a los fines de realizar las adaptaciones, sugerencias y correcciones del trabajo hasta llegar a la versión final.

I. INTRODUCCIÓN

"La libertad, Sancho, es uno de los más preciosos dones que a los hombres dieron los cielos; con ella no pueden igualarse los tesoros que encierra la tierra ni el mar encubre; por la libertad así como por la honra se puede y debe aventurar la vida [...]."

Don Quijote de La Mancha[1]

En la actualidad el desarrollo tecnológico imperante desafía los derechos y libertades de las personas. Pérez Luño advirtió de la importancia de la libertad informática ante estos avances y amenazas.[2]

La proliferación de datos personales y sobre todo sensibles generados en el último tiempo, han sido y siguen siendo recolectados en ingentes cantidades, de diversas maneras, por todo tipo de actores y sometidos a los más variados tratamientos.

Un proyecto de reglamento europeo cuyo pseudónimo es mundialmente conocido como "*e-privacy*", continúa siendo objeto de diversas deliberaciones, debates y revisiones dados los distintos intereses que resisten hasta la fecha su aprobación. La norma cuenta con contenidos y previsiones que conciernen derechos considerados fundamentales de las personas con implicaciones en sectores públicos y privados.

En un contexto global convulsionado en materia de privacidad, distintos países sancionaron leyes al respecto en los últimos tiempos. Brasil, Uruguay, Ecuador y Estados Unidos incorporaron nuevas legislaciones en materia de protección de datos y otros, como son los casos de Argentina, Colombia y Chile, cuentan con proyectos de reformas normativas en ciernes.

---

[1] CERVANTES DE, Miguel. *Don Quijote de la Mancha*. Edición Alberto Blecua y Andrés Pozo. Colección Austral. Espasa. Madrid, España.1998. Capítulo LVIII. P. 1028.

[2] PÉREZ LUÑO, Antonio Enrique. Las generaciones de los derechos humanos ante el desafío posthumanista. En: Tomás de la Quadra-Salcedo-José Luis Piñar Mañas. *Sociedad Digital y Derecho.* Primera edición. Madrid, España: Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. 2018. Pp. 137-155. P. 147. Al respecto, ha sostenido: "Es sabido que la etapa actual de desarrollo tecnológico, junto a avances y progresos indiscutibles, ha generado nuevos fenómenos de agresión a los derechos y libertades. En esas coordenadas se está iniciando un movimiento de la doctrina jurídica y de la jurisprudencia de los países con mayor grado de desarrollo tecnológico tendente al reconocimiento del derecho a la libertad informática y a la facultad de autodeterminación en la esfera informativa. En una sociedad como la que nos toca vivir en la que la información es poder y en la que ese poder se hace decisivo cuando, en virtud de la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario."

En una época de tecnologías emergentes y de pluralidad normativa, no es difícil advertir el desafío que supone para las personas reivindicar su derecho fundamental de libertad informática en un entorno digital globalizado.

El presente trabajo, nace de la inquietud y cuestionamiento de ciertas tecnologías y técnicas utilizadas en el entorno digital que afectan y en ocasiones dificultan el ejercicio del derecho de libertad informática por parte de los usuarios.

Concretamente, se intentará ilustrar cómo a pesar de que el derecho de libertad informática se encuentra vigente desde prácticamente el surgimiento de Internet, existen fenómenos, técnicas y tecnologías que afectan a su ejercicio y efectividad. Si bien este derecho se erigió como un límite a la informática, se advertirá cómo en la actualidad, la informática acaba por limitar la libertad y otros derechos fundamentales de los usuarios.

A la época que se redacta el presente trabajo, la situación sanitaria causada por la Covid-19 no ha sido superada y los riesgos e impactos a los derechos y libertades se han agravado. Se han suscitado cambios radicales a nivel global ocasionando impactos de diversa naturaleza. Los desesperados intentos de los distintos gobiernos por contener la propagación del virus durante los últimos tiempos junto con los esfuerzos de las organizaciones para adaptarse a la coyuntura, llevaron a la adopción e implementación intempestiva de todo tipo de medidas que tuvieron impactos relevantes en la manera de disfrutar el entretenimiento, trabajar, aprender, circular, en fin, de vivir.

II. TECNOLOGÍAS, FENÓMENOS Y TÉCNICAS QUE AFECTAN LA LIBERTAD INFORMÁTICA

"When people are unable to participate in the maintenance and use of their information, they can be rendered powerless."

Daniel J. Solove.[3]

En la actualidad, la tecnología constituye un inmenso cauce de desarrollo de la condición humana, en todas sus esferas. También, supone la aparición de riesgos y amenazas para la libertad.[4] En el presente capítulo, se indicarán y analizarán distintas tecnologías de seguimiento y control de los usuarios y dispositivos, que no siempre son perceptibles o se informan debidamente, ni se conocen en detalle sus consecuencias.

1. TECNOLOGÍAS DE SEGUIMIENTO

"El capitalismo de vigilancia no es una tecnología es una lógica que impregna la tecnología y que la pone en acción."

Shoshana ZUBOFF[5]

1.1. COOKIES

Entre los temas que han tenido un amplio debate en los últimos años y han despertado la curiosidad de los usuarios, la preocupación de los Estados y el interés de las empresas, se encuentran las *cookies*. Aunque hayan pasado inadvertidas la mayor parte de su existencia, tal vez por la inocencia de su nombre, no se puede ignorar que los usuarios han podido apreciar en las diversas páginas web un aumento exponencial de distintos avisos, anuncios y muros de información al respecto que han afectado su experiencia al navegar por Internet. La mayoría de los Estados las han regulado, existiendo proyectos de normas como el referido Reglamento *"e-Privacy"* al que se aludirá más adelante, que las contempla con detenimiento. Las empresas en la actualidad pueden obtener beneficios de los servicios que prestan a la sociedad de la información y tanto las

[3] SOLOVE, Daniel J. *Understanding Privacy*. Primera edición. Estados Unidos de América. Harvard University Press. 2008. P.135.

[4] PÉREZ LUÑO, Antonio E. Las libertades en la era de Internet. En: Francisco Javier ANSUÁTEGUI ROIG. *El derecho en red. Estudio en Homenaje al profesor Mario G:Losano.* Primera edición. Ed. Dykinson. Madrid. 2006. Capítulo: pp. 365-400. P.396 y 397.

[5] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia*. *La lucha por un futuro humano frente a las nuevas fronteras del poder*. SANTOS MOSQUERA, Alvino.Trad. Primera edición. Barcelona, España. Editorial Planeta. 2020. P. 30.

cookies como tecnologías afines son fundamentales para los diversos modelos de negocios basados en datos.

En este sentido, existen peligros al uso generalizado de estas herramientas digitales. La instalación y uso de *cookies* de rastreo permiten a la plataforma conocer la actividad del sujeto tanto dentro como fuera de la misma, sin advertencia alguna. Pueden detectar el lugar desde el que el interactor accede, el tiempo de conexión, el dispositivo de acceso, las páginas más visitadas, el número de *«clics»* realizados e infinidad de informaciones relativa a la navegación del usuario.[6] Aunque con frecuencia se refiera a *cookies* de manera genérica para denominar a distintas tecnologías de seguimiento, resulta propicio aclarar que no todas son *cookies* y no todas afectan a la intimidad de las personas.

Dependiendo del tipo de *cookie* de que se trate, puede tener diferentes implicaciones en los derechos fundamentales. En los próximos apartados se las conceptualizará, se abordará su origen y clasificación. Asimismo, se revelará cómo ciertas prácticas y programas comúnmente utilizados por los desarrolladores de estas tecnologías, han avanzado a lo largo del tiempo sin reparo sobre dimensiones que exceden sus propias fronteras. Se apreciará cómo en beneficio de sus intereses, han explotado durante años las vulnerabilidades de los usuarios aprovechando su ignorancia, inercia, desinterés, apuro, necesidad, entre otros; y éstos, no se han detenido a pensar ni cuestionar la existencia, diferencias, implicaciones y consecuencias de estos programas.

1.1.1 Concepto

Las *cookies* pueden definirse como *cualquier tipo de dispositivo de almacenamiento y recuperación de datos que se utilice en el equipo terminal de un usuario con la finalidad de almacenar información y recuperar la información ya almacenada [...]*[7]. Conforme se advierte, la definición de *Cookies* proporcionada por la AEPD, resulta ambigua. Se refiere a las *cookies* como un género. Puede ser cualquier dispositivo de almacenamiento y recuperación de datos. No se determina un dispositivo específico. Además, tiene que tener la finalidad de almacenar información y recuperar la información ya almacenada.

---

[6] NOAIN SÁNCHEZ, Amaya. *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*. Agencia Española de Protección de Datos. Boletín Oficial del Estado. Madrid. 2016. P.226. [en línea] [Fecha de consulta 28/04/2021] [https://www.aepd.es/sites/default/files/2019-10/la-proteccion-de-la-intimidad.pdf]

[7] Agencia Española de Protección de Datos. *Guía sobre el uso de las cookies.* [en línea][Fecha de consulta: 01/04/2021]. [https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf]. P.11.

No es extraño que exista cierta falta de claridad en la conceptualización de las *cookies*. La misma guía incluso refiere: *el artículo 22 de la LSSI y la presente guía se refieren a la utilización de* cookies *y tecnologías similares utilizadas (tales como* local shared objects *o* flash cookies, web beacons *o* bugs *, etc.) para almacenar y recuperar datos de un equipo terminal (por ejemplo, un ordenador, un teléfono móvil o una* tablet*) de una persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información. La citada norma también resulta de aplicación al empleo de técnicas de* fingerprinting*, es decir, a las técnicas de toma de la huella digital del dispositivo* [...][8].

Por su parte el RGPD también se refiere a las *cookies* en forma genérica en el considerando 30° surgiendo de su enunciado: *identificadores de sesión en forma de «cookies» u otros identificadores [...]*.

En el entorno digital, y específicamente en las normas es común referir a "*cookies* y tecnologías similares" lo que resulta al menos poco esclarecedor para el usuario. Se analizarán sólo algunas de estas tecnologías similares en razón de que la individualización a todas ellas, excedería los propósitos del trabajo.

1.1.2. Antecedentes de las cookies

Teniendo una noción de qué son las *cookies*, corresponde hacer mención a sus orígenes. Aunque en resumidas cuentas la historia de Internet se remonta a la década de 1960, surgiendo en entornos académicos y utilizada con propósitos militares para luego de abrirse al público a finales de 1980[9], Tim Berners Lee inventa la *World Wide Web* que no vio la luz sino hasta comienzos de la década de 1990.[10] En 1995, Lou Montulli, que trabajaba para *Netscape Communications Corporation*, inventó las *cookies* mientras trabajaba en la implementación de una manera de interactuar el navegador con un carrito de compras virtual. Conforme refiere Marta Peirano: *la idea era que la*

[8] Ibidem. P. 8.

[9] LEINER, Barry M., CERF, Vinton G. CLARK David D.,KAHN Robert E., KLEINROCK, Leonard, LYNCH Daniel C., POSTEL Jon, ROBERTS, Larry G., WOLFF, Stephen. *Breve historia de internet.* [en línea] [Fecha de consulta: 01/04/2021].[https://www.internetsociety.org/internet/history-internet/brief-history-internet/#]

[10] World Wide Web Fundation. *History of the Web.* [en línea] [Fecha de consulta: 01/04/2021].[https://webfoundation.org/about/vision/history-of-the-web/]

aplicación reconociera al usuario y recordara los distintos artículos que había en su cesta sin tener que guardar sus datos en el servidor de la tienda.[11]

En 1996 una empresa llamada *DoubleClick* comenzó a colocar *banners* en distintos sitios web que registraban a los usuarios que visitaban esas páginas. Además de identificarlos, se rastreaban las páginas que visitaban, los anuncios que miraban, los artículos que leían y los productos que compraban.[12] Resulta anecdótico que en el año 2007 *Google* adquiriera esa empresa y lo anunciara en una nota de prensa.[13] Esto porque desde unos años antes, *Google* ya contaba con herramientas de publicidad y seguimiento online como sus productos *AdWords* y *AdSense*. De esta manera fue conquistando los diferentes *blogs* y sitios web que incluían espacios de publicidad y colocaban una barra de su buscador como servicio: *Cada anuncio y cada buscador de Google es registrado por las cookies de Google, que ahora pueden seguir al usuario por millones de sitios y saber quién es, qué lee, dónde pincha, cuanto se queda y dónde va después.*[14]

Como todo en Internet, los distintos tipos de *cookies*, tanto las "técnicamente necesarias" como las de seguimiento y otras innominadas, fueron adoptadas masivamente por los sitios web sin que los usuarios hayan tenido la posibilidad de conocer y evaluar el funcionamiento y consecuencias de estos mecanismos.

1.1.3. Clasificación

Las *cookies* se clasifican según ciertos parámetros, de acuerdo a: la entidad que las gestione, su finalidad, y el plazo de tiempo que permanecen activadas.

Respecto de la entidad que las gestione, se distinguen las *cookies* propias y las *cookies* de terceros. Respecto de las primeras, *son aquellas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario […]*[15]. Las *cookies* de terceros *son aquellas*

---

[11] PEIRANO, Marta. *El enemigo conoce el sistema. Manipulación de ideas, personas e influencias después de la economía de la atención*. Primera edición. Barcelona. Penguin Random House Grupo Editorial. 2019. P.210.
[12] Ibidem. P. 210.
[13] Google Press. *Google to acquire DoubleClick.* [en línea] [Fecha de consulta: 01/04/2021]. [https://googlepress.blogspot.com/2007/04/google-to-acquire-doubleclick_13.html]
[14] PEIRANO, Marta. *El enemigo conoce el sistema...*, cit., p 211.
[15] Agencia Española de Protección de Datos. *Guía sobre el uso de las cookies...*, cit., p 11.

que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las cookies *[...].*[16]

El parámetro para diferenciar si pertenecen a uno u otro tipo radica en identificar quién es el que se beneficia de la información recogida o el que explota dicha información. Sirve la aclaración porque puede suceder que el que instale la *cookie* sea el editor pero que la información recolectada sea gestionada por un tercero para mejorar sus servicios o con fines publicitarios.

Sobre su finalidad, las *cookies* se pueden clasificar en: *cookies* técnicas; preferencia o personalización; analítica o medición y de publicidad comportamental. Las técnicas *son aquéllas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan, incluyendo aquellas que el editor utiliza para permitir la gestión y operativa de la página web y habilitar sus funciones y servicios […]*[17]. Las de preferencia o personalización *son aquéllas que permiten recordar información para que el usuario acceda al servicio con determinadas características que pueden diferenciar su experiencia de la de otros usuarios [...]*[18]. Las de analítica o medición *son aquellas que permiten al responsable de las mismas el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas, incluida la cuantificación de los impactos de los anuncios. La información recogida mediante este tipo de cookies se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.*[19] Las de publicidad comportamental *son aquellas que almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.*[20] En cuanto a éstas, son las más polémicas y las normas actuales sostienen la necesidad de consentimientos expresos dado que pueden suponer riesgos para la privacidad de los usuarios.

[16] Ibidem. P. 11.
[17] Ibidem. P. 11.
[18] Ibidem. P. 12.
[19] Ibidem. P. 12.
[20] Ibidem. P. 12.

Por último, considerando el plazo de tiempo que permanecen activadas se distinguen las de sesión y las persistentes. Las primeras, *son aquellas diseñadas para recabar y almacenar datos mientras el usuario accede a una página web. Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (por ejemplo, una lista de productos adquiridos) y desaparecen al terminar la sesión.*[21] Las persistentes, *son aquellas en las que los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años.*[22] A simple vista, resulta al menos cuestionable la temporalidad de *cookies* persistentes ya que podrían entrar en conflicto con ciertos principios como el de minimización de datos y de limitación de plazo de conservación.

