Universidad Internacional de La Rioja

Máster Universitario en Protección de Datos

OSINT y *big data*: Monitorización y búsqueda en fuentes abiertas

Trabajo de Fin de Máster presentado por: **MILLÁN LÓPEZ, JUAN ANTONIO**

Titulación: **MÁSTER UNIVERSITARIO EN PROTECCIÓN DE DATOS**

Área Jurídica: **DERECHO DE LAS NUEVAS TECNOLOGÍAS**

Director/a: **NOAIN SÁNCHEZ, AMAYA**

Ciudad: **SEVILLA**

19 DE SEPTIEMRE DE 2019

Firmado por: **MILLÁN LÓPEZ, JUAN ANTONIO**

MILLAN LOPEZ JUAN ANTONIO - 30252195L

Firmado digitalmente por MILLAN LOPEZ JUAN ANTONIO - 30252195L
Fecha: 2019.09.19 01:16:40 +02'00'

Índice

I. ABREVIATURAS Y SIGLAS UTILIZADAS

ARCO	Derechos de acceso, rectificación, cancelación y oposición
ARSALPO	Derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y no ser sujeto de decisiones automatizadas
DPD/DPO	Delegado de Protección de Datos / *Data Protection Officer*
DPDP	Directiva de Protección de Datos Personales (derogada)
LOPD	Ley Orgánica de Protección de Datos (derogada)
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales
LSSI-CE	Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico
NNTT	Nuevas Tecnologías
OSINT	*Open-Source Intelligence*
RDLOPD	Reglamento de Desarrollo de la LOPD (derogado)
RGPD	Reglamento General de Protección de Datos
TIC	Derecho de las Tecnologías y la Comunicación

II. RESUMEN

En el presente trabajo analizaremos los medios de búsqueda de información que las nuevas tecnologías nos ha proporcionado en esta última década, demostrando la facilidad con la que nuestros datos personales pueden ser susceptibles de tratamientos ilícitos –o desconocidos–, especialmente cuando esta información provenga de fuentes accesibles al público, donde el volumen de datos que pueden obtenerse es casi ilimitado, generando efectos jurídicos significativos sobre nuestra esfera más personal.

También examinaremos las implicaciones legales que el uso de estas tecnologías tiene sobre nuestra privacidad y hasta qué punto el hecho de compartir una publicación en nuestras redes permite a terceros obtener determinada información relativa a nosotros.

Además, a raíz de la jurisprudencia hallada, veremos si es posible homogeneizar el avance de las Nuevas Tecnologías con la regulación que nos brinda el actual **Reglamento Europeo de Protección de Datos** y la **Ley Orgánica 3/2018**, en lo relativo al impacto tecnológico sobre la privacidad de las personas físicas.

Keywords:

RGPD, LOPDGDD, protección de datos, privacidad, *big data*, OSINT, monitorización, *internet*, redes sociales, *apps*, *deep web*.

III. INTRODUCCIÓN

Estamos siendo testigos de un nuevo panorama, un cambio sobre la forma en cómo percibimos la información que recibimos y otorgamos día a día. Desde la obligatoria aplicación –que no vigencia– del nuevo **Reglamento Europeo de Protección de Datos** (**RGPD**), hemos empezado a tomar conciencia de cuan determinantes pueden llegar a ser aquellos datos de carácter personal que conciernen a cada individuo.

Igualmente, poco a poco, hemos comenzado a entender la importancia que puede llegar a adquirir nuestro simple consentimiento para que terceros puedan tratar esos datos atribuidos a nosotros mismos: cada vez que decidimos crear una cuenta en cualquier red social, foro o *web*; cuando instalamos una aplicación en nuestro *smartphone*; o el mero hecho de encontrarnos navegando por *Internet*. Son en estas situaciones cuando, ya sea de manera consciente o inconsciente, estamos facultando a ciertas entidades para almacenar información relativa a nuestra personalidad (hábitos, preferencias, opiniones, etc.), y que posteriormente serán tratadas para que en última instancia se obtenga un rédito económico, derivado de dicho tratamiento. Es por esto, por lo que muchos '*gurús*' afirman que los datos personales se están convirtiendo en el '*petróleo*' del siglo XXI.

Y es aquí donde entra en escena una figura que juega un importante papel en la recolección de estos datos de carácter personal, la **inteligencia de fuentes abiertas** (en inglés "***open-source intelligence***", **OSINT**), una herramienta que es capaz de recopilar toda aquella información relativa a una persona (o entidad), haciendo uso para ello de cualquier fuente que sea accesible al público (redes sociales, blogs, motores de búsqueda, foros, etc.), analizando el comportamiento de los usuarios a raíz de la compilación masiva de datos –y es aquí donde entra en juego el concepto de ***big data***, que más adelante desarrollaremos–, permitiendo de esta manera la composición de patrones y predicciones relativos a los usuarios titulares de dichos datos.

Por ello, a lo largo de este ejercicio de investigación, vamos a abordar el procesamiento que realiza esta herramienta sobre tal cantidad de datos personales, las finalidades que pueden buscar las entidades encargadas de su tratamiento, y las implicaciones y dilemas jurídicos que estas actividades entrañan.

1. Objetivos

1.1. Objetivo principal

Nuestro objetivo principal a seguir en este trabajo de investigación será tratar de averiguar la respuesta que nuestro ordenamiento da a los problemas que las nuevas tecnologías están generando en el devenir de la sociedad actual.