No se puede continuar abordando este tema considerando a las *cookies* de manera genérica. Tampoco corresponde que no se las distinga. No todas deben ser miradas con suspicacia, ya que algunas se encuentran exentas de conflicto. Existen normas que han superado ciertas controversias existentes, como es el caso de las *cookies* técnicas. En el plano europeo, se prevé esta circunstancia en la Directiva 2000/31/CE[23]. En España, la LSSICE en el Artículo 22.2 último párrafo establece: *...no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario*.[24] El Grupo de protección de datos del artículo 29, conocido como "GT29", a través del dictamen 4/2012, interpretó qué tipo de *cookies* y tecnologías similares quedan exentas del requisito de consentimiento informado, sintetizándolas en las siguientes: *Cookies* de "entrada del usuario"; *Cookies* de autenticación o identificación de usuario (únicamente de sesión); *Cookies* de seguridad del usuario; *Cookies* de sesión de reproductor multimedia; *Cookies* de sesión para equilibrar la carga; *Cookies* de personalización de la interfaz de

[21] Ibidem. P. 13.
[22] Ibidem. P. 13.
[23] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). [en línea] [Fecha de consulta: 11/05/2021]. [https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295]
[24] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.[en línea] [Fecha de consulta: 02/04/2021].[https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758]

usuario y determinadas *cookies* de complemento para intercambiar contenidos sociales. Se entiende que éstas quedan exceptuadas de los extremos de consentimiento informado del artículo 22.2 LSSICE.[25]

El uso que se haga de las *cookies*, su pertinencia, la manera en que la información se presenta al usuario, la lealtad y respeto de sus preferencias en el tratamiento, marcarán su naturaleza benévola u hostil. En este sentido se ha dicho: *Las cookies, ya sean de navegador o de seguimiento, son fragmentos de programa necesarios para desarrollar muchas de las acciones que ejecutamos en Internet. Estos pequeños archivos de texto, a menudo encriptados, se ubican en el navegador del usuario, de manera que el sitio Web puede consultar la actividad previa del interactor, así como sus preferencias. Su pertinencia dependerá de que su uso esté justificado o no por la prestación del servicio.*[26]

A los fines prácticos se ha resumido la clasificación conforme el enfoque de la autoridad de protección de datos española. Sin perjuicio de ello, nada obsta que existan otros tipos y denominaciones de *cookies* que no se encuadren en las clasificaciones brindadas. De cualquier modo, el que instale, desarrolle y se valga de las mismas, deberá respetar el deber de información en honor al principio de transparencia para evitar infringir los derechos de los usuarios respetando el resto de los principios receptados por la legislación vigente. Estos conceptos son imprescindibles y volveremos a ellos constantemente en el presente trabajo.

1.2. FINGERPRINTING

"Privacy is threatened in ways that far exceed our comprehension and imagination."

Firmin DEBRABANDER[27]

Dentro de los términos asociados genéricamente a las *cookies* como "otras tecnologías de seguimiento" se encuentra el *fingerprint* o huella digital. Conforme surge de un estudio elaborado por la AEPD, en el dinámico entorno digital van surgiendo diversas técnicas de identificación y seguimiento de los dispositivos y usuarios a los fines del

[25] Grupo de protección de datos del artículo 29. *Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies.* [en línea] [Fecha de consulta: 02/04/2021]. [https://www.apda.ad/sites/default/files/2018-10/wp194_es.pdf].

[26] NOAIN SÁNCHEZ, Amaya. *La protección de la intimidad...*, cit., p. 312.

[27] DEBRABANDER, Firmin. *Life after privacy. Reclaiming democracy in a surveillance society.* Primera edición. Reino Unido. Cambridge University Press. 2020. P.36.

perfilamiento adecuado que han superado a las propias *cookies*. En el estudio se conceptualiza a la huella digital del dispositivo de la siguiente manera: *es una recopilación sistemática de información sobre un determinado dispositivo remoto con el objetivo de identificarlo, singularizarlo y de esa forma, poder hacer un seguimiento de la actividad del usuario del mismo [...].*[28]

Sirve para realizar una recopilación de información de los terminales que se conectan a los servidores y hacer un seguimiento de la navegación de los usuarios que lo utilizan. Las técnicas más avanzadas permiten registrar movimientos que realiza el usuario a través de la página web con el *mouse* con un nivel de detalle que detecta por donde se detiene y cuánto tiempo. De esta manera, se puede construir un perfil individualizado de los sujetos atento que habitualmente no se comparten los dispositivos.[29] La huella digital presenta algunas particularidades preocupantes relacionadas a la intimidad y privacidad de las personas.

Otro documento que aborda el tema de la huella digital es el elaborado por el Comité Europeo de Protección de Datos, el Dictamen 9/2014 sobre la aplicación de la Directiva 2002/58/CE a la huella digital de dispositivos.

Lo que resulta más alarmante es que aunque uno haya tomado sus cautelas para configurar sus preferencias sobre las *cookies* no puede evitar ser individualizado mediante otros dispositivos como la huella digital del dispositivo. *La realidad es, que el uso de las técnicas de huella digital permiten volver a asignar al mismo usuario la información vinculada al identificador de la* cookie *eliminada y no perder la trazabilidad sobre los datos de navegación del usuario o simplemente realizar el seguimiento en base únicamente a la huella digital. En conclusión, si a la vez que se genera una* cookie *de identidad se detecta y almacena su huella digital, en el caso de que el usuario borre las* cookies *en su navegador, éstas se pueden restituir utilizando la huella digital para reidentificar al usuario, por lo que el borrado de cookies no sería eficaz.*[30] Se puede apreciar que existen severos obstáculos para ejercer los derechos de protección de datos en las plataformas, resultando totalmente imposible para el usuario

[28] Agencia Española de Protección de Datos. *Estudio Fingerprinting o Huella digital del dispositivo.* P. 4. [en línea] [Fecha de consulta: 10/04/2021] [https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf]
[29] Ibidem. P. 4.
[30] Ibidem. P. 5.

el control y disposición de la información que genera como consecuencia de su interacción con sus dispositivos con acceso a Internet. Mientras tanto, el derecho a la intimidad y privacidad es socavado sin solución de continuidad.

1.3. PIXEL DE SEGUIMIENTO

Existen otras técnicas y tecnologías a los fines de individualizar personas, dispositivos y conductas en el entorno digital. Por una cuestión de extensión no se abordarán todas, pero para terminar no se puede prescindir de los píxeles de seguimiento. Según el CNIL, es un método alternativo a las *cookies* para el seguimiento. Tradicionalmente se ha implementado en forma de una imagen de un *píxel* por un *píxel*, incrustado en el sitio, pero invisible para el usuario. La carga de esta imagen, cuyo nombre contiene un identificador de usuario, informa al servidor en el que está alojada, que el usuario rastreado ha visitado una página o leído un correo electrónico.[31] Generalmente, los *píxeles* de seguimiento son utilizados en las campañas de *marketing* lanzadas por las organizaciones. Se incorporan los *píxeles* en los correos electrónicos para recolectar información de la campaña y entre otras cosas, pueden verificar si el destinatario lo ha leído, la hora, el dispositivo y la localización. La apertura de correos electrónicos puede poner en peligro la privacidad de los usuarios, que al desconocer la presencia de *píxeles*, quedan expuestos al acceso ilegítimo de su información personal por parte de terceros.[32]

No resultará difícil advertir que la existencia de un rastreador invisible a la percepción del usuario sea, al menos, polémica; circunstancia que sería aún más grave si no es debidamente informada. Existe una clara incidencia en el derecho de la autodeterminación informativa. *Al ser invisibles y recoger y transferir datos personales sin el consentimiento expreso del usuario, los píxeles de seguimiento suponen una violación de los derechos sobre la privacidad de aquél, que se deben proteger.*[33]

El hecho de ser un objetivo potencial de campañas de *marketing* directo en la actualidad es inevitable. El envío masivo de publicidad no siempre se realiza a usuarios que han prestado consentimiento para recibir promociones, novedades y ofertas. Al respecto se

[31] Sitio web CNIL. [en línea]. [fecha de consulta: 13/04/2021] [https://www.cnil.fr/fr/definition/tracking-pixelweb-beacon-ou-pixel-espion]

[32] ENGLEHARDT Steven, HAN Jeffrey, and NARAYANAN Arvind. *I never signed up for this! Privacy implications of email tracking*. [en línea] [Fecha de consulta 5/05/2021]. [https://senglehardt.com/papers/pets18_email_tracking.pdf].

[33] DOMÍNGUEZ Leandro José. *Tracking Pixels: La nueva amenaza para nuestra privacidad.* [en línea]. [Fecha de consulta: 13/04/2021] [https://www.lapoliticaonline.es/nota/tracking-pixel/].

ha sostenido: *El problema es que la información que se puede recopilar de los usuarios en función de estos píxeles es similar a la información que se obtiene de una cookie. En ese sentido, las agencias de marketing emplean campañas de seguimiento a veces incluso personalizado, lo que puede ocasionar invasiones de la privacidad.*[34]Los *píxeles* de seguimiento entonces, se incrustan en las comunicaciones aunque no hayan sido solicitadas, orientadas a recolectar información personal de un usuario de manera ilegítima.

2. FENÓMENOS DE CONTROL QUE PASAN INADVERTIDOS EN EL ENTORNO DIGITAL

Los dispositivos y programas que utilizan los usuarios son impregnados por tecnologías de seguimiento que generan información precisa de distinta índole. Además, generan una falsa sensación de control sobre esa información a partir de comandos que se facilitan para interactuar sobre menús de opciones preconfiguradas y adornadas por diseñadores. ¿Existe un control efectivo de la información que generan los usuarios y sus dispositivos? ¿Es el entorno digital un lugar propicio para acceder libremente a la información y contenidos que se desean o son los programas los que determinan y delimitan las opciones del menú? ¿Los usuarios controlan las tecnologías o estas éstas sirven para controlar a los usuarios? Se ha sostenido: *[...] a pesar de que son los propios usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance muy superior al inicialmente previsto, ya que las redes sociales, las aplicaciones y las plataformas de Internet disponen de potentes herramientas de intercambio de información, llegando a perder en muchas ocasiones el usuario el control sobre dicha información.*[35]En los siguientes capítulos se analizarán ciertos fenómenos de control: quién controla, quién decide y sobre qué.

2.1. *EL FILTRO BURBUJA*

"The individual has a right to cultivate his mind and body alone, in peace, and determine his own will and voice."

Firmin DEBRABANDER[36]

---

[34] AGUIAR, Alberto R. *Tu correo está lleno de "píxeles espía" capaces de detectar si has abierto un email: cómo afecta esta tecnología tan extendida a tu privacidad*.[en línea][Fecha de consulta: 5/5/2021] [https://www.businessinsider.es/son-pixeles-espia-te-llegan-correo-como-evitarlos-814643]

[35] TOURIÑO Alejandro. *El derecho al olvido y a la intimidad en Internet.* Primera edición. Editorial Catarata. Madrid. 2014. P. 64.

[36] DEBRABANDER, Firmin. *Life after Privacy...*, cit., p 96.

El filtro burbuja es un fenómeno que se produce como consecuencia del uso de ciertas tecnologías diseñadas con propósitos de personalización. Los algoritmos que subyacen ciertos programas, valiéndose de la información recogida por la interacción de los usuarios, realizan inferencias sobre sus gustos y suministran contenidos que considera que serán acordes a las preferencias. En el presente capítulo se referirá a este efecto, a los impactos que tienen individual y colectivamente.

Eli Pariser, autor del libro el *filtro burbuja,* cuenta cómo funcionan las distintas tecnologías con las que interactuamos a diario y proporciona valiosa información e interesantes reflexiones a los fines del presente trabajo. En resumidas cuentas, explica cómo los modelos de negocio actuales utilizan y se benefician de mecanismos sofisticados de personalización. La inteligencia artificial que subyace a ciertos programas se alimenta de los datos generados por la interacción de los usuarios en Internet, en busca de conseguir predicciones de las preferencias de los usuarios para suministrar información acorde. Expone las diversas consecuencias individuales y colectivas que pueden acarrear estas tecnologías. *La nueva generación de filtros de internet observa las cosas que parecen gustarte- las cosas mismas, o las que les gustan a las personas como tú- e intenta extrapolar. Son máquinas de predicción cuyo objetivo es crear y perfeccionar constantemente una teoría acerca de quién eres, lo que harás y lo que desearás a continuación. Juntas elaboran un universo de información único para cada uno de nosotros- lo que he llamado una burbuja de filtros- que, en esencia altera nuestra manera de encontrar ideas e información.*[37] El autor revela cómo las redes sociales y otras importantes empresas de la industria digital son diseñadas de modo similar, con algunas variantes entre sí ajustadas a sus intereses y negocios, pero alude a empresas como *Google; Facebook; Amazon; Netflix*; entre otras, con inmensa convocatoria de usuarios. Las tecnológicas y los defensores de la personalización argumentan que *muestran una visión del mundo hecho a medida que se ajusta a nosotros a la perfección.*[38] Describe cómo la tecnología subyacente compuesta por complejos algoritmos, condiciona la vida de los usuarios de manera individual y sus repercusiones colectivas. Presenta argumentos sólidos para sostener que los usuarios pueden ser influenciados y manipulados a través de las plataformas.

[37] PARISER, Eli. *El filtro burbuja: cómo la red decide lo que leemos y lo que pensamos*. VAQUERO GRANADOS Mercedes, Trad. Primera edición. Barcelona. Editorial Taurus. 2017. Pp.18-19.
[38] Ibidem. P. 21.

2.1.1. Consecuencias individuales de la burbuja de filtros

"La tecnología diseñada para darnos más control sobre nuestras vidas en realidad nos la está quitando".

Eli Pariser.[39]

La burbuja de filtros introduce dinámicas desconocidas a las que no nos habíamos enfrentado antes. *En primer lugar, estás solo [...] tú eres la única persona dentro de tu burbuja. En una época en la que el intercambio de información es la base de la experiencia compartida, la burbuja de filtros actúa como una fuerza centrífuga que nos separa.*[40] La burbuja se construye por la interacción individual del usuario con su dispositivo mientras utiliza los programas. Es invisible, no se puede apreciar ni conocer lo que la burbuja ha interpretado de las interacciones realizadas y cómo ha llegado a los resultados que suministra. *Como no has elegido los criterios según los cuales las páginas filtran la información que entra y sale, resulta fácil imaginar que la información que pasa por un filtro burbuja sea imparcial, objetiva y verdadera. Pero no lo es. De hecho, desde dentro de la burbuja es prácticamente imposible ver lo sesgada que es. Por último, uno no elige entrar en la burbuja. [...].* [41]

En la faz individual el usuario pierde el acceso a la diversidad de contenidos. No es consciente del horizonte que descarta la personalización. Asimismo, puede afectar su equilibrio cognitivo y su capacidad de aprender. El filtro burbuja *nos cerca con ideas con las que ya estamos familiarizados induciéndonos a un exceso de confianza en nuestros esquemas mentales [...] elimina de nuestro entorno algunos elementos clave que nos hacen querer aprender.*[42] Al no mostrar cosas distintas, reprime la curiosidad y la creatividad. La información que llega al usuario será relacionada a lo que el algoritmo asume o infiere que es de su interés, eliminando el poder de decisión del usuario, y rechazando aquella información que no considere acorde, afectando así el derecho a la libertad de información. Además, la inteligencia artificial que domina los programas cada vez se hace más inteligente, mientras que el usuario se ve privado de acceder a contenido que fomente la diversidad de pensamiento y aprendizaje. En este sentido, se

[39] Ibidem. P. 216.
[40] Ibidem. P. 19.
[41] Ibidem. P.19.
[42] Ibidem. P.89.

ha afirmado: *La personalización puede interferir en la creatividad e innovación. [...] limita artificialmente el espacio mental en el que buscamos soluciones a los problemas. [...] alienta un enfoque más pasivo con respecto a la obtención de información, incompatible con la clase de exploración que conduce al descubrimiento [...]. No ves lo que no te interesa en absoluto. Ni siquiera eres consciente de que existen acontecimientos e ideas importantes que te estás perdiendo.*[43]El control y poder de decisión lo tiene el algoritmo.