1.2. Objetivos complementarios

Adicionalmente, con el presente trabajo de investigación jurídica también pretendemos:

- Analizar el ordenamiento jurídico que compete a esta materia, tanto comunitaria como nacional, haciendo una breve reseña a su pasado, su presente, y su inminente futuro.
- Explicar brevemente algunas de las cuestiones más significativas del *big data*, así como de la obtención de datos personales a través de las conocidas fuentes abiertas, siempre desde una perspectiva jurídica.
- Por último, exponer las repercusiones que puede suponer el uso de esta tecnología a la esfera más personal de un individuo, su privacidad.

2. Metodología

La metodología a seguir para la elaboración de este trabajo se compone por la documentación, el estudio y la síntesis de algunos aspectos fundamentales ligados a esta área legal, que es el *Derecho aplicado a las Nuevas Tecnologías* (de ahora en adelante las denominaremos **NNTT**), para lo que contaré con algunos manuales, la legislación comunitaria y nacional vigente en la materia, revistas, páginas web y –en menor medida, debido a lo novedoso de este ámbito– jurisprudencia.

3. Justificación

La idea de este Trabajo de Fin de Máster reside en tratar de aclarar las implicaciones jurídicas que esta materia tiene sobre nuestros derechos y libertades más fundamentales.

A fin de cuentas, nos encontramos ante un terreno novedoso en términos jurídicos, y en la realidad más práctica la mayoría de personas no saben cómo tratar sus datos más reservados, ni pueden hacerse una idea del tratamiento que se les pudiera dar en las condiciones o circunstancias más inverosímiles.

4. Limitaciones

Como decíamos anteriormente, nos encontramos ante una materia no tanto novedosa por su concepto como por la forma de su tratamiento, a raíz del uso de dispositivos tecnológicos de nueva generación. Hay pocos estudios al respecto y no conocemos con exactitud las confrontaciones que estas nuevas tecnologías suponen para nuestros derechos.

Al ser una materia reciente, de la cual todavía no se encuentra una jurisprudencia lo suficientemente sólida, mi intención es tratar de profundizar en el estudio de esta investigación; y en la medida de lo posible, arrojar algo de luz y contribuir de alguna manera al estudio y análisis de la inteligencia de fuentes abiertas y su relación con el **Derecho de las NNTT**.

Y es que el *Derecho de las Tecnologías de la Información y la Comunicación* (también denominado **Derecho TIC**) es un sector actualmente en constante crecimiento, y aquí la *Protección de Datos* cumple un factor decisivo para dicho crecimiento, puesto que es este ámbito el que logra implementar tanto en entidades u organismos públicos y privados los sistemas de gestión de seguridad de la información necesarios para adecuarse al ordenamiento jurídico, así como para garantizar la confidencialidad, integridad y disponibilidad de aquellos datos que se ven sujetos al tratamiento de estos organismos.

IV. DESARROLLO

1. Marco normativo

1.1. Antecedentes: Directiva 95/46/CE y LOPD 15/99

Para empezar el estudio, debemos poner en pie el sistema jurídico que ha sostenido la regulación de la privacidad de los ciudadanos pertenecientes a la Unión Europea; y es que no fue hasta los años 80 cuando la Comisión Europea empezó a tomar conciencia sobre la legislación de dicha materia. Si bien ya existían normativas europeas al respecto[1], no había una armonización de las mismas en el Espacio Económico Europeo. Es por ello que en 1990, la Comisión Europea acabó planteando una propuesta legislativa para llevar a cabo esa armonización, que se acabó materializando con la **Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995**, relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a su libre circulación (también conocida como Directiva de Protección de Datos Personales o **DPDP**)[2], la cual se limitaba a regular el tratamiento de los datos de carácter personal, con independencia de que dicho tratamiento se llevase a cabo por medios automatizados o no.

Esta directiva tenía marcado un doble objetivo: de un lado, obtener un claro compromiso por parte de todos los Estados miembro que conforman la Unión Europea que garantizase la protección de las libertades y los derechos fundamentales de las personas físicas, pero sobre todo en lo que respecta a su privacidad; es decir, establecer una regulación en relación con aquellos tratamientos de los datos personales que conciernen a cada individuo.

Y por otro lado, se trataba de impedir cualquier limitación a la circulación de datos personales entre los Estados miembro de la Unión Europea en base al derecho fundamental que supone para las personas físicas la protección de sus datos de

[1] Suecia fue el primer país europeo con una ley nacional que hacía referencia a esta materia, estableciendo la ***Data Lag*** en **1973**; y en enero de **1977** Alemania aprobó su primera Lay Federal de Protección de Datos (***Bundesdatenschutzgesetz***).

[2] No obstante, el ámbito de aplicación de la **Directiva 95/46/CE** supuso una mayor restricción que la establecida en el **Convenio 108** –que supuso el punto de partida para dicha directiva– , al no aplicarse a cualquier tratamiento de datos personales que llevase a cabo una persona física en el ejercicio de sus actividades personales o domésticas, ni a aquellos supuestos amparados en el ámbito de aplicación del derecho comunitario, cuyo objeto sea la seguridad pública, la defensa, la seguridad del Estado y aquellas actividades que competan al Estado en materia penal (artículo 3.2 **DPDP**).

carácter personal, siempre que se garantizase un nivel de protección adecuado y exigible para toda la Comunidad Económica Europea que, de una forma u otra, afianzara la continuidad del mercado único.

La **DPDP** fue la encargada de cimentar los principios sobre los que ampararse en relación con el tratamiento de datos personales:

- ***Transparencia***, por el que el interesado tendría el derecho a ser informado cuando sus datos personales fueran a ser recabados y objeto de futuros tratamientos, y siempre bajo unos determinados casos tasados[3]. En este punto, corresponderá al responsable del fichero o del tratamiento[4] proporcionar información en relación a sus datos de contacto, la finalidad del tratamiento, los destinatarios de los datos de los interesados, y así como cualquier otra información que se considerase necesaria para asegurar el correcto proceso del tratamiento de datos.
- ***Legitimación***, los datos personales de los interesados únicamente podrán ser recabados para una, o varias finalidades, siempre que sean concretas y lícitas. Además, estos datos no podrán ser tratados ulteriormente para una finalidad opuesta[5] a aquella que motivó su recogida.
- ***Proporcionalidad***, los datos personales que vayan a ser objeto de tratamiento serán estrictamente los pertinentes, siendo incompatible la recogida de aquellos datos que excedan en relación con la finalidad que el responsable –o aquel que actúe en su nombre– persigue. Igualmente, dichos datos deben ser exactos y actualizados, puesto que será obligación del responsable del fichero adoptar las medidas necesarias para suprimir o rectificar aquellas que resultaren inexactos o incompletos para la finalidad perseguida.

Esta directiva también fijó los derechos de los que disponen las personas físicas[6] en torno a sus datos personales, las obligaciones de los responsables de los ficheros; y

[3] **Artículo 7** de la **Directiva 95/46/CE**.
[4] Antes de la llegada del **Reglamento (UE) 2016/679**, el concepto correcto para hablar de esta figura era el de **responsable del fichero**, pues era donde se contenían los datos de carácter personal de los interesados en el tratamiento de sus datos; ya con la entrada en vigor del **RGPD** dicho concepto dio paso al que solemos tratar actualmente, el **responsable del tratamiento**.
[5] **Artículo 6**, letra ***b)*** de la **Directiva 95/46/CE**.
[6] Derechos **ARCO**: **A**cceso, **R**ectificación, **C**ancelación y **O**posición al tratamiento de datos personales.

además, estableció que cada Estado miembro dispusiese de una autoridad de control independiente y encargada de velar por el cumplimiento de la normativa en protección de datos.

Actualmente, en España contamos con una autoridad de control de ámbito nacional, la **Agencia Española de Protección de Datos** (**AEPD**); y otras tres entidades que operan a nivel autonómico, catalana, euskera y andaluza (*Autoritat Catalana de Protecció de Dades*, *Agencia Vasca de Protección de Datos*[7] y *Consejo de Transparencia y Protección de Datos de Andalucía*, respectivamente).

Ha sido tal la importancia de esta directiva que ha supuesto una referencia para aquellos Estados al margen del **Espacio Económico Europeo**, puesto que podrán llevarse a cabo transferencias de datos personales con países terceros a la Unión Europea, siempre que estos mantuvieran o garantizasen un nivel de protección adecuado para las libertades y los derechos fundamentales de aquellas personas físicas cuyos datos vayan a ser objeto de tratamiento. Esto ha ayudado a que esos países terceros hayan acercado su nivel de protección en relación con el tratamiento de datos personales a lo dispuesto por la **DPDP**.

No obstante, al tratarse de una directiva emanada de la UE, éstas se encontraban ciertamente limitadas pues, aunque se dirigían los Estados miembros que la conforma, ciertamente tampoco eran legalmente vinculantes, sino que correspondía a sus Estados miembros la facultad de transponerla a su normativa nacional.

Aun así, todos los Estados miembros de la Unión Europea han ido estableciendo, paulatinamente, su propia normativa en materia de protección de datos en sus respectivos ordenamientos.

En el caso de España, dicha DPDP no llegó trasponerse en nuestro ordenamiento jurídico hasta finales del siglo pasado, concretamente en diciembre de 1999, a través de la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal** (**LOPD**)[8], la cual acabó entrando en vigor en enero del año 2000.

Pero esta Ley Orgánica adolecía de un cierto carácter ordinario y abusivo en relación con los procedimientos reglamentarios. Aunque es cierto que los reglamentos ayudan

[7] *Datuak Babesteko Euskal Bulegoa* en euskera: https://www.avpd.euskadi.eus/s04-5213/eu/

[8] Esta Ley Orgánica vino a suceder a la ya derogada **Ley Orgánica 5/1992**, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (**LORTAD**).

a desarrollar las leyes, no eran pocas las remisiones que establecían conforme a la vía reglamentaria[9], cuyo reflejo se encuentra en el **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el **Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos** (**RDLOPD**).

En cuanto a su ámbito de aplicación, al igual que la **DPDP**, regulaba los ficheros o tratamientos de datos de carácter personal; es decir, únicamente afectaba a los datos relativos a las personas físicas –el tratamiento de personas jurídicas encontraban su regulación en otras normativas, como el **Código Penal**–, ya fuere por medios manuales o automatizados, o que dichos ficheros fueran de titularidad pública o privada. Y al igual que la directiva, se excepcionaba de su ámbito de aplicación los ficheros o tratamientos de datos realizados por una persona física en el ejercicio de sus actividades más personales o domésticas; tratamientos relativos a la investigación del terrorismo y a otras materias clasificadas.