2.1.2. Consecuencias colectivas de la burbuja de filtros

"Cuanto más afanosamente se hermetiza el pensamiento a su ser condicionado en aras de lo incondicionado es cuando más inconsciente y, por ende, fatalmente sucumbe al mundo."

Theodor L.W. Adorno[44]

En cuanto al impacto colectivo, la tecnología funcionará a la perfección para radicalizar posturas ya que no dosifica con variedad de contenidos ni proporciona alternativas para que los usuarios reconfiguren sus preferencias, las corrijan, se opongan, ni ejerzan en fin, derecho alguno de protección de sus datos. Los usuarios reciben contenidos de terceros indexados de manera automática, sin posibilidad de verificación de las fuentes, por lo que se hacen vulnerables a la desinformación.

El sesgo de confirmación aludido como efecto de explotación individual, tiene impacto colectivo cuando se trata, por ejemplo, de información de índole política; social; cultural; ideológica; sindical u otro tipo de información sensible. Al respecto se ha expresado: *Si internet dice lo mismo que yo pienso, es que tengo razón. Como resultado, no vemos la información con la que no estamos de acuerdo, aislándonos en nuestras propias burbujas culturales o ideológicas.*[45] Los usuarios no conscientes de estas complejas dinámicas, aunque parezca llevado al extremo, pueden ser víctimas de manipulaciones causadas por los algoritmos y adoptarse posturas radicales con repercusiones masivas posibilitando la afectación de la paz social y el propio sistema democrático. Las plataformas más utilizadas se componen de algoritmos que refuerzan

[43] Ibidem.P. 98-110.
[44]ADORNO, Theodor L.W. *Minima Moralia. Reflexiones desde la vida dañada. Obra completa, 4*. CHAMORRO MIELKE, Joaquín, trad. Edición de Bolsillo. Ediciones Akal. Madrid. 2006. Parágrafo 153. P.257.
[45]PARISER, Eli. *El filtro burbuja...*, cit., pp 169-170.

posturas y las radicaliza. Un ejemplo, se da en redes sociales como *Facebook* que con su función de grupos (una funcionalidad permitida y trasladable a casi todas las redes sociales) tiende a afianzar creencias, al tiempo que las hace más extremas y más fuertes contra tendencias y contenidos diferentes. Algunos escándalos como el de *Cambridge Analytica*, el *Brexit* y otros conflictos sociales se han intensificado a través de las redes sociales con la colaboración de las burbujas de filtros.[46]

La personalización conduce a la falta de libertad de información. *Estamos avanzando a gran velocidad hacia un régimen repleto de información personalmente relevante. Y aunque esto puede ser útil, algo demasiado bueno puede causar verdaderos problemas. Abandonados a su suerte, los filtros personalizados presentan cierta clase de autopropaganda invisible, adoctrinándonos con nuestras propias ideas, amplificando nuestro deseo por cosas que nos son familiares y manteniéndonos ignorantes con respecto a los peligros que nos acechan en el territorio oscuro de lo desconocido.*[47]

Se destaca como circunstancia adicional, la falta de transparencia de los programas. El hecho de que la burbuja de filtros sea invisible no la convierte en transparente, sino en un fenómeno imperceptible, inescrutable y lo que es peor, incontrolable.

2.2. *DARK PATTERNS*

"Freedom involves or demands a zone of no interference."

Firmin DEBRABANDER[48]

Los patrones oscuros son *aquellos diseños que en Internet consiguen conducir deliberadamente y de forma poco ética al usuario hacia una concreta acción interesada*.[49]

A los efectos de aclarar lo analizado en el presente capítulo, es preciso referir que el término "*Dark Patterns*", patrones oscuros en su traducción española, se lo atribuye Harry Brignull, consultor en diseño basado en la experiencia del usuario y editor del sitio web conocido como Darkpatterns.org. *Los patrones oscuros son trucos que se utilizan en sitios web y aplicaciones que te obligan a hacer cosas que no quisiste, como*

[46] Ibidem. P. 171.
[47] PARISER, Eli. *El filtro burbuja...*, cit., p 24.
[48] DEBRABANDER, Firmin. *Life after privacy...*, cit., p102.
[49]BENITO MARTIN Ruth. Protección de datos: el principio de lealtad y los dark patterns. En: Paloma, LLANEZA GONZALES. *Ellas. Retos, amenazas y oportunidades en un mundo conectado.* Primera edición. Las Rozas, (Madrid) España: Wolter Kluwer, 2019. Capítulo: pp. 164-209. P. 199.

comprar o registrarte en algo.[50] El propósito del proyecto es dar a conocer y avergonzar a las empresas que lo utilizan. Tuvo origen en una publicación que hiciera en un blog titulada: *"Dark Patterns: dirty tricks designers use to make people do stuff".*[51] A la fecha, continúa vigente, plantea la concientización y fomenta la revelación, denuncia y exposición de prácticas de diseño confusas, oscuras, desleales y no transparentes que implementan los responsables de los sitios web y aplicaciones en el entorno digital.

Aunque los patrones oscuros no sean tecnologías en sí, son técnicas y astucias de las que se valen desarrolladores de sitios web, aplicaciones y otras tecnologías que tienen repercusiones en derechos fundamentales de los usuarios. Las artimañas desplegadas en el entorno digital principalmente se encuentran asociadas al diseño y su utilización pueden afectar el derecho de información y con ello, desviar intencionalmente la voluntad de los usuarios y su capacidad de tomar decisiones.

La CCPA de EEUU, establece en el apartado de definiciones (1798.140) que el acuerdo obtenido mediante el uso de patrones oscuros no constituye consentimiento. Asimismo, define a los patrones oscuros expresamente: *significa una interfaz de usuario diseñada o manipulada con el efecto sustancial de subvertir o perjudicar la autonomía del usuario, la toma de decisiones o la elección.*[52]

2.2.1. Detección de patrones oscuros

Se puede advertir que se está en presencia de patrones oscuros cuando, por ejemplo, al navegar en Internet se aparece un aviso y la información que se proporciona no se logra visualizar con claridad o cuando el botón de aceptar tiene tonalidades más llamativas que el de rechazar, por lo que se alienta de manera subrepticia a adoptar la primera opción antes que la segunda. Otro ejemplo, puede ser cuando no se proporciona una opción para cancelar una operación o suscripción o en caso de existir la alternativa, se encuentre camuflada o de difícil acceso para el usuario, lo que implica una intención de disuadir la elección de dicha opción. Estas prácticas y técnicas tienen manifestaciones de las más variadas y transversales. En un estudio llevado a cabo por académicos de

[50] Sitio web oficial de Dark Patterns.org [en línea] [Fecha de consulta: 10/04/2021]. [https://www.darkpatterns.org/]

[51] BRIGNULL, Harry. *Dark Patterns: dirty tricks designers use to make people do stuff.* [en línea] [Fecha de consulta: 10/04/2021]. [https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/]

[52] California Consumer Privacy Act 2018. Apartado 1798.140. [en línea] [Fecha de consulta 5/05/2021][https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5].

Princeton publicado a fines del 2019 se explicó cabalmente el funcionamiento de estas prácticas y cómo afecta en la toma de decisiones de los consumidores.[53] Principalmente pueden afectar como se dijo al derecho de información; la libertad de elección del usuario, la validez del consentimiento a través de la manipulación. Según el artículo académico, estas técnicas apelan a los sesgos cognitivos del usuario, atacando a la consciencia por medio de una influencia dirigida. Se busca que el usuario tome decisiones apresuradas y no razonadas que de otro modo no tomaría si contara con la información completa y con tiempo suficiente para analizarlo. De esta manera, los consumidores o usuarios pueden ser privados de la libertad de elegir, controlar su propio destino y el de su información. Se presenta, así, otro supuesto donde la autodeterminación informativa se ve afectada. Shoshana Zuboff, sostuvo que las nuevas formas de mercado atentan contra lo que llama el derecho al tiempo futuro y lo conceptualiza de la siguiente manera: *es el derecho a actuar libres de la influencia de unas fuerzas ilegítimas que operan al margen de nuestra conciencia con el objeto de influir, modificar y condicionar nuestros comportamientos.*[54]

El Consejo del Consumidor de Noruega publicó un informe en inglés titulado: "*Deceived By Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*".[55] Concretamente, se refiere a cómo las empresas tecnológicas utilizan patrones oscuros para desalentarnos a ejercitar nuestros derechos de privacidad. Resulta muy interesante porque expone las deficiencias en materia de privacidad que empresas como *Facebook, Google y Windows* proporcionan por defecto en las plataformas, utilizando palabras y símbolos que desaniman la configuración de preferencias en favor de la privacidad.

2.2.2. Controversias en los patrones oscuros

Con todo lo expuesto en el presente capítulo, no resultará difícil al lector advertir las implicaciones que estas técnicas tienen respecto de los derechos de los usuarios en el entorno digital.

---

[53] MATHUR Arunesh, ACAR Gunes, FRIEDMAN Michael J., LUCHERINI Elena, MARSHINI CHETTY Jonathan, and NARAYANAN Arvind. *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 81 (November 2019), 32 pages. [https://doi.org/10.1145/3359183] [en línea] [Fecha de consulta: 6/5/3032]. [https://arxiv.org/pdf/1907.07032.pdf]

[54] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia...*, cit., p 268.

[55] Forbrukerrådet Report. *Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy.* [en línea] [Fecha de consulta: 10/04/2021] [https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf]

Es común que las prácticas se proyecten en las plataformas de comercio electrónico, o en los documentos que rigen las relaciones en la web como las políticas de *cookies*, de privacidad, términos y condiciones, entre otras. A este respecto Noain Sánchez ha sostenido: *[...] dichas políticas no están diseñadas para ser leídas: Son altamente complejas, el lenguaje usado contiene demasiadas ambigüedades como para saber, exactamente, qué sucede con los datos introducidos y tiende a ser farragoso. […] Por su parte, el diseño tipográfico no es accesorio, sino que añade más dificultad. Suelen usarse fuentes difíciles de leer, cuerpos de letra pequeños y, a ser posible, en mayúsculas, propiciando que la tipografía se convierta en texturas más que en palabras y espacios. Finalmente, la extensión de dichas condiciones tampoco es desdeñable.*[56]

Es preciso mencionar el claro conflicto que se erige en perjuicio del artículo 25 del RGPD dado que a través de estas técnicas se puede afectar directamente la protección de datos desde el diseño y por defecto, al obstaculizar el ejercicio de los derechos, mediante procedimientos poco claros, o suministrando información deficiente. Las técnicas transgreden el principio de responsabilidad proactiva vinculante a los titulares de las plataformas. Además, atentan contra los principios de lealtad y transparencia. Como surge del estudio académico citado, buscan manipular e influenciar las decisiones de los usuarios en perjuicio de sus intereses. Los patrones oscuros no comulgan con la privacidad desde el diseño y por defecto sino que tienen defectos de privacidad en sus diseños.

También se ha referido sobre los textos legales de internet: *Las políticas de privacidad rara vez especifican usos secundarios futuros, entonces las personas no pueden tomar decisiones informadas sobre su información porque tienen poca idea acerca del rango de los usos potenciales.*[57] Se afecta además, al principio de limitación de finalidad de tratamiento.

A modo de resumen se podría decir que los patrones oscuros se proyectan a través de las interfaces de las pantallas y plataformas. A diferencia del filtro burbuja el fenómeno se esconde en la propia infraestructura y es totalmente invisible para el usuario, los patrones oscuros son visibles pero incognoscibles, diseñados para engañar. De los casos

[56] NOAIN SÁNCHEZ, Amaya. *La protección de la intimidad...*, cit., pp 237-238.

[57] SOLOVE, Daniel J. *Understanding Privacy...*, cit., p 132. El autor citado expresó: *"Privacy policies rarely specify future secondary uses, so people cannot make an informed decision about their information because they have little idea about the range of potential uses."* La frase fue traducida a los fines del trabajo.

expuestos hasta aquí, nada obsta que estas técnicas y tecnologías se vinculen entre sí en una sola plataforma, de hecho, las más conocidas contienen todos estos ingredientes.

3. LA MERCANTILIZACIÓN DE LOS MECANISMOS DE SEGUIMIENTO Y CONTROL

De lo explicado hasta el momento se puede apreciar el rol preponderante de los mecanismos de seguimiento y control existentes en el entorno digital. Entre la información que se capta a través de estos mecanismos predominan la información personal de los usuarios, sus dispositivos, el navegador que utilizan, sistema operativo, la dirección IP, localización, patrones de interacción en el sitio web o de conducta, entre otros datos que pueden servir para la elaboración de distintos perfiles con valor significativo para fines publicitarios y explotación económica. En ese sentido se introduce el estudio respecto de la huella digital oportunamente citado: *Actualmente, el modelo que subyace tras la mayoría de los servicios web se basa en prestar un servicio de forma totalmente gratuita a cambio de la monetización de los datos recopilados de los usuarios. En la mayoría de los casos la información recogida de los usuarios se rentabiliza a través de servicios de marketing que dirigen campañas de publicidad personalizadas por quien desea publicitar un producto o servicio. Por lo tanto, además de identificar al usuario y realizar un seguimiento y recopilación de datos, necesitan perfilarlo con el objetivo de maximizar la eficacia de la publicidad que se les ofrece.*[58]

La explotación económica de las tecnologías con fines publicitarios adquiere una dimensión global.[59] En la comunicación de la Comisión Europea sobre la Estrategia de Mercado Único Digital del 2015, hizo alusión al panorama actual y ante la interrogante de por qué se necesitaba un Mercado único Europeo, se estableció: *La economía mundial se está convirtiendo rápidamente en digital. Las tecnologías de la información y la comunicación (TIC) ya no son un sector específico sino el fundamento de todos los sistemas económicos innovadores modernos. Internet y las tecnologías digitales están transformando la vida que llevamos y la forma en que trabajamos (como personas, en las empresas y en nuestras comunidades) cuanto más se integran en todos los sectores de nuestra economía y nuestra sociedad [...].*[60] En España solamente, conforme el

[58] Agencia Española de Protección de Datos. *Estudio Fingerprinting*..., cit., p 3.

[59] ORTIZ LÓPEZ, Paula. Cookies, fingerprinting y la privacidad digital. En: LÓPEZ CALVO, José. *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Segunda edición. Las Rozas (Madrid). Wolters Kluwer. 2019. Capítulo Pp. 961- 972. P. 961.

[60] Comisión Europea. *Comunicación de la comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia para el Mercado Único Digital*

informe del 2020 del sector de los contenidos digitales elaborado por el ONTSI se destaca el incremento en las ganancias en el sector de la publicidad digital: *El crecimiento más significativo se ha producido en la rama de publicidad digital. En 2019, esta actividad facturó 3.150 millones de euros, un 59,7% más que en 2018[...].* [61] Se deja aclarado que no se realiza juicio alguno debido a que se reconoce que las tecnologías analizadas son una fuente de ingresos importantes para la economía general. Sin embargo, existen falencias entorno a la información suministrada a los usuarios.