La **LOPD** –con apoyo del **RDLOPD**– ayudo a desarrollar y definir todos aquellos conceptos relacionados con la protección de datos (*dato personal*, *fichero*, *tratamiento*, *consentimiento*[10], *responsable* y *encargado* del fichero o tratamiento, *afectado* o *interesado*, *responsable de seguridad*), además de establecer una serie de principios inspiradores para la materia en el Título II de dicha Ley (artículos 4 a 12 de la **LOPD**):

- *Calidad de los datos* (**artículo 4**)
- *Derecho de información en la recogida de datos* (**artículo 5**)
- *Consentimiento del afectado* (**artículo 6**)
- *Datos especialmente protegidos* (**artículo 7**)
- *Datos relativos a la salud* (**artículo 8**)
- *Seguridad de los datos* (**artículo 9**)
- *Deber de secreto* (**artículo 10**)
- *Comunicación de datos* (**artículo 11**)

[9] Algunos ejemplos los encontramos en los **artículos 4.5**, **9.3**, **17.1** y **18.1** de la **LOPD**.

[10] A diferencia del nuevo **RGPD**, con la **Ley Orgánica 15/1999** el consentimiento del interesado se podía obtener bien de manera expresa, tácita, presunta o mediante cualquier cesión o comunicación por la que el interesado consiente el tratamiento de aquellos datos de carácter personal que le conciernan (**artículo 3*.h)-i)*** de la **LOPD**).

- *Acceso a datos por cuenta de terceros* (**artículo 12**)

En consonancia con la Directiva Europea, la **LOPD** también tomó como referencia los derechos que asistían al interesado o afectado en relación con aquellos datos de carácter personal que fueran concernientes a su propia esfera privada: acceso, rectificación, cancelación y oposición al tratamiento de datos; además de incorporar un derecho de indemnización como consecuencia de cualquier incumplimiento de lo establecido en la **LOPD** (**artículo 19**).

No obstante, sobre esta Ley Orgánica también sobrevolaba una cierta inseguridad jurídica, puesto que a veces la decisión final quedaba al arbitrio de la autoridad de control competente –en este caso la **AEPD**–, lo que dificultaba en ocasiones seguir el *íter* marcado desde un inicio por la normativa en materia de protección de datos.

1.2. Actualidad: RGPD y LOPDGDD

Tanto la **Directica Europea 95/46/CE** como la **LOPD** y el reglamento que desarrolla la misma ayudaron a vertebrar este derecho fundamental que es la protección de los datos de carácter personal, pero también es cierto que toda esta normativa no evolucionó en la medida que lo ha ido haciendo la sociedad conforme a los avances tecnológicos que han acontecido en las últimas décadas[11] gracias al fenómeno de la globalización.

A esto, se le unió que la Unión Europea, a pesar de que cada Estado miembro contara con su propia normativa relativa a la protección de datos, no contaba con una cohesión reguladora de la materia. Y es que aunque la DPDP siempre tuvo como objetivo instaurar un cuerpo normativo común para todos los Estados, se dio un elevado margen de discreción a estos a la hora de transponer dicha directiva a sus propias normativas locales.

[11] Una de los primeros rastros de jurisprudencia donde se hace referencia explícita a la protección de datos como derecho fundamental la encontramos en la STJUE (Gran Sala), de 29 de enero de 2008 – Productores de Música de España (*Promusicae*) contra Telefónica de España, S.A.U. (**Asunto C-275/06**), donde una asociación que reúne a varias discográficas españolas) demandó a ***Telefónica, S.A.U.***, exigiéndole a esta una lista con la identidad y dirección de aquellos clientes que hubieran compartido contenido sujeto a derechos de explotación mediante programas de intercambio de archivos entre partes (**P2P**, acrónimo de '***peer to peer***'). Fuente: http://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=2134680

Todo esto llevo a un marco regulatorio muy disperso, con diferentes niveles de protección y dispares requisitos, aun dentro de la UE.

De ahí la necesidad de establecer una nueva normativa que consiguiese esa armonización legislativa para toda la Unión Europea y que logró materializarse con el **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 (**RGPD**), siendo aprobado el 14 de abril de 2016 en el Parlamento Europea y publicado en el Diario Oficial de la Unión Europea el 4 de mayo, entrando en vigor a los veinte días de su publicación.

No obstante, se concedió tanto a las Administraciones Públicas como a las entidades privadas un periodo de dos años[12] para adecuarse a la nueva normativa tras su entrada en vigor. Por tanto, no fue hasta el 25 de mayo del pasado año (2018) cuando este Reglamento adquirió el carácter de obligatorio y directamente aplicable para todos sus Estados miembros, sin necesidad de su transposición a los distintos ordenamientos jurídicos. Este Reglamento trajo consigo una serie de novedades, como:

- La incorporación de nuevos principios en relación con el tratamiento de los datos personales (transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva o *accountability*), todos ellos reflejados en el **artículo 5** del **RGPD**.
- La clasificación de los datos pasaron de agruparse en tres tipos (datos básicos, datos de nivel medio y datos de nivel alto) a formar únicamente 2 grupos (datos básicos y datos especialmente protegidos, donde coexisten tanto los datos sobre la salud de las personas físicas, como aquellos datos relativos a los delitos y condenas penales registradas sobre personas con antecedentes).

[12] Aunque pueda parecer una ***vacatio legis***, este peculiar periodo de adecuación no se definiría como tal, ya que la vacatio legis es el período que transcurre entre la publicación de una norma y su entrada en vigor, que por regla general consta de 20 días. En este caso, lo que se concedió fue una prórroga de 2 años para que el **RGPD** fuera de obligatoria aplicación para todos los Estados miembro de la **Comunidad Económica Europea**, tras su entrada en vigor.

- La incorporación de una nueva serie de derechos[13] inherentes a las personas físicas propietarias de los datos, a los ya conocidos derechos ARCO se le suman los derechos de portabilidad, limitación del tratamiento y a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles. No obstante, el derecho de cancelación queda sustancialmente modificado, derivando a un derecho de supresión (dentro del cual hay una pequeña parcela para el famoso derecho al *olvido*).
- En cuanto a las obligaciones de los responsables y encargados del tratamiento, se amplía el deber de información que estos tienen para con los interesados: informar sobre la base legitimadora en la que se ampara el tratamiento, los plazos de conservación que se le aplicarán a los datos, los derechos con los que cuentan los interesados, la posibilidad de hacer reclamaciones ante la autoridad competente, etc.
- Otra nueva obligación prevista en **artículo 25** del **RGPD** es la de tener en cuenta la privacidad de los datos desde el diseño (***by desing***) y por defecto (***by default***); es decir, desde el momento en que se determinan los medios de tratamiento como durante el período de dicho tratamiento, contar con las medidas apropiadas (por ejemplo, la seudonimización) para garantizar la efectiva aplicación de los principios de protección de datos; medidas que, por defecto, garantizarán que solo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento.

  Este punto se encuentra estrechamente vinculado a uno los nuevos principios que han surgido con el nuevo **RGPD**, la responsabilidad proactiva (***accountability***) del responsable del tratamiento; esto es, que dicho responsable tiene la obligación de cumplir con las obligaciones a las que le sujeta la nueva normativa, y además, demostrar ese cumplimiento normativo.

[13] Para una agilización en su escritura, el acrónimo de estos nuevos derechos ha pasado de **ARCO** a **ARSALPO** (**A**cceso, **R**ectificación, **S**upresión, no ser objeto de decisiones **A**utomatizadas, **L**imitación del tratamiento, **P**ortabilidad de datos y **O**posición al tratamiento).

Por ello, será necesario que, antes de iniciar el tratamiento de datos, el responsable del tratamiento lleve a cabo una serie de obligaciones[14]:

- La obligatoria llevanza de un registro de las actividades de tratamiento que llevará a cabo;
- La elaboración de un informe derivado del análisis de los riesgos que pueden acarrear el tratamiento de datos de carácter personal;
- Realizar una evaluación de impacto, con carácter previo al inicio del tratamiento, si del anterior informe se desprendiese que el tratamiento de datos implicará un alto riesgo para los derechos y libertades de los interesados;
- Establecer las medidas técnicas y organizativas de seguridad necesarias para garantizar la integridad y disponibilidad de la información;
- Notificar toda posible brecha de seguridad a la autoridad de control competente en protección de datos;
- Y en aquellos casos que la normativa lo establezca, proceder a la obligatoria designación de un **delegado de protección de datos** (artículo 37 del **RGPD**). Esta figura también es una de las novedad más destacadas que ha incorporado el Reglamento Europeo, el cual se encargará de asesorar al responsable o encargado del tratamiento en todo lo relativo a la normativa sobre protección de datos, gozando de total independencia en el ámbito de sus funciones y ocupando una posición de nivel superior en el seno de la organización. Ejercerá de punto de contacto entre el responsable (o el encargado) y la autoridad de control competente.

  En los casos que no sea obligatoria su designación, siempre quedará al arbitrio del responsable o el encargado del tratamiento la facultad de proceder a su nombramiento.

[14] <<Guía del Reglamento General de Protección de Datos para responsables de tratamiento>>. *Agencia Española de Protección de Datos*. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

- En lo que respecta al consentimiento del interesado, si algo diferencia al RGPD de anteriores normativas, es que éste ha hecho hincapié en la concreción de su recogida.

  A la hora de obtener el consentimiento para la recogida de datos, debe otorgarse de manera expresa; no hay lugar a un consentimiento tácito o presunto.

  Aquí el **Reglamento** es muy explícito en su **Considerando 32**, ya que el consentimiento deberá darse "*mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal*", y siempre que sea para el tratamiento de una actividad concreta.

  En cuanto al consentimiento que ya hubieran dado el interesado antes de la directa y obligatoria aplicación del Reglamento, éste también se pronuncia en su **Considerando 171**, aclarando que no será necesario volver a recabarlo "*si la forma en que se dio* [...] *se ajusta a las condiciones del presente Reglamento*", bastando con una mera comunicación del cambio de **políticas de privacidad**.

  Esto último ha chocado bastante en la práctica con la situación que se vivió que las semanas anteriores –y posteriormente también– al 25 de mayo, fecha en la que el RGPD comenzó a ser de obligada aplicación, cuando cada usuario recibía diariamente en su cuenta de correo electrónico decenas de emails de determinados portales web.