Se ha sostenido que *en los últimos años están surgiendo modelos de negocio muy rentables basados en la recopilación, almacenamiento, depuración, filtrado, enriquecimiento y extracción de valor de los datos y de su comercialización masiva en un mundo cada vez más interconectado. Parte de ese proceso consiste en un intenso "tracking" y "profiling" de la actividad online de los usuarios.*[62] Asimismo, *los modelos de negocio que han hecho de los datos su materia prima entrañan algunos riesgos desde la perspectiva del derecho a la protección de datos, especialmente los que se basan en la generación de perfiles a partir del seguimiento y monitorización de la actividad de los usuarios en la red.*[63]

En una economía basada en datos, las *cookies* y tecnologías similares aludidas, son unos de los componentes que alimentan al sistema suministrando información generada en el entorno digital y, conforme lo demostrado, producen grandes impactos en la economía. Cuestiones como las ofertas de tiempo real (RTB, *real-time bidding* en inglés) son objeto de serios debates que enfrentan a los derechos fundamentales y a la economía de datos, específicamente en el rubro de la publicidad digital. Las ofertas de tiempo real consisten en pujas que se llevan a cabo en internet entre anunciantes para mostrar al usuario una publicidad determinada y dirigida. Para que ello suceda, la información de usuarios y dispositivos recolectada por los mecanismos de seguimiento y control, es accedida por terceras partes interesadas sin conocimiento ni consentimiento. En

---

de Europa [en línea]. [Fecha de consulta: 03/04/2021] [https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52015DC0192]

[61] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información. *Informe anual del sector de los Contenidos Digitales en España 2020* [en línea]. Madrid: Secretaría General Técnica. Centro de Publicaciones. [Fecha de consulta: 02/04/2021] [http://doi.org/10.30923/]

[62] GARCÍA MEXÍA, Pablo y PERETE RAMÍREZ, Carmen. Internet, el RGPD y la LOPDGDD. En: LÓPEZ CALVO, José. *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD.* Segunda edición. Las Rozas (Madrid). Wolters Kluwer. 2019. Capítulo pp.851-872. P.853.

[63] Ibidem. P.855.

cuestión de milisegundos los anunciantes compiten por el espacio publicitario *online* disponible a través de un sistema de pujas durante el tiempo que tarda en cargarse el sitio web y las aplicaciones. El ganador mostrará el anuncio más pertinente de acuerdo al perfil del usuario. Recientemente la ICO, publicó un reporte donde se destacó que la falta de madurez de la industria presenta serias amenazas a los derechos y libertades de los usuarios[64]. Además, de acuerdo al informe, estos sistemas automatizados de pujas llevan a cabo tratamientos de datos de manera ilegal valiéndose de *cookies* y otras tecnologías, justificadas en bases legales insuficientes sin el consentimiento de los interesados. Finalmente, destaca la falta o deficiente información sobre estos asuntos: *La información de privacidad proporcionada a las personas carece de claridad mientras que también resulta compleja.* Luego de una pausa en las investigaciones a causa de la pandemia, la ICO anunció la reanudación de las mismas mediante una declaración publicada en el sitio oficial destacando: *El complejo sistema de RTB puede utilizar los datos personales confidenciales de las personas para publicar anuncios y requiere el consentimiento explícito de las personas, lo que no está sucediendo en este momento.*[65] El Consejo Irlandés de Libertades Civiles, ha presentado una reclamación en Hamburgo, Alemania el pasado 24/03/2021 con el objetivo de investigar estas prácticas y poner el freno a los tratamientos ilegales que vulneran el derecho de protección de datos personales. [66]

A raíz de todo lo comentado, no se puede ignorar que existen implicaciones relevantes en la privacidad de los usuarios, pero, especialmente, en el derecho de libertad informática. En el marco de deliberaciones de la propuesta de Reglamento *e- privacy*, el Consejo Europeo adoptó un texto consolidado en el 2017 donde se destacó la importancia de encontrar un equilibrio entre el aseguramiento de la adecuada protección de la privacidad sin socavar modelos comerciales legítimos.[67]

---

[64] Oficina del Comisionado de Información -ICO. Versión en inglés del "Informe de actualización en adtech y pujas en tiempo real". 20 Junio 2019. [en línea] [Fecha de consulta: 18/06/2020] [https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf]

[65]MCDOUGALL, Simon, Comisionado Adjunto de la ICO.[en línea][Fecha de consulta: 18/06/2021] [https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes]

[66] Reclamación presentada por el Consejo Irlandés de Libertades Civiles. [en línea] [Fecha de consulta 18/06/2021][https://www.iccl.ie/wp-content/uploads/2021/06/ENGLISH-TRANSLATION-MACHINE-TRANSLATED-COMPRESSED-Schriftsatz-an-das-Landgericht-Hamburg.pdf]

[67] Council of the European Union. *"Interinstitutional File: 2017/0003 (COD)"* [en línea] [Fecha de consulta: 27/02/2021]. [https://data.consilium.europa.eu/doc/document/ST-15333-2017-INIT/en/pdf] P. 2

Hasta aquí se ha presentado el caso de las *cookies* y algunas tecnologías similares de seguimiento y control, habiendo conceptualizado, caracterizado y clasificado las mismas. Además, se ha dejado plasmado su relevancia en el entorno digital, las cuestiones que las circundan y destacado su relevancia respecto a la privacidad de los usuarios.

III. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

El derecho a la protección de datos es un derecho fundamental, autónomo e independiente que garantiza a las personas un poder de disposición y control sobre el uso y destino de sus datos personales. Se ha sostenido que: *atribuye al titular un poder de disposición sobre sus propios datos personales y se configura como un derecho autónomo e independiente del derecho a la intimidad. Hoy está sometido a constantes amenazas derivadas del uso de las nuevas tecnologías, que permiten el tratamiento masivo de datos personales y nos sitúan en una sociedad constantemente vigilada.*[68] Ciertamente, el entorno digital actual y la incesante evolución tecnológica, imprimen serios desafíos para el ejercicio efectivo de este derecho por parte de las personas.

A lo largo de la historia mucho se ha escrito al respecto del derecho fundamental de libertad informática. No es objeto del presente trabajo abordar ni analizar el instituto de manera integral ni acabada dado que la extensión de su desarrollo implicaría una desproporcionada explicación que excedería los propósitos que se pretenden resaltar. En definitiva, en el capítulo se abordarán extractos normativos, doctrinales y jurisprudenciales que ilustran el derecho bajo análisis y se podrá advertir cómo las tecnologías, técnicas y fenómenos desarrollados a lo largo del trabajo, influyen en su eficacia.

1. BREVE EVOLUCIÓN NORMATIVA Y JURISPRUDENCIAL

Un antecedente relevante del instituto del derecho de la libertad informática puede identificarse en la conocida Sentencia del Tribunal Constitucional de la República Federal de Alemania de 1983[69]. En referencia a esta sentencia, Perez Luño sostuvo: *En*

[68] PIÑAR MAÑAS, José Luis. *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio.* Documento de trabajo 147/2009. Fundación Alternativas. P.5. [en línea] [Fecha de consulta 28/4/2021].
[http://www.cepc.gob.es/docs/ley-de-transparencia/ponencia-j-luis-pi%C3%B1ar.pdf?sfvrsn=0]

[69] Tribunal Constitucional de la República Federal de Alemania. Sala Primera (Ref. BVR 209/1983). Véase CSJN, 15/10/1998, *Urteaga, Facundo R.* c. Estado Mayor Conjunto de las Fuerzas Armadas", voto del Dr. Santiago E. Petracchi, LA LEY, 1998-F, 237. Surge de la sentencia: "[...] el Tribunal

dicha decisión jurisprudencial se reconocía el derecho a la "autodeterminación informativa", hasta entonces invocado por la doctrina jurídica, y concretado en la facultad de todo ciudadano de las sociedades democráticas de determinar: quién, qué, cuándo y con qué motivo puede conocer datos que le conciernen.[70] Concretamente surge la idea de que el ciudadano ostenta el señorío de la información que genera y/ó que le concierne.[71]

El derecho fundamental bajo análisis ha sido objeto de regulación en diversos instrumentos internacionales incluyendo: el Artículo 8 del CEDH[72]; Convenio N°108 del Consejo de Europa, de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[73]; el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea[74], entre otros. En España se encuentra previsto en el artículo 18.4[75] de la Constitución, desde el año 1978. El precepto se desarrolló mediante la promulgación de la Ley Orgánica 5/1992[76], de 29 de octubre, que como

---

Constitucional Alemán se expidió con relación a una Ley de Censo, votada por el Parlamento [Bundestag], según la cual, y a fin de mejorar el aprovechamiento de los recursos sociales, se compelía a los ciudadanos a responder un interrogatorio que abarcaba una serie de datos privados. Aunque los datos eran relevados en forma anónima, iban a ser cotejados con los registrados en los estados federados [Länder], y ello, hipotéticamente, permitiría identificar a sus titulares. El Tribunal, si bien confirmó la validez de la mayor parte de la ley, obligó a realizar modificaciones en ciertos puntos, relativos al modo en que se podía autorizar la recolección y almacenamiento de los datos, lo cual significó, finalmente, que el censo se postergara por cuatro años con un considerable costo para el Estado."
Se puede descargar la sentencia en el enlace que se proporciona: [en línea] [Fecha de consulta: 13/5/2021] [http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-urteaga-facundo-raul-estado-nacional-estado-mayor-conjunto-ffaa-amparo-ley-16986-fa98001242-1998-10-15/123456789-242-1008-9ots-eupmocsollaf]

[70] PÉREZ LUÑO, Antonio E. La tutela de la libertad informática en la sociedad globalizada. *Isegoría: revista de filosofía moral y política. 2000*, vol. 22, no. 22, Consejo Superior de Investigaciones Científicas, Instituto de Filosofía, pp. 59–68. p 61.

[71] Vid; ALTMARK Daniel R., MOLINA QUIROGA, Eduardo. *Tratado de derecho informático*. Primera edición. Buenos Aires. Editorial La Ley. 2012. Tomo II. p. 322. Al respecto los autores refirieron: *"*El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, sus relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la autodeterminación informativa.*"*

[72] Carta de los derechos fundamentales de la Unión Europea. [en línea][Fecha de consulta 13/5/2021][https://www.europarl.europa.eu/charter/pdf/text_es.pdf]

[73] 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. [en línea][Fecha de consulta 13/5/2021][https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447]

[74] TFUE. Artículo 16.1: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan." [en línea][Fecha de consulta 13/5/2021][https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12012E/TXT&from=ES]

[75] Constitución Española. Artículo 18.4:"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".[en línea][Fecha de consulta 13/5/2021][https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229]

[76] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.[en línea][Fecha de consulta 13/5/2021][https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750]

consecuencia de la transposición de la Directiva 95/46/CE[77], aquélla fue derogada por la Ley Orgánica 15/1999 de protección de datos de carácter personal[78]. Actualmente, luego de la entrada en vigor del RGPD (UE 2016/679)[79] de obligado cumplimiento y aplicación directa, convive a nivel local con la Ley orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[80].

Más allá del trayecto normativo, que es abundante y no se puede abordar por completo en esta oportunidad en detalle, la evolución jurisprudencial en España ha proporcionado aportes trascendentales sobre la materia. De la misma manera, se destacan algunos extractos que ilustran el derecho de referencia.[81]

Con posterioridad a la previsión constitucional de 1978, en el fundamento jurídico 6° de la STC 254/1993, de 20 de julio, se reparó en la importancia de los riesgos para el tratamiento de datos mediante la informática. Así, distingue la independencia del derecho a la libertad informática respecto del derecho al honor y la intimidad. Se advertía: *En el presente caso 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*

[77] 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] [Fecha de consulta 13/5/2021] [https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678]

[78] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.[en línea][Fecha de consulta 13/5/2021][https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189]

[79] Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.[en línea][Fecha de consulta 13/5/2021][https://www.boe.es/doue/2016/119/L00001-00088.pdf]

[80] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.[en línea][Fecha de consulta 13/5/2021][https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673]

[81] A este respecto véase el preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, donde refiere: "El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso."

uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama «la informática» [...].[82]

Posteriormente, distintos pronunciamientos fueron delineando conceptos de la libertad informática. A lo largo de las sentencias del Tribunal Constitucional se han citado fundamentos jurídicos de otros antecedentes. A modo de ejemplo, el concepto de libertad informática al que recurrió el Fundamento 5° de la STC 292/2000: *La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y 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 (SSTC 11/1998, F.J. 5, 94/1998, F.J. 4)*[83]. Aquella sentencia reconoce el derecho de protección de datos como derecho fundamental y vale la pena detenerse en algunos de sus fundamentos jurídicos.

Entre otros aspectos establece respecto del derecho de protección de datos que *[…] atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley.*[84] El pronunciamiento, no sólo aporta importantes reflexiones a la materia, también distanciando el derecho de intimidad del derecho de protección de datos, aclara en el considerando 6° que el interesado ostenta: *[...] 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. […] garantiza a los individuos un poder de disposición sobre esos datos. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin. [...]*[85]. La sentencia hace expresa mención, del derecho a saber, a ser informado de manera que sea posible y eficaz la disposición y control por parte del interesado.

Continúa la sentencia respecto del propósito del derecho fundamental que es: *garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y*

[82] Fragmento del Fundamento jurídico 6° de la Sentencia del Tribunal Constitucional: STC 254/1993, de 20 de julio.
[83] Fragmento del Fundamento jurídico 5° de la Sentencia del Tribunal Constitucional: STC 292/2000, de 30 de noviembre.
[84] Ibidem.
[85] Ibidem.

efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.[86] Resulta con claridad que el presupuesto de la información es crucial para ejercitar las facultades que la sentencia menciona y que sea requerido un consentimiento previo al tratamiento.

Para cerrar la referencia a la importante sentencia bajo análisis, aporta en su fundamento 7°: *Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. [...]*[87].

A los propósitos del trabajo resulta interesante, por último, referir al fundamento jurídico 4° de la STC 17/2013, que sostuvo: *[...] la finalidad del derecho fundamental 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 [...].*[88]

Sucintamente, recogiendo parte de los extractos referenciados, corresponde resaltar que el derecho de protección de datos se proyecta, o se debería proyectar de manera eficaz, a través de un binomio de dimensiones.[89] Se identifica una faz negativa, mediante la cual los terceros deben cumplir con deberes y abstenciones en respeto de los derechos de las

[86] Fragmentos del Fundamento jurídico 6° de la Sentencia del Tribunal Constitucional STC 292/2000, de 30 de noviembre.
[87] Fragmento del Fundamento jurídico 7° de la Sentencia del Tribunal Constitucional STC 292/2000, de 30 de noviembre.
[88] Fragmento del Fundamento jurídico 4° de la Sentencia del Tribunal Constitucional STC 17/2013, de 31 de enero.
[89] Tribunal Constitucional Español, Sentencia 292/2000, BOE núm. 4. del Jueves 4 enero 2001-104.Fundamento jurídico 5°.

personas y una faz positiva mediante el cual el interesado tiene el poder de conocer, controlar y disponer la información personal que le concierne en su sentido más amplio.

2. LOS PRINCIPIOS EN LA NORMATIVA DE PROTECCIÓN DE DATOS

Corresponde referir al punto neurálgico de todo análisis sobre los que se asienta el cumplimiento y respeto de los derechos y libertades. En el presente apartado haremos una breve mención de los principios de protección de datos atento que como se señalará en los próximos capítulos, los patrones encontrados salpican a todos ellos.

El RGPD enseña en su artículo 5 los principios que rigen el tratamiento de datos personales. Sin ánimo de profundizar sobre todos ellos, son: licitud, lealtad y transparencia; minimización de datos; exactitud; limitación de conservación; integridad y confidencialidad y responsabilidad proactiva.

En los casos desarrollados en el trabajo predominan aquellos que refieren al principio de licitud, lealtad y transparencia. Por ejemplo, existen cuestiones respecto de las *cookies* que atentan contra los principios de licitud, lealtad y transparencia del tratamiento de datos. En este sentido, se ha sostenido: *Especial consideración en relación con el principio de licitud merecen los avisos de cookies, de los que se encuentra plagado en internet. La mayoría de ellos no cumplen con el principio de lealtad, ni con el principio de transparencia ni con el de licitud: se le dice al navegante que las cookies sirven para mejorar su experiencia de usuario (información incorrecta o inexacta), no ofrecen la posibilidad de rechazar fácilmente las cookies cuando sí la ofrecen para aceptarlas o resulta forzoso aceptar o rechazar todas en bloque (no hay consentimiento específico y es desleal), el enlace a la segunda capa informativa no está habilitado (falta de información y transparencia), se interpreta que la mera permanencia o navegación por la web supone la aceptación de las cookies (no hay consentimiento inequívoco), directamente las cookies se instalan antes de haber sido aceptadas (vulnera el principio de licitud y lealtad).*[90] El principio de lealtad, acogido entre otros cuerpos normativos, por la Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 8.2 y en el artículo 5 del Convenio 108 (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). La licitud y transparencia están directamente

[90] BENITO MARTIN Ruth. Protección de datos: el principio de lealtad..., cit., p 187.

vinculadas a la lealtad. Se ha señalado: *si un tratamiento no es lícito o en él no se emplean medios lícitos, tampoco será un tratamiento leal para con el interesado ya que, la introducción de un elemento ilícito viene a suponer la quiebra de la debida honestidad o buena fe [...].*[91]

El Tribunal Supremo de la Unión Europea ha sostenido: [...] *para garantizar un tratamiento de datos leal y transparente, el responsable del tratamiento debe facilitar al interesado información, entre otras cosas, sobre el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, sobre los criterios utilizados para determinar este plazo.*[92] Asimismo, sobre los principios de minimización y limitación de conservación, refiriéndose al tratamiento desleal de las *cookies* subrayó: *un período 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.*[93]

En Holanda, la Corte de la Haya, prohibió el uso de un algoritmo que analizaba a los ciudadanos para detectar posibles fraudes por considerar que vulneraba los principios: *La corte toma en consideración los principios fundamentales de protección de datos bajo la legislación europea (Carta Europea y RGPD), específicamente los principios de transparencia, limitación de finalidad y minimización.*[94] Se volverá sobre la sentencia con posterioridad.

Es indudable la injerencia sobre los derechos y libertades de los usuarios que pueden tener la tecnología, las técnicas y fenómenos si no observan los principios aludidos. Inciden en la posibilidad de ejercer y reivindicar otros derechos, afectando institutos como la información y, derivado de este, el poder de decisión vulnerando la autodeterminación informativa. Éstos serán los temas a tratar en los próximos capítulos.

---

[91] Ibidem: P. 172.

[92] Tribunal de Justicia de la Unión Europea, 1/10/2019, *"Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V./Planet49 GmbH (Asunto C-673/17)"* [en línea]. [Fecha de consulta 19/04/2021]
[https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62017CJ0673&from=EN]

[93] Ibidem.

[94] Corte de La Haya. Versión en inglés del Caso: *NJCM, Platform Bescherming Burgerrechten, Privacy First, Koepel van DBC-Vrije Praktijken, Landelijke Cliëntenraad against the State of de Netherlands. Case number / cause list number: C/09/550982 / HA ZA 18-388.* 5/02/2020. Versión en inglés. [en línea] [Fecha de consulta: 22/04/2021].
[https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878]

3. LA AFECTACIÓN DE LOS MECANISMOS DE SEGUIMIENTO Y CONTROL A LOS PRINCIPIOS Y DERECHOS DE PROTECCIÓN DE DATOS.

Las tecnologías más utilizadas no se han diseñado por defecto para garantizar la privacidad ni los derechos de protección de datos de los usuarios sino para permitir su funcionalidad. Esto se traduce en que, si el usuario pretende una expectativa razonable de privacidad, debe tomar la iniciativa para modificar las configuraciones de dispositivos y plataformas, aunque no siempre sea posible modificar esas preferencias. Lo propio sucede si sufre algún menoscabo en sus derechos y libertades. Enrique Badía, en referencia a la responsabilidad que las tecnológicas endilgan al usuario por el manejo de sus datos y respecto al principio de transparencia, estableció: *Ciertamente, la transparencia surge como un elemento imprescindible, acaso en teoría idóneo e insuperable, para permitir al usuario el libre albedrío sobre sus datos personales. [...] nadie mejor que la propia persona para determinar y decidir quién, cómo, cuándo y para qué pueda utilizarlos, difundirlos o, en su caso, comercializarlos. […] ningún marco se puede considerar idóneo si su esencia descansa en una suerte de sobrecarga sobre el usuario*[95]. En la economía de la atención y explotación de datos, los usuarios interactúan con infraestructuras complejas que escapan al nivel común de entendimiento. En una reconocida sentencia del Tribunal Constitucional Federal Alemán, se reconoció el derecho fundamental de garantía de la confidencialidad e integridad de los sistemas de tecnología de información como una manifestación del derecho de autodeterminación informativa. El Tribunal, analizó la constitucionalidad de una ley que permitía a los servicios de inteligencia utilizar mecanismos de vigilancia secretos para infiltrarse en los sistemas de los objetivos sin conocimiento ni consentimiento de ellos. Se desarrollaron detalladamente las afectaciones de los sistemas tecnológicos de información en la conformación de la personalidad de los sujetos. Además, se describió el funcionamiento de las redes y sistemas advirtiendo el limitado control que un usuario con conocimiento medio ostenta frente a la amenaza de que terceros puedan acceder a su información personal. Se consideró: *[...] la conexión en red del sistema proporciona acceso técnico a terceros que puede utilizarse para espiar o manipular los datos del sistema. En algunos casos, el individuo ni siquiera puede percibir dicho acceso, sino que solo puede defenderlo hasta cierto punto. Los*

[95] BADÍA, Enrique. Marco conceptual. Derecho ¿pendiente?. En: Jorge Pérez y Enrique Badía. *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados.* Primera edición. Editorial Ariel. Madrid. 2012 P.19.

sistemas de tecnología de la información han alcanzado ahora un grado de complejidad tan alto que una autoprotección social o técnica eficaz puede plantear dificultades considerables y al menos abrumar al usuario medio.[96]

Los principios de protección de datos están para limitar los excesos de la tecnología sobre los derechos y libertades. El principio de protección de datos desde el diseño y por defecto, busca que no se inserten programas espías de seguimiento sin el consentimiento afirmativo y explícito del usuario; los otros principios buscan que la recogida y tratamientos no se lleven a cabo sin previa información completa de quiénes serán los destinatarios, con qué finalidades y durante cuánto tiempo se utilizarán. Estas bases ya habían sido asentadas en la sentencia del Tribunal Constitucional Alemán N° 209 del año 1983 mencionada en el apartado de evolución normativa y jurisprudencial, donde se estableció: [...] *Quien no pueda estimar con suficiente seguridad, qué informaciones sobre sí mismo son conocidas en determinadas esferas de su medio social, y quien no pueda de algún modo valorar el conocimiento previo que los posibles interlocutores tienen de uno mismo, puede verse restringido esencialmente en su libertad para planear o decidir con base en su propia autodeterminación. Un ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos, serían incompatibles con el derecho a la autodeterminación informativa.* [97]

Se deben proporcionar herramientas y mecanismos eficaces de control y disposición de la información personal. En la realidad virtual, no resulta fácil reivindicar los poderes de disposición y control a los que se aludían en las sentencias del Tribunal Constitucional Español como manifestación del ejercicio del derecho de libertad informática.

En el panorama de las asimetrías aludido a lo largo del trabajo, pareciera que la autodeterminación informativa implica un esfuerzo adicional a cargo del usuario para hacerlo valer. Un claro ejemplo de lo expuesto es el emblemático caso *"Costeja*

[96] Sentencia del Tribunal Constitucional Federal Alemán. BVerfG de 27 de febrero de 2008. Caso: 1 BvR 370/07. Párrafo 180. [en línea] [Fecha de consulta: 17/06/2021]. [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html].

[97] Tribunal Constitucional de la República Federal de Alemania. Sala Primera (Ref. BVR 209/1983). Párrafo 146. [en línea] [Fecha de consulta: 17/06/2021]. [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html]. Véase la versión traducida al idioma español por Manuel Daranas: "Sentencia de 15 de diciembre de 1983: Ley del Censo. Derecho de la Personalidad y Dignidad Humana". Boletín de Jurisprudencia Constitucional. Dirección de Estudios y Documentación del Congreso de los Diputados, vol. IV, núm. 3, enero de 1984, Madrid. pp. 126-170.

González" que ha sido paradigmático a nivel global en la reivindicación efectuada por un interesado respecto del ejercicio de su derecho de libertad informática ante un gigante de Internet. En dicha sentencia se sostuvo: *[...] un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales.*[98] La tecnología puede cercenar el ejercicio de los derechos cuando los caminos son intrincados y lentos de transitar. Estas características generan que los interesados se den por vencidos en su búsqueda de autodeterminación informativa. No resulta razonable atravesar por los escollos padecidos por *Costeja* para hacer efectivos derechos en el entorno digital. En el fallo se proclamó el *"derecho al olvido"* y ha tenido repercusiones globales.

Los poseedores, o mejor dicho, mercaderes de datos no siempre ofrecen procedimientos expeditivos para controlarlos y disponerlos. Según Shoshana Zuboff, en el capitalismo de la vigilancia se anulan los derechos elementales asociados a la autonomía individual.[99]

Las nuevas normativas de protección de datos han intentado corregir estas asimetrías, pero como se ha expuesto con los diversos casos traídos a colación, en el ámbito digital abundan tecnologías, técnicas y fenómenos que resisten con éxito la autoridad de la ley.

La libertad informática pese a encontrarse seriamente regulada, encuentra dificultades de eficacia atento a la influencia de los factores abordados. Se ha señalado: *las prácticas desleales de las compañías, la estructura difusa y afortunadamente ácrata de Internet y la desinformación que envuelve las acciones tomadas por los usuarios contribuyen a que estos no sean capaces de ejercer sus derechos de autodeterminación informativa.*[100]

Asimismo, Piñar Mañas, en esta línea aludió: *Ante los avances tecnológicos, este derecho sigue evolucionando para hacer frente a nuevos y sofisticados ataques que pueden amenazar su contenido y razón de ser.*[101] No se ha de ceder en la cautela y

[98] STJUE (Gran Sala), de 13 de mayo de 2014, asunto C-131/12. Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González. [en línea][Fecha de consulta: 02/05/2021][https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES]
[99] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia...*, cit., p 26.
[100] NOAIN SÁNCHEZ, Amaya. *La protección de la intimidad...*, cit., p 430.
[101] PIÑAR MAÑAS, José Luis. *Seguridad, transparencia y protección de datos...*, cit., p 10.

protección del derecho de libertad informática, mientras el instituto no permanezca estático, el dinamismo implica progreso.

4. EL ADVENIMIENTO DE LOS DERECHOS DIGITALES

Los avances tecnológicos generan cambios normativos que intentan armonizar, adecuar y equilibrar las asimetrías de conocimiento y poder. Luego de la aparición del RGPD, en España se sancionó la Ley Orgánica 3/2018, que incluyó en el Título X un elenco de derechos digitales. A partir del apartado IV del Preámbulo se preconiza el reconocimiento con rango constitucional de los derechos digitales, y a su vez, se menciona que los mismos encuentran anclaje en el artículo 18.4 de la Constitución Española. Es decir, en el derecho fundamental de libertad informática. En noviembre del 2020, se sometió a consulta pública una Carta de Derechos Digitales impulsada por el Ministerio de Asuntos Económicos y Transformación Digital Español, donde se estableció expresamente: *no trata de descubrir nuevos derechos fundamentales sino de concretar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros.*[102]

Sin entrar en la valoración de la técnica legislativa de la Ley Orgánica 3/2018, el debate estriba en si efectivamente estamos en presencia de nuevos derechos o no.

Pareciera, *a priori,* que no era necesario legislar "nuevos derechos digitales", pues en realidad, los derechos agregados como nuevos, encontraban acogida en el marco normativo vigente en las leyes y principios que rigen la protección de datos personales. Sin perjuicio de ello, no se suele aclarar el entorno donde se suscita la controversia o se pretenda reivindicar el derecho. Tal vez, mejorando la técnica legislativa se pueda incluir tecnologías, fenómenos y técnicas, no existentes hasta la fecha.

Sin duda en el entorno digital las novedades desarrolladas en el presente colisionan con las normas y principios, sin embargo, es la tecnología la que debe adecuarse a la ley y no la ley a la tecnología. La modernización de derechos tradicionales no siempre debe conllevar la creación de "nuevos derechos", y menos en un escenario que como se dijo, se encuentra considerablemente regulado. Se ha sostenido: *vivimos ya en una "law-saturated society", una sociedad repleta de derecho, de reglas jurídicas de las más*

[102] Carta de los Derechos Digitales. [en línea] [Consultado con fecha: 8/06/2021]. [https://www.mptfp.gob.es/portal/funcionpublica/secretaria-general-de-funcion-publica/Actualidad/2020/11/2020-11-19.html]

variadas procedencias, dictadas por públicos o privados, con una intensidad que evoca no tanto una necesidad como una imparable deriva. La conciencia social no acaba de estar a la altura de la complejidad de un fenómeno como éste que produce asimetrías y desequilibrios enormes, espacios llenos y vacíos con un derecho demasiado presente en algunos ámbitos y a la vez ausente en lugares en que sería más necesario."[103] Todos los fenómenos, tecnologías y técnicas analizadas en el presente trabajo se encuentran previstas y reguladas en el derecho vigente, lo que permite que sea factible abordarlas si se garantizara el cumplimiento efectivo del derecho de libertad informática.

IV. IMPLICACIONES JURÍDICAS DE LOS PRINCIPALES MECANISMOS DE SEGUIMIENTO Y CONTROL DEL USUARIO EN EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

"El capitalismo de la vigilancia emplea muchas tecnologías pero no podemos equipararlo a ninguna. Puede que para sus actividades utilice plataformas, pero esas actividades no son lo mismo que las plataformas de las que se vale para ellas. Emplea inteligencia de máquinas pero no es reducible a esas máquinas. Produce algoritmos y depende de ellos, pero capitalismo de la vigilancia y algoritmos no son lo mismo."

ZUBOFF, Shoshana[104]

Aunque a lo largo del trabajo se señalaron diversas repercusiones jurídicas sobre los temas abordados, se entrará de manera más específica sobre las repercusiones legales de diversos patrones detectados en los casos desarrollados. En el presente capítulo se pretende congregar ciertos aspectos que tienen en común las técnicas y tecnologías aludidas (junto con otras no desarrolladas) que inciden en el control y dirección de las acciones de los usuarios acerca de la información que les concierne.

En la actualidad, fenómenos como el filtro burbuja, la automatización de procesos y servicios de organizaciones privadas y administraciones públicas se llevan a cabo valiéndose de tecnologías como la inteligencia artificial, el *big data* y computación en la nube[105], entre otras. El libro blanco de la inteligencia artificial elaborado por la

[103] RODOTÁ, Stefano. *La vida y las reglas. Entre el derecho y no derecho*. Traducción de GREPPI, Andrea. Trotta. Madrid. 2010. Pp 25 y 26.

[104] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia*..., cit., p 31.