  Es cierto que algunas entidades actuaron correctamente, informando únicamente de ese cambio de Políticas de Privacidad de su página, adecuándose de esta manera a la nueva normativa comunitaria; pero no fueron pocas webs las que, por un mal asesoramiento de la materia, mandaban además correos para volver a solicitar el consentimiento del interesado[15],

[15] En relación con este tipo de situaciones, destaca el caso de Burger King que, semanas antes de la obligatoria aplicación del **RGPD**, mandó estos correos para volver a solicitar el consentimiento de aquellos interesados que ya lo dieron en su momento para la misma finalidad que la actual. Para mayor información, **Pablo Fernández Burgueño**, abogado experto en derecho tecnológico, habló de este

consentimiento que ya había dado anteriormente para la misma finalidad que fue obtenido originalmente.

- Por último, sería conveniente hacer una breve mención a las cuantías de las sanciones que impone el Reglamento a los responsables y encargados del tratamiento que incumplan sus obligaciones en materia de protección de datos. Con anterioridad a la llegada del RGPD, las sanciones por incumplimiento podían oscilar entre los novecientos y seiscientos mil euros, en función de la gravedad de la posible infracción; ahora, si bien no se establece un mínimo, estas cuantías pueden llegar a los diez millones de euros o bien, si se tratara de una empresa, el 2% de su facturación de volumen global en el ejercicio anual anterior (en caso de **infracción grave**); y hasta veinte millones de euros o, si se tratara de empresa, hasta el 4% de su facturación de volumen global en el ejercicio anual anterior (**infracción muy grave**). Y en cualquier caso, siempre se optará por la cantidad más elevada.

Si bien es cierto que esta normativa comunitaria está cumpliendo ese objetivo unificador que hemos mencionado inicialmente, también hay varios países que han desarrollado –y algunos siguen en vías de alcanzar dicho objetivo– sus propias leyes de protección de datos, en sintonía con el nuevo RGPD.

España recientemente ha estado trabajando desde noviembre de 2017 en proyecto de esta nueva Ley. Proyecto que acabó materializándose en la actual **Ley Orgánica 3/2018**, de 5 de diciembre, de **Protección de Datos Personales y Garantía de los Derechos Digitales** (**LOPDGDD**). Con la llegada del RGPD, este paso era necesario en nuestra legislación nacional, ya que al igual que otros países europeos contábamos con una normativa que databa de finales de los años 90, lo que producía un gran desfase con el devenir de nuestra sociedad a raíz de los avances tecnológicos que hemos vivido en las últimas dos décadas.

El contenido de esta nueva normativa nacional, en su amplia mayoría no hace más que remitirse a lo ya establecido por el **RGPD**, si bien complementa y desarrolla algunas cuestiones ya especificadas en la normativa comunitaria:

---

asunto en su cuenta personal del *Twitter* sobre las nefastas consecuencias que puede tener un mal asesoramiento en protección de datos. Fuente: https://twitter.com/pablofb/status/994614827032203265

- Amplía los supuestos en que será obligatorio designar a un Delegado de Protección de Datos (artículo 34 de la **LOPDGDD**), si bien se trata de una lista abierta (*numerus apertus*);
- Constituye un régimen de sanciones a aplicar por parte de las autoridades de control, distinguiendo entre sanciones de carácter leve y grave, detallando el uso de medidas correctivas, y además establece sus plazos de prescripción;
- Se prohíbe explícitamente el envío de comunicaciones en aquellos casos que no haya sido solicitado el consentimiento del interesado, exceptuando aquellos supuestos que queden al amparo de la **Ley 34/2002**, de 11 de julio, de **Servicios de la Sociedad de la Información y de Comercio Electrónico** (**LSSI-CE**), bien porque ya hubiera una relación precontractual, o bien porque los productos o servicios ofertados por el responsable del tratamiento fueran similares a los que ya contratase el interesado;
- Hace una breve alusión a los sistemas de denuncias internas, incluyendo la posibilidad de que esas denuncias también se realicen de manera anónima, ya que con la anterior **LOPD** se precisaba la identificación del denunciante (artículo 24 de la **LOPDGDD**);
- Y uno de los puntos más novedosos es el reconocimiento que se hace a los derechos digitales (**Título X**, **artículos 80 a 96** de la **LOPDGDD**), de los que las personas físicas podremos hacer uso para realizar determinadas funciones, siempre que suponga la interacción con un dispositivo electrónico o una red de comunicaciones. Estos derechos no dejan de estar estrechamente vinculados a otros derechos fundamentales, como son la privacidad o la libertad de expresión ampliados al ámbito de las **NNTT**.

1.3. Una mirada al futuro: el Reglamento e-Privacy

La instauración del **RGPD** está suponiendo todo un cambio en nuestra sociedad, tanto para los usuarios de los servicios de la sociedad de la información, como para el modelo de negocio de entidades públicas y privadas. No obstante, tampoco podemos

decir que con su aplicación hayamos *tocado techo* en lo relativo a la regulación de los dispositivos electrónicos y sus aplicaciones.

Desde principios de 2017, la Comisión Europea se encuentra desarrollando un proyecto de Reglamento (denominado **Reglamento *e-Privacy***) que vendrá a sustituir a nuestra actual **LSSI-CE** y a la **Directiva 2002/58/CE**, cuyo objetivo será reforzar la privacidad de los usuarios y consumidores de estos servicios, en lo que respecta al envío de comunicaciones electrónicas.