[105] Vid; GIL GONZÁLEZ, Elena. *Big data, privacidad y protección de datos.* Madrid, España. Agencia Española de Protección de Datos. 2016. P.132-133. La autora se refiere a los desafíos que presenta la computación en la nube para el derecho de protección de datos. En este sentido se refirió: *Gracias a la computación en nube, los datos se transfieren y cambian de manos de forma veloz y poco transparente para el individuo, incluso fuera de las fronteras europeas. Esto provoca una pérdida de control de los*

Comisión Europea lo pone en evidencia al sostener: *La inteligencia artificial es una de las partes más importantes de la economía de los datos. Hoy en día, la mayor parte de los datos son relativos a los consumidores y se almacenan y tratan en infraestructuras ubicadas en nubes centralizadas [...]*.[106] Los casos desarrollados en capítulos anteriores, se interrelacionan (y en ocasiones se conforman) con estas tecnologías y comparten patrones similares que se replican en el entorno digital en perjuicio de los usuarios y evidencian la existencia de asimetrías de conocimiento y de poder. En este sentido, Zuboff sostiene que: *Los capitalistas de la vigilancia lo saben todo sobre nosotros pero sus actividades están diseñadas como lo están para que no puedan ser conocidas por nosotros.*[107]Además, alude a que uno de los problemas más destacados es *el hecho de que nuestros derechos de decisión se disipen antes incluso de que sepamos que teníamos alguna decisión que tomar*.[108]

Cuando se analizan técnicas; tecnologías y fenómenos, resulta de gran utilidad tener como referencia los principios,[109]a los efectos de medir el compromiso de aquéllas respecto del cumplimiento y respeto de los derechos y libertades de las personas. Puede ser relevante valorar el enfoque adoptado sobre la protección de datos desde el diseño y por defecto,[110] como también, si se observa la concesión a los usuarios de mecanismos eficaces para el ejercicio de sus derechos de protección de datos[111]. Se propone destacar la existencia de características semejantes advertidas tomando como parámetro los indicadores mencionados. Así, se ensaya a tenor de los objetivos del trabajo, una sistematización de esas similitudes, de carácter meramente enunciativo y no taxativo ni limitado, a saber: patrones asociados al incumplimiento del deber de información; a la

---

datos por parte del individuo a quien le resulta muy complejo tomar decisiones para prestar su consentimiento.

[106] Comisión Europea. *Libro blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.* [en línea]. [Fecha de consulta: 15/04/2021] [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf]

[107] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia*..., cit., p 25.

[108] Ibidem. p.134.

[109] Vid; PIÑAR MAÑAS, José Luis. Identidad y persona en la sociedad digital. En: Tomás de la Quadra-Salcedo-José Luis Piñar Mañas. *Sociedad Digital y Derecho.* Primera edición. Madrid, España: Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. 2018. Capítulo pp. 95-111. P. 109.

[110] Vid; MANTELERO, Alessandro. Ciudadanía y gobernanza digital entre política, ética y derecho. En: Tomás de la Quadra-Salcedo-José Luis Piñar Mañas. *Sociedad Digital y Derecho.* Primera edición. Madrid, España: Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. 2018. Capítulo pp. 159-178. P. 167.

[111] Vid; SÁNCHEZ DEL CAMPO REDONET, Alejandro. Inteligencia artificial y privacidad. En: José, LÓPEZ CALVO. *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD.* Segunda edición. Las Rozas (Madrid). Wolters Kluwer. 2019. Pp. 983-995. p. 987.

falta de disposición y control de los datos por parte del usuario, la relevancia del consentimiento y los defectos de diseño en el entorno digital.

1. PATRONES ASOCIADOS AL INCUMPLIMIENTO DEL DEBER DE INFORMACIÓN

"Power derived from knowledge, and knowledge defined by power, can be all the more dominant when there is an asymmetry of knowledge between two parties."

Carissa Véliz[112]

El deber de informar y el derecho a la información es determinante en Internet y se proyecta transversalmente en otros derechos y libertades de los usuarios. Si se vulnera la información, si no se proporciona de manera adecuada y suficiente, aumentan las desigualdades, convirtiéndose el contexto virtual en un lugar oscuro donde unos pocos manejan la información de muchos. En palabras de Carissa Véliz, la economía de la vigilancia es mala porque crea y aumenta asimetrías indeseables de poder.[113]

Además, tiene implicaciones en los principios de protección de datos ya analizados, puede viciar el consentimiento de los usuarios y condicionar su libertad de acción y elección. Noain Sánchez, pondera este instituto del derecho a la información a los fines del ejercicio del derecho a la autodeterminación informativa, expresando con contundencia: *Un ciudadano informado es capaz de llevar a cabo, de manera activa, su potestad sobre sus informaciones privadas y personales y, en definitiva, sus derechos a la intimidad y vida privada, valorando, en consecuencia, cuándo desplegar cierta información sin que eso suponga un riesgo para la preservación de su ámbito reservado. […]*.[114] Además, plantea y argumenta que en el entorno digital, y específicamente en las plataformas, *[...] el individuo no obtiene la suficiente información para interpretar las normas que operan en los escenarios, por cuanto los flujos de información no son transparentes e implican un grado de complejidad que dificultan la comprensión y posterior toma de decisiones.*[115] En el entorno digital la información es abundante, insuficientemente suministrada, difusa y en consecuencia, altera la capacidad de acción y decisión de los usuarios.

---

[112] VÉLIZ, Carissa. *Privacy is power*. *Why and how you should take back control of your data.* Primera edición. Reino Unido: Bentham Press, Penguin Random House 2020. p. 53.
[113] Ibidem. P 4.
[114] NOAIN SÁNCHEZ, Amaya. *La protección de la intimidad...*, cit., pp 219-220.
[115] Ibidem. P. 220.

Aunque durante los últimos años, diversas autoridades de protección de datos europeas, entre ellas ICO[116]; CNIL[117] y la AEPD[118], se han mostrado muy comprometidas con la persecución y sanción de incumplimientos al deber de información en materia de *cookies*, no han sido muchos los asuntos que han llegado a instancias judiciales. El Tribunal de Justicia de la Unión Europea, destacó en primer lugar, que toda información recogida por *cookies* debe ser protegida aunque no se trate de datos personales. En este sentido, sostuvo: *[...] toda información almacenada en el equipo terminal de los usuarios de una red de comunicaciones electrónicas forma parte de la esfera privada de los usuarios, que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta protección se aplica a toda información almacenada en dicho equipo, con independencia de si se trata de datos personales o no, y tiene como finalidad, en particular, según se desprende de ese mismo considerando, proteger a los usuarios contra el riesgo de que identificadores ocultos u otros dispositivos similares puedan introducirse en el equipo terminal del usuario sin su conocimiento.*[119] Surge con claridad que se refiere a las *cookies* y tecnologías de seguimiento afines al referirse a "identificadores ocultos u otros dispositivos similares".

En otro orden de cosas, establece la manera en que debe ser suministrada la información a los usuarios para que puedan comprender el funcionamiento de las *cookies: una información clara y completa debe permitir al usuario determinar fácilmente las consecuencias de cualquier consentimiento que pueda dar y garantizar que dicho consentimiento se otorgue con pleno conocimiento de causa. Debe ser claramente comprensible y suficientemente detallada para que el usuario pueda comprender el funcionamiento de las cookies empleadas.*[120]Aunque se abordará el consentimiento más

[116] Sitio Web oficial de la autoridad de aplicación de protección de datos del Reino Unido donde publica las acciones llevadas a cabo sobre las Cookies. Information Commissioner´s Office. [en línea]. [Fecha de consulta:19/4/2021] [https://ico.org.uk/action-weve-taken/cookies/]

[117] AYUSO, Silvia. *Francia multa con 100 millones de euros a Google y 35 a Amazon por no informar a los usuarios de las 'cookies'*. [en línea]. [Fecha de consulta: 19/04/2021]. [https://elpais.com/economia/2020-12-10/francia-multa-con-100-millones-de-euros-a-google-y-35-a-amazon-por-no-informar-a-los-usuarios-de-las-cookies.html]

[118] Agencia Española de Protección de Datos. "Memoria AEPD 2019". p.80 [en línea]. [Fecha de consulta:19/4/2021] [https://www.aepd.es/sites/default/files/2020-05/memoria-AEPD-2019.pdf]

[119] Tribunal de Justicia de la Unión Europea, 1/10/2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V./Planet49 GmbH (Asunto C-673/17).* [en línea]. [Fecha de consulta 19/04/2021]. [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62017CJ0673&from=EN]

[120] Ibidem.

adelante, se evidencia la clara relevancia de la manera que debe proporcionarse la información en el entorno digital para la adecuada toma de decisiones.

Otro aspecto de la información que aborda la sentencia en cuestión, refiere a la temporalidad de los tratamientos y el acceso de terceras partes a la información: *la información que el proveedor de servicios debe facilitar al usuario de un sitio de Internet incluye el tiempo durante el cual las cookies estarán activas y la posibilidad de que terceros tengan acceso a ellas.*[121]

Los considerandos 39 y 60 del RGPD, ponen énfasis a la importancia de suministrar a los interesados la información suficiente y complementaria, de manera clara y sencilla en relación al tratamiento de sus datos personales y la forma de ejercer sus derechos. Involucra actividades de tratamiento, la elaboración de perfiles, los fines y las consecuencias derivadas de estas circunstancias. Por último, se exige que la información tenga que ser proporcionada de manera "inteligible", "fácilmente visible" y "claramente legible", extremos no observados en los casos analizados en el trabajo como la utilización de patrones oscuros, las *cookies* y la ausencia de referencia sobre los riesgos que pueden entrañar los filtros burbuja.[122]

Recientemente en relación a los identificadores ocultos, la Asociación *"NOYB"* interpuso una reclamación contra *Google* ante la Autoridad de protección de datos francesa, CNIL.[123] Se acusó a la empresa de introducir identificadores ocultos sin el consentimiento de los usuarios en violación al artículo 5.3 y considerando 24° de la Directiva 2002/58/CE.[124]

Resulta oportuno recordar cuando *Disconnect Inc.*, una empresa desarrolladora de software para móviles, presentó una reclamación similar contra *Google* ante la Comisión Europea.[125] En ella se denunció entre otras cosas, la inserción y explotación

[121] Ibidem.
[122] Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
[123] Reclamo de la Asociación NOYB vs. Google presentada ante CNIL, versión en Inglés y Francés. [en línea] [Fecha de consulta: 7/06/2021]. [https://noyb.eu/sites/default/files/2021-04/AAIDcomplaint_Redacted.pdf]
[124] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).
[125] Reclamación de *Disconnect Inc.* presentada contra *Google* ante la Comisión Europea en Junio del 2015. [En línea] [Fecha de consulta: 16/06/2021]
[http://assets.documentcloud.org/documents/2109044/disconnect-google-antitrust-complaint.pdf]

de mecanismos invisibles de seguimiento sin conocimiento ni consentimiento de los usuarios a los fines de perfilamiento publicitario. La reclamación, además, tuvo trascendencia porque denunció las prácticas desleales y abuso de posición dominante de la gigante tecnológica a la que sancionaron severamente.[126]

La falta de información es frecuente en todos los casos analizados en el trabajo, y de ello, se deriva directamente el incumplimiento de los principios de protección de datos afectando el poder de decisión del usuario. Paula Ortiz López se ha referido al respecto: *los algoritmos aplicados a los datos desempeñan un papel cada vez más importante en la información que reciben los individuos, porque, entre otras cosas, puede influenciar sus orientaciones y acciones individuales y sociales. [...] En muchas ocasiones se oculta a los ciudadanos el riesgo y la dimensión del control social que se puede realizar mediante el tratamiento y vigilancia de las redes sociales y otros servicios con el uso del Big Data.* [127] El fenómeno del filtro burbuja y sus consecuencias colectivas se identifican con lo postulado. Lo propio sucede con las tecnologías de seguimiento analizadas.

2. EL DERECHO DE AUTOCONTROL SOBRE LOS PROPIOS DATOS

La información brindada de manera correcta permite a los usuarios tomar decisiones. La cuestión se torna controvertida cuando el usuario no es capaz de tomar una decisión ya sea porque carece de información o porque el poder de decisión lo ostenta una máquina.

El RGPD ha previsto en el considerando 71 la prohibición de la elaboración de perfiles de los interesados exclusivamente automatizadas sin intervención humana. Además, ante el requerimiento, se deben brindar explicaciones respecto de las decisiones adoptadas por los programas y la posibilidad de impugnarlas. En el considerando 75, refiere a los riesgos que se exponen los derechos y libertades de los interesados y, entre ellos, se contempla la pérdida de control de sus datos personales.[128] Gil González se ha referido a la consternación por parte de los legisladores europeos por limitar la actividad

[126] Decisión de la Comisión Europea del 18/07/2018. Caso N° 40099. [en línea] [Fecha de consulta 16/06/2021][https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf]

[127] ORTIZ LÓPEZ, Paula. La ética en el tratamiento de los datos digitales para un futuro sostenible. En: Paloma, LLANEZA GONZÁLEZ. *Ellas.Retos, amenazas y oportunidades en un mundo conectado.* Primera edición. Las Rozas, (Madrid) España: Wolter Kluwer, 2019. P 142-143.Capítulo: Pp. 138-161.

[128] Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

de elaboración de perfiles y la toma de decisiones individuales automatizadas en el RGPD.[129] Este extremo será en un futuro no lejano de difícil cumplimiento.

Se ha afirmado que: *estamos entrando en una era en la que las acciones de los individuos serán jugadas por estándares que no pueden controlar y donde ese juicio no puede ser borrado.*[130] Al respecto de la falta de transparencia e información relativa a la explicabilidad y comprensibilidad de los tratamientos y procesos que llevan a cabo estas plataformas, Caty O´Neil ha subrayado: *en los próximos años, enormes cantidades de datos conductuales irán directos a sistemas de inteligencia artificial que, a nuestros ojos, seguirán siendo cajas negras. [...] En la era de las máquinas inteligentes, la mayoría de las variables serán un misterio. [...] Estos programas automáticos determinarán cada vez más cómo nos tratarán el resto de las máquinas: las que escogen los anuncios que vemos, deciden los precios que debemos pagar, nos ponen en la lista de espera del dermatólogo o confeccionan nuestras rutas. Serán muy eficientes, aparentemente arbitrarias y no darán explicaciones de ningún tipo. Nadie podrá entender su lógica ni explicarla.*[131] En la misma línea, se señaló categóricamente: *Ahora los procesos automatizados llevados a cabo por máquinas no sólo conocen nuestra conducta, sino que también moldean nuestros comportamientos en igual medida.*[132] En el entorno digital predomina la falta de disposición y control de los datos personales, la oscuridad y la inescrutabilidad de códigos que gobiernan los programas.

Las tecnologías, técnicas y fenómenos buscan la personalización de los usuarios. Al respecto: *los tratamientos personales ligados al desarrollo de la sociedad digital, pueden por suministrar información significativa de la persona y porque lo hacen sin que ésta repare en esta realidad ni en que se usa para influirle, producir esta incidencia manipulativa y consecuentemente pueden mermar o incluso anular la*

[129] GIL GONZÁLEZ, Elena. *Big data, privacidad...*, cit., p 123.
[130] BOTSMAN, Rachel. *Big data meets Big Brother as China moves to rate its citizens*. [en línea] [Fecha de consulta: 02/05/2021] [https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion]
Extracto traducido a los fines del presente trabajo: *[...] We are entering an age where an individual's actions will be judged by standards they can't control and where that judgement can't be erased*.
[131] O´NEIL, Cathy, *Armas de destrucción matemática*. *Cómo el big data aumenta la desigualdad y amenaza la democracia*. ARRANZ DE LA TORRE, Violeta. Trad. Primera edición. Madrid. Capitan Swing Libros, S.L. 2017. Versión traducida al español. P. 213.
[132] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia*..., cit., p 21.

privacidad del sujeto entendida como espacio de libre decisión o, dicho en otras palabras, de autonomía personal.[133]

El poder de los algoritmos puede configurar la identidad de una persona. Afirmó Piñar Mañas: *una identidad controlada, diseñada y vigilada. […] pone en cuestión el propio derecho al libre desarrollo de la personalidad.*[134] Así, la repercusión toma una dimensión preocupante, *[...] en definitiva el algoritmo va a adecuar procesos a nuestros gustos, por lo que no será fácil objetar las indicaciones que de ello deriven. Pero al mismo tiempo puede cercenar la apertura y diversificación de la personalidad y por tanto de la propia identidad*.[135]Como consecuencia, el autor concluye que el ser humano será más controlable y maleable.[136]

No escapará al lector que la personalización pone en riesgo el autocontrol de los datos personales, afectando el libre desarrollo de la personalidad y con ello, la conformación de la identidad de las personas en el entorno digital vulnerando la libertad informática. Asimismo, la ocultación de información y las dinámicas de los algoritmos destinadas a influir en las conductas, perturban y afectan el consentimiento.

3. EL CONSENTIMIENTO COMO CONDICIÓN DE LICITUD PARA LA RECOGIDA Y TRATAMIENTO DE LOS DATOS

Actualmente a nivel europeo se exige el consentimiento explícito como base legal primordial del tratamiento de datos personales, pero hay quienes consideran que esta circunstancia puede ser contraproducente. Elena Gil González refiere: *la normativa confía demasiado en el consentimiento informado del individuo para recopilar y tratar sus datos de carácter personal. Esto supone un problema dada la experiencia de que la mayoría de los individuos no lee las políticas de privacidad antes de prestar consentimiento; y aquellos que lo hacen no las comprenden. Así, otorgar el consentimiento es con carácter general un ejercicio vacío.*[137]

---

[133] HERNÁNDEZ CORCHETE, Juan Antonio. Expectativas de privacidad, tutela de la intimidad y protección de datos. En: Tomás DE LA QUADRA SALCEDO, José Luis PIÑAR MAÑAS. *Sociedad Digital y Derecho*. Primera edición. Madrid, España: Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. 2018. p 281. Capítulo Pp. 279-300. P.282.

[134] PIÑAR MAÑAS, José Luis. Identidad y persona en la sociedad digital..., cit., p 102.

[135] Ibidem.

[136] Ibidem.

[137] GIL GONZÁLEZ, Elena. *Big data, privacidad*..., cit., p 53.

Sin duda uno de los debates más candentes que existen sobre las *tecnologías de seguimiento y control* abordadas y la privacidad radica en el consentimiento informado del usuario. En la sentencia del Tribunal de Justicia de la Unión Europea citada, se analizó la legalidad del consentimiento en materia de *cookies* y tecnologías de seguimiento dejando valiosos aportes sobre la cuestión. Definió que el consentimiento: *no se presta de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de cookies se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento.*[138] Valga recordar lo ya mencionado respecto del consentimiento debe ser prestado con pleno conocimiento de causa.

En esta nueva economía basada en datos, los datos personales no pueden ser utilizados y explotados sin la participación del interesado. Es necesario que las personas sean parte de la negociación. [139] No sólo formar parte de la negociación, además, quienes realicen tratamientos sobre los datos de los interesados, deben ampararse en consentimientos válidos. También deben proporcionar canales efectivos para revocar el consentimiento y eliminar las *cookies.*[140]

El proyecto de Reglamento "e-Privacy" resulta esclarecedor respecto de la polémica privacidad y las *cookies* (y tecnologías similares). El proyecto aborda de manera completa el asunto y lo analiza en varios considerandos (20 - 24) y también proporciona un informe de evaluación que clarifica la controversia de estas tecnologías y la vida privada de los interesados. Esto evidencia lo indicado al principio del trabajo sobre la relevancia que ocupan en el entorno digital. En el considerando 20 se explica detalladamente cómo los dispositivos que utilizan los usuarios y la información que se genera con su interacción, forman parte de su esfera privada y advierte de la necesidad de su protección. Se señala expresamente, que las *cookies* de rastreo y tecnologías similares, pueden introducirse en el equipo terminal del usuario sin su consentimiento lo

[138] Tribunal de Justicia de la Unión Europea, 1/10/2019, *"Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V./Planet49 GmbH (Asunto C-673/17)"* [en línea]. [Fecha de consulta 19/04/2021] [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62017CJ0673&from=EN]

[139] ORTIZ LÓPEZ, Paula. La ética en el tratamiento..., cit., pp 142-143.

[140] PANIZA FULLANA, Antonia. El comercio electrónico y la protección del consumidor internauta. En: Francisco, PÉREZ BES. *El derecho de Internet. Primera edición. Atelier. Barcelona. 2016. Pp. 125-143. P.143.*

cual puede suponer una grave intromisión en la vida privada por lo que se requiere el consentimiento expreso.[141]

Estos extremos durante muchos años no fueron observados ni cumplidos por los desarrolladores, controlados por los usuarios ni exigido por las autoridades. Estas técnicas y tecnologías se encuentran presentes en el entorno digital desde prácticamente la vida comercial y global de Internet. No se escapará que muchos debates sobre estos temas continúan vigentes a la fecha.

El proyecto de Reglamento aludido deja asentada la importancia del consentimiento en las comunicaciones electrónicas y tratamientos de datos de los interesados debido a los elevados riesgos que entrañan para sus derechos y libertades.

4. LOS DEFECTOS DE DISEÑO QUE AFECTAN A LOS USUARIOS

El RGPD en el considerando 78 y el artículo 25, aluden a la protección de datos desde el diseño y por defecto[142]. Se imponen obligaciones a los responsables, encargados y productores de tecnologías tendientes a reducir los tratamientos innecesarios, proporcionar transparencia a los mismos, y brindar facultades de supervisión para los interesados. Entre las obligaciones se encuentra la implementación de medidas técnicas y organizativas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Sin embargo, en las técnicas y tecnologías de la sociedad digital predominan patrones de diseño que no se ajustan a las normas previstas. Los ardides en las deficiencias informativas y afectaciones al consentimiento desarrollados en el apartado anterior no son hechos accidentales.

En el capítulo donde se explicaron los patrones oscuros, se hizo referencia a la utilización de diseños de interfaces, avisos e informaciones suministradas a los usuarios destinadas a influenciar, manipular o incidir en su comportamiento y libertad de

[141] Comisión Europea. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)[en línea]. [https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010]

[142] Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

elección. Las deficiencias informativas afectan los principios de protección de datos y amenazan el poder de decisión del usuario.

Pero los defectos de diseño, en una concepción más general no sólo se exteriorizan a través de anuncios visibles, también, pueden encontrarse incrustados en las propias infraestructuras y códigos que subyacen las tecnologías que se benefician a costa de los datos de los usuarios. Noain Sánchez sostuvo: *la Web semántica no está diseñada para respetar la coherencia del contexto, ni para satisfacer plenamente los deseos de protección de la información y autodeterminación informativa de las personas.*[143]

Se puede apreciar que el ámbito virtual está edificado con deficiencias estructurales que inciden en la privacidad y protección de datos desde el diseño y por defecto. Juan Antonio Hernández Corchete contextualizado en el análisis de la economía basada en datos y los modelos de negocios que se benefician de aquellos, señaló: *siendo posible obtener información significativa de un usuario con el fin de comunicarle publicidad que sea de su interés o prestarle otro servicio de análisis que le beneficie, es igualmente factible hacerlo con propósitos que, prescindiendo absolutamente de su interés, se orienten a condicionar sus decisiones para ventaja exclusiva de un tercero.*[144] Con esto se quiere puntualizar que muchas las herramientas y tecnologías que se están desarrollando se diseñan con fines específicos que no siempre respetan los principios de la protección de datos.

No todo transcurre en el mundo privado, y los defectos de diseño pueden ser relevantes para la privacidad y protección de datos. En el caso resuelto por la Corte de la Haya aludido, se prohibió el uso del algoritmo llamado *SyRI* que utilizaba el Estado Holandés para detectar fraudes de los ciudadanos al sistema de bienestar social.[145] Se cuestionó por parte de un grupo de activistas que el Estado hacía uso del algoritmo sin ningún tipo de transparencia respecto de lo que hacían con los datos de los ciudadanos sin ofrecer garantía alguna ni información acerca de qué datos estaban siendo analizados y tratados por *SyRI*.[146]

---

[143] NOAIN SANCHEZ, Amaya. *La protección de la intimidad...*, cit., p 414.

[144] HERNÁNDEZ CORCHETE, Juan Antonio. Expectativas de privacidad..., cit., p 281.

[145] VERVLOESEM, Koen. "*How Dutch activists got an invasive fraud detection algorithm banned"*.[en línea][Fecha de consulta: 22/04/2021][https://algorithmwatch.org/en/syri-netherlands-algorithm/].

[146] Corte de la Haya. Caso: *NJCM, Platform Bescherming Burgerrechten, Privacy First, Koepel van DBC-Vrije Praktijken, Landelijke Cliëntenraad against the State of de Netherlands. Case number / cause*

Aunque sólo se ha tenido acceso a la resolución en una versión en inglés, se tradujo a los propósitos del presente la parte pertinente del considerando 6.7: *"La legislación SyRI no reúne los requerimientos sobre los que se asienta el artículo 8 parágrafo 2 del CEDH esa interferencia con el ejercicio del derecho al respeto de la vida privada es necesaria en una sociedad democrática, significa que debe ser necesaria proporcionada y subsidiaria en relación con la finalidad prevista. [...] La corte es de opinión que la legislación no logra el "equilibrio justo" requerido bajo la CEDH entre el interés social al que sirve la legislación y la violación a la vida privada a la que da lugar la legislación para calificar como violación suficientemente justificada de la vida privada. [...] La corte sostiene que la legislación perteneciente a la aplicación de SyRI es insuficientemente transparente y verificable.[...]"*[147]. En la resolución se cuestionó que el algoritmo por diseño no era transparente. La regulación que daba sustento a las condiciones de aplicación del sistema *SyRI*, había sido criticada y cuestionada por la autoridad de protección de datos holandesa. Concretamente, se puede concluir que de nada sirve una norma poco clara, transparente e inaccesible, para regular tecnologías que cuentan intrínsecamente con esas mismas características. Si la ley por diseño, peca por defecto en su función de limitar el uso de la tecnología, avanzando en su injerencia sobre los derechos fundamentales de las personas faltando al principio de proporcionalidad, estará condenada a la ineficacia.

Entre otras características que pueden derivar de las insuficiencias de diseño, se identifican: la naturaleza adictiva de las plataformas y la irreversibilidad de sus diseños.

4.1. *LA ADICCIÓN POR DISEÑO*

Lejos de respetarse las cautelas y garantías mencionadas en el apartado anterior, predominan en el entorno digital el desarrollo de tecnologías adictivas. Los diseños

---

list number: C/09/550982 / HA ZA 18-388. 5/02/2020. Versión en inglés.[en línea] [Fecha de consulta: 22/04/2021] [https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878]

[147] Ibidem. Considerando 6.7: *"The SyRI legislation does not meet the requirement laid down in Article 8 paragraph 2 ECHR that interference with the exercise of the right to respect for private life is necessary in a democratic society, meaning that it should be necessary, proportionate and subsidiary in relation to the intended purpose. The court weighs the substance of the SyRI legislation in light of the aims the legislation pursues against the violation of private life by the SyRI legislation. The court is of the opinion that the legislation does not strike the 'fair balance' required under the ECHR between the social interest the legislation serves and the violation of private life to which the legislation gives rise to qualify as a sufficiently justifiable violation of private life. The court takes into consideration the fundamental principles underlying the protection of data under Union law (the Charter and the GDPR), specifically the principles of transparency, purpose limitation and data minimisation. The court holds that the legislation pertaining to the application of SyRI is insufficiently transparent and verifiable.[…]."* Traducida al español por el autor a los fines del trabajo.

oscuros, pueden tener efectos perniciosos en perjuicio de la voluntad de los usuarios, encontrándose expuestos a engaños o manipulaciones a la hora de navegar por internet. Noain Sánchez sostuvo: *al examinar el papel que juegan ciertas aplicaciones de la Web 2.0 encontramos que su diseño y las estructuras constitutivas que sustentan dichas plataformas son todo, salvo neutras.*[148] Por su parte, Marta Peirano considera que las tecnologías que dominan la industria de la atención son diseñadas por expertos en comportamiento para generar adicción. Además, afirmó: *La tecnología que mantiene internet funcionando no es neutral, y la que encontramos o instalamos en nuestros teléfonos móviles tampoco.*[149] Sobre la plataforma *Youtube* sostuvo que es una de las plataformas más adictivas que cuenta con un potente algoritmo de recomendación basado en la personalización y completamente inaccesible. La autora refirió: *no podemos saber cómo lo hace porque es un algoritmo opaco, inauditable, una caja negra protegida por abogados, criptografía y leyes de propiedad intelectual.*[150]

Natasha Dow Schüll escribió un libro titulado: "*Addiction by Design*"[151], donde analiza este fenómeno del desarrollo de tecnologías adictivas, que buscan maximizar el tiempo de las personas con sus dispositivos.

Como derivación del diseño adictivo de las tecnologías, la dosificación de contenidos satisface las preferencias de los usuarios manteniéndolos encerrados en su burbuja de filtros, proporcionándoles contenidos acordes y confirmadores de sus gustos y deseos. Esa dependencia no es circunstancial, sino que es provocada. Se ha dicho: *nuestra dependencia es un elemento básico del proyecto de vigilancia comercial, en el que las necesidades que sentimos de aumentar la eficiencia en nuestra vida compiten con nuestra inclinación a resistirnos a tan osadas incursiones por parte de aquél.*[152]

Tristan Harris, un ex empleado de *Google*, escribió un artículo titulado: *"How Technology is Hijacking your mind- from a Magician and Google design ethicist"*. Sucintamente, relata cómo las tecnologías por diseño, secuestran las mentes de las personas. Sostiene que, aunque la mayoría de las personas defiendan su derecho de libertad de elección, ignoran que las elecciones a las que se someten en las plataformas

[148] NOAIN SÁNCHEZ, Amaya. *La protección de la intimidad*..., cit., p 304.
[149] PEIRANO, Marta. *El enemigo conoce el sistema*..., cit., pp 22-23.
[150] Ibidem. Pp 45-46.
[151] SCHÜLL, Natasha Dow. *Addiction by Design.Machine Gambling in Las Vegas*. Princeton University Press. 2014.
[152] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia*..., cit., p 25.

fueron manipuladas al proporcionar opciones no elegidas en primera instancia. Concretamente, afirma que las plataformas, como magos, crean la ilusión de que sus usuarios adoptan elecciones libres pero el menú provisto, ha sido diseñado para que las plataformas ganen sin importar las elecciones que aquéllos hagan. También, apunta a los diseños adictivos de las tecnologías que cuentan con recompensas de variables intermitentes que agudizan esa adicción.[153] En este mismo sentido, en referencia a las aplicaciones y plataformas, Paloma Llaneza, afirma: *[...] se crean, a propósito, ciclos repetidos de incertidumbre, anticipación y retroalimentación, dando de vez en cuando y de manera aleatoria unas recompensas, que siempre serán suficientes para que el usuario siga viniendo. Si uno osa a desconectarse, el servicio o la aplicación se encargará de mandar mensajes, ofertas o recompensas para llamar la atención del usuario y atraerlo de nuevo al servicio.*[154] En los casos analizados, si al usuario se le brinda la oportunidad de elegir, puede experimentar una falsa sensación de autonomía y libertad. Resulta una ilusión dado que las elecciones tomadas en los entornos digitales muestran opciones preestablecidas que, probablemente no contemplen alternativas que el usuario hubiera preferido. Al final de cuentas, lo que no figura como opción, no podrá elegirse, lo que implica que no existe. Como derivación de los defectos de diseño, se afecta también al poder de decisión abordado anteriormente.

4.2. *DINÁMICA DE IRREVERSIBILIDAD PREDOMINANTE EN LOS DISEÑOS*

Otra manifestación de la dependencia fomentada por las tecnologías consiste en la *dinámica de irreversibilidad* de sus diseños. Aunque el término no se lo atribuye el autor, Eli Pariser sostiene al respecto: *los usuarios están tan involucrados en su tecnología que, aunque los competidores tal vez ofrezcan mejores servicios, no merece la pena hacer el cambio.*[155]En la economía basada en datos, los propósitos escalables de los productos y servicios fomentan diseños de tecnologías cuyo costo de trasladar la información acumulada a otra, sea mayor que permanecer y seguir proporcionando datos e interacciones.