En un principio, estaba pensado que tanto el **RGPD** como el **Reglamento *e-Privacy*** se aplicasen paralelamente, es decir, a partir del 25 de mayo de 2018[16]. No obstante, la fuerte presión a la que se ha visto sometida por ciertos lobbies del sector ha conseguido frenado su avance.

Esta futura normativa tratará de exigir unos requerimientos más rigurosos a los prestadores de servicios de la sociedad de la información, de manera que ofrezcan a los consumidores y usuarios sus productos o servicios, con independencia de que estos consientan o no que puedan tratar sus datos, algo que ya se refleja en su contenido, concretamente en el segundo apartado del **artículo 1** de dicho proyecto, el cual "*garantiza la libre circulación de datos* [...] *que no será posible restringir ni prohibir por motivos relacionados con el respeto de la vida privada y las comunicaciones de las personas físicas y jurídicas y la protección de las personas físicas en lo que respecta al tratamiento de datos personales*"

Esta idea resulta interesante, ya que tal situación supondría para muchas empresas del sector las comunicaciones electrónicas (en especial, para grandes multinacionales, como por ejemplo ***Gmail***, ***WhatsApp*** o ***Skype***) la correcta prestación de sus servicios a los usuarios, a los cuales no se les podrá negar o entorpecer su uso por el hecho de no aceptar unas determinadas condiciones sobre el tratamiento de nuestros datos de personales. Sobre el papel, es un factor positivo, puesto que garantiza un mayor control de la privacidad de las personas físicas a la hora de interactuar con otras personas en entornos digitales, mediante el uso distintos dispositivos electrónicos habilitados para ello.

[16] Incluso el **artículo 2** de esta **propuesta de Reglamento** sigue haciendo referencia en su segundo apartado a la fecha, a partir de la cual comenzaría a ser aplicable para sus Estados miembro. Fuente: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017PC0010&from=ES

Y estamos siendo testigo de ello, poco a poco vemos como determinados portales *web* nos proporciona, al instante de acceder a su web, un cuadro informativo sobre el uso de ***cookies***[17] que posee dicho prestador, facilitando en ese mismo momento un panel de configuración para que sea el propio usuario el que decida si quiere dejar activadas o desactivadas dichas *cookies*, salvo aquellas que resulten estrictamente necesarias para el correcto rendimiento y funcionamiento del portal web. No obstante, seguimos viendo en muchas páginas web, como siguen contando con un listado excesivo de *cookies*, algo que este proyecto de Reglamento pretende evitar.

El futuro Reglamento e-Privacy incluye algunos conceptos novedosos en relación con las comunicaciones electrónicas, como son los metadatos de comunicaciones electrónicas (**artículo 4.3.*c)*** del **Reglamento *e-Privacy***), que podría definirse como aquel "*conjunto de datos que describen el contenido informativo de un archivo*" y que, por tanto, puede arrojar de información de los mismos.

Este proyecto persigue que los prestadores de servicios de comunicaciones electrónicas puedan hacer uso de esos metadatos, siempre que conculque con algunos de los supuestos que establece la normativa: para la calidad del servicio prestados, por motivos de seguridad, o bien cuando el usuario final diese su consentimiento (**artículo 6.2**); sin perjuicio de que estos metadatos sean suprimidos una vez que ya no sean necesarios para la transmisión de comunicaciones, o bien sean anonimizados si el usuario no hubiese dado su consentimiento (**artículo 7.2**).

Esta situación se da con frecuencia cuando el usuario está navegando en Internet: entras en un web o blog y descubres que el contenido al que intentas acceder queda bloqueado, ya que ese navegador usa una ***ad-block*** (una extensión o aplicación) que se encarga de evitar que el usuario reciba cualquier tipo de publicidad no deseada mediante ***pop-ups*** (ventanas emergentes).

En estos casos, el prestador de servicios hace uso de los metadatos para saber si los usuarios suelen tener instaladas esas extensiones en sus navegadores, y si es así,

[17] Podríamos definir una ***cookie*** como "*un pequeño archivo informático creado por un portal web que contiene pequeñas cantidades de datos, cuya finalidad consiste en identificar al usuario y almacenar un historial con la actividad del mismo en sobre una web determinada*". Es decir, se trata de un pequeño registro que ayuda a los prestadores de servicios de la sociedad de la información a establecer unos determinados patrones de sus usuarios, para así ofrecerles futuros servicios en atención a sus hábitos de búsqueda.

bloquear su acceso al contenido, lo que obligaría al usuario a desbloquear esa extensión para acceder al contenido que estaba buscando.

Este tipo de problemáticas son las que pretende, de alguna manera, solventar el futuro **Reglamento *e-Privacy***, pero debido a que gran parte de los prestadores de servicios de comunicaciones electrónicas hacen uso de esta publicidad, ya que suponen una fuente de ingresos para los mismos, es una cuestión que el legislador todavía no sabe cómo abordar –por algo, esta ha sido una de esas razones por las que el proyecto aún no ha prosperado–.