---

[153] HARRIS,Tristan. *How Technology is Hijacking your mind- from a Magician and Google design ethicist.* [en línea] [Fecha de consulta: 20/04/2021] [https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3]

[154] LLANEZA GONZÁLEZ, Paloma. *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*. Segunda edición. España. Editorial Planeta. Ediciones Deusto. 2019. P.143.

[155] PARISER, Eli. *El filtro burbuja...*, cit., p 49.

Se puede apreciar fácilmente que este patrón afecta íntegramente al derecho de portabilidad de los datos, desde que el diseño de la tecnología disuade al usuario de optar por otros productos y servicios. Esa dependencia de productos y servicios con tendencia ascendente acentúa las asimetrías de poder y conocimiento ya mencionadas. Recoger más información, aunque no comulgue con el principio de minimización, tiene un sentido específico, entrenar algoritmos de predicción. Shoshana Zuboff al abordar la explicación del término de *capitalismo de vigilancia*, manifestó: *reclama unilateralmente para sí la experiencia humana, entendiéndola como la materia prima gratuita que puede traducir en datos de comportamiento. Aunque alguno de dichos datos se utilizan para mejorar productos y servicios, el resto es considerado como un excedente conductual y se usa como insumo de procesos avanzados de producción conocidos como inteligencia de máquinas con los que se fabrican productos predictivos.*[156] Carissa Véliz argumentó que el motivo por el cual las compañías tecnológicas están mejorando tanto en la predicción de nuestro comportamiento, es porque parcialmente están dándole forma. Sustentó su punto de vista aduciendo: *si una compañía tiene el control sobre una porción significante de tu vida a través de tus dispositivos, si puede influenciar mediante la elección del contenido al que te da acceso y controla las plataformas mediante las cuales interactúas con otros, realizas compras y trabajas, entonces no es difícil predecir lo que harás después. Al final, te provee las opciones y te empuja en el camino*.[157]

En atención a lo desarrollado en el presente trabajo, la revolución tecnológica presenta de los más variados desafíos para los derechos y libertades de las personas. Depende de todos trabajar para reivindicarlos y bregar por que se garantice el cumplimiento de las leyes en lo que respecta a la limitación tecnológica. En palabras de Perez Luño: *La decisión sobre los impactos presentes y futuros de Internet en la esfera de las libertades, corresponde a los ciudadanos de las sociedades democráticas: se trata de una responsabilidad de la que no deben abdicar*.[158]

[156] ZUBOFF, Shoshana. *La era del capitalismo de la vigilancia*..., cit., p 21.
[157] VÉLIZ, Carissa. *Privacy is power*..., cit., p 74.
[158] PÉREZ LUÑO, Antonio E. Las libertades..., cit., p 397.

CONCLUSIONES

Tomando como referencia lo analizado, se ha arribado a las siguientes conclusiones:

1. *En el entorno digital predominan tecnologías, fenómenos y técnicas que influyen en el ejercicio eficaz del derecho de libertad informática por los usuarios.*

En el caso de las *cookies* y tecnologías similares de seguimiento y control, existe una ambigüedad terminológica que afecta al derecho de información de los usuarios. Resulta técnicamente posible introducir mecanismos de seguimiento y control sin consentimiento ni conocimiento de los usuarios. Aunque se eliminen las *cookies*, los usuarios y los dispositivos pueden ser identificados mediante otras técnicas de seguimiento. No se cumple con la configuración de preferencias ni se garantiza el derecho de oposición a distintos tratamientos.

En cuanto al fenómeno del filtro burbuja, el poder de decisión del usuario se encuentra anulado. La máquina decide. El usuario no elige entrar ni salir de la burbuja. Tampoco puede modificarla ni conocer las inferencias que sobre sus interacciones se realizan, ni sus riesgos. Mediante patrones oscuros, se intenta restringir la libertad de elección del usuario. Se instrumentan para influir en sus acciones y manipular las conductas camuflados en textos y colores.

En todos estos casos, se extrae información de los usuarios sin que éstos sean conscientes de sus repercusiones.

2. *Se contravienen los principios de protección de datos proyectándose a través de defectos en el suministro de información; en los diseños y en la falta de herramientas de control y disposición.*

En el caso de *cookies* y tecnologías similares, no siempre se cumple con el suministro de información adecuada. Prácticas como las pujas de tiempo real erosionan los derechos de protección de datos de los usuarios. No existen medios adecuados para auditar y controlar que se respetan las elecciones. Los *pixel* de seguimiento se insertan en correos no deseados ni solicitados por los usuarios y recolectan de manera ilegítima información personal.

En el filtro burbuja el usuario desconoce la información que no conforma la burbuja de filtros que lo rodea. No puede auditar ni controlar el proceso ni tratamiento de información. No existen mecanismos de corrección, oposición ni rectificación.

Los patrones oscuros pueden desalentar el ejercicio de los derechos de protección de datos en políticas de privacidad, avisos legales y otros documentos electrónicos.

En tecnologías como la inteligencia artificial, el *big data* y la computación en nube, los usuarios pierden el control y disposición de su información. No siempre pueden rectificar, portar, acceder, oponerse y eliminar la información que les concierne. Los procesos y tratamientos carecen de transparencia y contravienen principios como el de minimización, limitación de finalidad y plazo del tratamiento.

En todos los casos, no suelen proporcionarse medios y herramientas inteligibles a los interesados para controlar, disponer y realizar un seguimiento de la información que les concierne de acuerdo a sus preferencias.

3. *En el entorno digital predominan asimetrías de conocimiento y poder que afectan a la autodeterminación informativa del usuario.*

Los responsables de las tecnologías, fenómenos y técnicas analizadas, cuentan con más información de los usuarios que la que éstos conocen y pueden acceder sobre aquéllos.

Las políticas de privacidad, avisos legales y demás documentos electrónicos, no satisfacen el derecho de información y afectan la libertad informática. Se ocultan las identidades, finalidades y tratamientos de las “terceras partes”.

Recae sobre el usuario la carga de configurar los programas para evitar mantenerse en desventaja. No admiten mecanismos para equilibrar las asimetrías. Las normas buscan que el tratamiento se lleve a cabo luego de una acción afirmativa previa (*opt-in*), sin embargo, prevalece que los usuarios actúen para evitarlo (*opt- out*).

En el entorno digital, no se puede monitorear la información personal. No se garantiza el cumplimiento de la protección de datos desde el diseño y por defecto.

4. *En la actualidad, las tecnologías, fenómenos y técnicas analizadas no respetan el derecho de protección de datos en su faz positiva ni negativa.*

El derecho de protección de datos se proyecta mediante una faz negativa y otra positiva. Conforme a los casos analizados, no se cumplen las abstenciones, se manipula e incide en las decisiones de los usuarios. No se garantiza a los usuarios el poder de control y disposición de su información. Tampoco se brindan mecanismos efectivos para el ejercicio de los derechos de protección de datos.

5. *En una economía basada en datos, se diseñan productos y servicios escalables adictivos que fomentan la dependencia e impiden la libertad de elección.*

A medida que se utiliza un producto o servicio, se acumula información, lo que disuade y compromete el ejercicio del derecho de portabilidad y el de oposición. Así, resulta cada vez más difícil y menos conveniente prescindir de las plataformas. Se afecta el principio de minimización y limitación de conservación. A mayor información, mayor predicción lo que conlleva mayor personalización y mayor asimetría.

La inserción de identificadores ocultos en el entorno digital amenaza los principios de protección de datos y privan a los usuarios del poder de decisión en el ejercicio de sus derechos. Los algoritmos de personalización, ponen en riesgo el desarrollo de la libre personalidad y afectan la conformación de la identidad digital.

6. *La libertad informática es un instituto en constante evolución, pero de cumplimiento diferido.*

Aunque la libertad informática se encuentra regulada desde antes del surgimiento de los mecanismos abordados, no ha logrado impedir su desarrollo y evolución. Se ha intentado limitar a la tecnología con abundante legislación, pero al estar fragmentada, los esfuerzos de control y cumplimiento no han sido suficientes para disuadir las prácticas desleales de las compañías tecnológicas.

7. *Los datos seguirán siendo el combustible del desarrollo y puede especularse un aumento de su valoración en este contexto de tecnologías emergentes. El respeto por la privacidad y protección de datos no es óbice para la innovación.*

Es esencial no subestimar las consecuencias nocivas sobre los derechos y libertades individuales que pueden tener las tecnologías, técnicas y fenómenos para aspirar a un desarrollo tecnológico sostenible. Existen marcos legales suficientes, pero corresponde a todos trabajar para que se garantice el cumplimiento efectivo de las leyes.

BIBLIOGRAFÍA

ADORNO, Theodor L.W. *Minima Moralia. Reflexiones desde la vida dañada. Obra completa, 4*. CHAMORRO MIELKE, Joaquín, trad. Edición de Bolsillo. Akal. Madrid. 2006.

ALTMARK Daniel R., MOLINA QUIROGA, Eduardo. *Tratado de derecho informático*. Primera edición. Buenos Aires. Editorial La Ley. 2012.

BENITO MARTÍN Ruth. Protección de datos: el principio de lealtad y los dark patterns. En: Paloma, LLANEZA GONZÁLEZ. *Ellas. Retos, amenazas y oportunidades en un mundo conectado.* Primera edición. Las Rozas, (Madrid) España: Wolter Kluwer, 2019, pp164-209.

CERVANTES DE, Miguel. Don Quijote de la Mancha. Edición Alberto Blecua y Andrés Pozo. Colección Austral. Espasa. Madrid, España.1998.

DEBRABANDER, Firmin. *Life after privacy. Reclaiming democracy in a surveillance society.* Primera edición. Reino Unido. Cambridge University Press. 2020.

DE LA QUADRA SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás. Retos, riesgos y oportunidades de la sociedad digital. En: Tomás de la Quadra-Salcedo-José Luis Piñar Mañas. *Sociedad Digital y Derecho.* Primera edición. Madrid, España: Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado, 2018, pp. 21-85.

GARCÍA MEXÍA, Pablo, PERETE RAMÍREZ, Carmen. Internet, el RGPD y la LOPDGDD. En: José, LÓPEZ CALVO. *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD.* Segunda edición. Las Rozas (Madrid). Wolters Kluwer. 2019, pp 851-872.

GIL GONZÁLEZ, Elena. *Big data, privacidad y protección de datos.* Madrid, España. Agencia Española de Protección de Datos. 2016.

HERNÁNDEZ CORCHETE, Juan Antonio. Expectativas de privacidad, tutela de la intimidad y protección de datos. En: Tomás de la Quadra-Salcedo-José Luis Piñar Mañas. *Sociedad Digital y Derecho.* Primera edición. Madrid, España: Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado, 2018, pp. 279-300.

LLANEZA GONZÁLEZ, Paloma. *Datanomics*. *Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*. Segunda edición. España. Editorial Planeta. Ediciones Deusto. 2019.

MANTELERO, Alessandro. Ciudadanía y gobernanza digital entre política, ética y derecho. En: Tomás de la Quadra-Salcedo-José Luis Piñar Mañas. *Sociedad Digital y Derecho.* Primera edición. Madrid, España: Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. 2018, pp. 159-178.

NOAIN SÁNCHEZ, Amaya. *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014).* Agencia Española de Protección de Datos. Agencia Estatal Boletín Oficial del Estado Madrid. 2016.

O´ NEIL, Cathy. *Armas de destrucción matemática*. *Cómo el BIG DATA aumenta la desigualdad y amenaza la democracia*. ARRANZ DE LA TORRE, Violeta. Trad. Primera edición. Madrid. Capitan Swing Libros, S.L. 2017. Versión traducida al español.

ORTIZ LÓPEZ, Paula. Cookies, fingerprinting y la privacidad digital. En: LÓPEZ CALVO, José. *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Segunda edición. Las Rozas (Madrid). Wolters Kluwer. 2019, pp. 961-972.

ORTIZ LÓPEZ, Paula. La ética en el tratamiento de los datos digitales para un futuro sostenible. En: Paloma, LLANEZA GONZÁLEZ. *Ellas. Retos, amenazas y oportunidades en un mundo conectado.* Primera edición. Las Rozas, (Madrid) España: Wolter Kluwer, 2019, pp. 138-161.

PALAZZI, Pablo A. *Delitos contra la intimidad informática*. 1ra ed. CDYT colección Derecho y Tecnología. Ciudad Autónoma de Buenos Aires, Argentina. 2019.

PANIZA FULLANA, Antonia. El comercio electrónico y la protección del consumidor internauta. En: Francisco PÉREZ BES. *El derecho de Internet.* Primera edición. Atelier. Barcelona. 2016, pp. 125-143.

PARISER, Eli. *El filtro burbuja: cómo la red decide lo que leemos y lo que pensamos*. VAQUERO GRANADOS Mercedes, Trad. Primera edición. Barcelona. Editorial Taurus. 2017.

PEIRANO, Marta. *El enemigo conoce el sistema*. *Manipulación de ideas, personas e influencias después de la economía de la atención*. Primera edición. Barcelona. Penguin Random House Grupo Editorial. 2019.

PÉREZ LUÑO, Antonio E. Informática y libertad. Comentario al artículo 18.4 de la Constitución. *Revista de estudios políticos*. N° 24, Instituto de Estudios Políticos y Constitucionales, 1981, pp. 31–54.

PÉREZ LUÑO, Antonio E. Las libertades en la era de Internet. En: Francisco Javier ANSUÁTEGUI ROIG. *El derecho en red. Estudio en Homenaje al profesor Mario G. Losano.* Primera edición. Ed. Dykinson. Madrid. 2006, pp. 365-400.

PÉREZ LUÑO, Antonio E. La tutela de la libertad informática en la sociedad globalizada. *Isegoría: revista de filosofía moral y política. 2000*, vol. 22, no. 22, Consejo Superior de Investigaciones Científicas. Instituto de Filosofía, pp. 59–68.

PIÑAR MAÑAS, José Luis. *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio.* Documento de trabajo 147/2009. Fundación Alternativas. [en línea] [Fecha de consulta 28/4/2021] [http://www.cepc.gob.es/docs/ley-de-transparencia/ponencia-j-luis-pi%C3%B1ar.pdf?sfvrsn=0]

POLO ROCA, Andoni. El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político.* UNED. Nº 108. Mayo agosto 2020, pp. 165-193.

RECIO GAYO, Miguel. *Protección de datos personales e innovación: ¿(in)compatibles?*. Primera edición. Editorial Reus. Madrid. 2016.

RODOTÁ, Stefano. *La vida y las reglas. Entre el derecho y no derecho*. GREPPI, Andrea, trad. Trotta. Madrid.2010.

SÁNCHEZ DEL CAMPO REDONET, Alejandro. Inteligencia artificial y privacidad. En: José, LÓPEZ CALVO. *La adaptación al nuevo marco de protección de datos tras*

el RGPD y la LOPDGDD. Segunda edición. Las Rozas (Madrid). Wolters Kluwer. 2019, pp. 983-995.

SCHÜLL, Natasha Dow. *Addiction by Design.Machine Gambling in Las Vegas*. Princeton University Press. 2014.

SNOWDEN, Eduard. *Vigilancia permanente.* CRUZ SANTAELLA, Esther, trad. Primera edición en libro electrónico. Barcelona, España. Editorial Planeta. 2019.

SOLOVE, Daniel J. *Understanding Privacy.* Primera edición. Estados Unidos de América. Harvard University Press. 2008.

TOURIÑO Alejandro. *El derecho al olvido y a la intimidad en Internet.* Primera edición. Editorial Catarata. Madrid. 2014.

VÉLIZ, Carissa. *Privacy is power*. *Why and how you should take back control of your data.* Primera edición. Reino Unido: Bentham Press, Penguin Random House 2020.

ZUBOFF, Shoshana, *La era del capitalismo de la vigilancia*. *La lucha por un futuro humano frente a las nuevas fronteras del poder.* SANTOS MOSQUERA, Alvino. Trad. Primera edición. Barcelona, España. Editorial Planeta. 2020.