A diferencia del **RGPD**, este reglamento se aplicará tanto a personas físicas como personas jurídicas. Pero, en consonancia con el mismo Reglamento Europeo de Protección de Datos, el ámbito de aplicación del proyecto de **Reglamento *e-Privacy***[18] vinculará a cualquier entidad que prestase sus servicios a los residentes de la Unión Europea, con independencia de su nacionalidad originaria; en general, se aplicará a todas las entidades que tengan acceso a datos de estos residentes, ya sean o no de carácter personal. De hecho, a finales de julio de 2019 se dio a conocer un nuevo borrador de este proyecto de Reglamento; y además, está previsto que el **9 de septiembre** de este mismo año se discuta su propuesta.

Por tanto, es necesario contar con una normativa armonizada que garantice la privacidad de las personas y regule debidamente la manera en que las entidades corporativas traten y compartan esos datos personales.

2. Big Data

El modo en que percibimos la realidad ha cambiado en las dos últimas décadas: la forma de comunicarnos con terceros, la manera de relacionarnos con nuestros seres más cercanos y distantes, y hasta la interacción con los objetos más cotidianos con los que funcionamos en el día a día.

[18] ALDEA, M. <<*e-Privacy*: La UE propone normas más estrictas para las comunicaciones electrónicas>>. *Écija Blog*. 18 enero 2017. Disponible en: https://ecija.com/e-privacy-la-ue-propone-normas-mas-estrictas-las-comunicaciones-electronicas/

La irrupción del fenómeno que conocemos como el ***Internet* de las cosas** (**IoT**, en inglés "***Internet of Things***") ha supuesto toda una revolución para el mundo globalizado, actuando como una fuente de datos mediante la interconexión de dispositivos informáticos aplicados tanto a objetos o maquinas que podemos usar en nuestra rutina (por ejemplo, los *smartphones*, las *roombas* o los frigoríficos inteligentes) como en animales o personas (un paciente con marcapasos, o una mascota con un chip implantado) que permite una monitorización contante a través del espacio y el tiempo.

2.1. Concepto

Esta obtención de datos basada en la monitorización es lo que en gran medida ha llevado a la sociedad a inmiscuirse, sin tan siquiera ser consciente de ello, en el fenómeno del ***big data***.

Pero antes que nada, ¿*qué es el big data*? Se trata de un concepto que hace referencia al conglomerado de tecnologías que, mediante el uso de algoritmos informáticos, puede captar y analizar un gran volumen de datos procedentes de distintas fuentes.

En la actualidad, este tipo de tecnologías es el que suelen usar la gran mayoría de organizaciones con la última finalidad de crear un valor añadido a su modelo de negocio. Gracias a esta captación masiva de datos, las empresas pueden adquirir un mayor conocimiento de las tendencias de consumo y realizar diversos análisis que ayuden a segmentar al público, creando distintos perfiles de potenciales consumidores. Esto sin duda puede suponer uno de los mayores valores de las empresas, pues ayudará a gestionar sus recursos de una manera más eficiente.

2.2. Tratamiento y analítica

Algo que debemos tener en cuenta es que en todo modelo de negocio, de nada sirve obtener una masiva cantidad de datos, si a estos no se les aplica un correcto tratamiento que filtre aquellos que resulten necesarios para la finalidad específica que el responsable del tratamiento haya definido desde un primer momento. Solo a partir del tratamiento de estos datos y de su análisis podremos hallar resultados con los que establecer o previsualizar hechos que antes no quedaban a la vista, formando así

patrones de conducta sobre los hábitos de los consumidores[19] que ayuden a las empresas a ofrecer determinados productos o servicios a estos últimos.

La incorporación de las **NNTT** al sector económico ha supuesto toda una revolución, pues gracias a la creación de ciertas aplicaciones tecnológicas se ha permitido simplificar la carga de trabajo de las empresas. Aplicaciones que, gracias a la integración de la **inteligencia artificial**, consiguen elaborar perfiles, pronosticar escenarios que favorezcan el modelo de negocio de una entidad y establecer criterios objetivos que les permita obtener una mayor productividad y eficiencia.

A modo de ejemplo, podríamos fijarnos en el sector legal –a fin de cuentas, es la cuestión en torno a la gira este trabajo de investigación–, donde empiezan a aflorar despachos y consultorías jurídicas que han comenzado a apoyarse en el ***big data*** para orientar sus decisiones a la hora de abordar determinados litigios[20] basándose en determinados aspectos: calcular la posibilidad de que un caso pueda ser recurrido o estimado, establecer la duración del litigio en función del Tribunal o Juez asignado, etc.

En este terreno podemos destacar *softwares* como **Jurimetría** o ***Vlex Analytics***, que a partir del **procesamiento de lenguajes naturales**[21] han permitido analizar millares de sentencias, las cuales ya se encontraban en la base de datos de sus respectivos servidores, y obtener de estas mismas **metadatos** que si bien en apariencia no serían de verdadera relevancia, a medio largo plazo acaban enriqueciendo este tipo de programas en base a la información extraída y analizada.

Es decir, con este tipo de *software*[22] podrían inferirse ciertos patrones que ayudarían a mejorar la experiencia del profesional que haga uso de las mismas en cualquiera de las

---

[19] PERETÓ, A. <<El caso *Walmart*>> *ICEDM Blog: La gestión del Big Data en la inteligencia de negocio*. 11 noviembre 2015. El caso de ***Walmart*** ha constituido un referente en el campo del ***big data***, ya que gracias a la recopilación masiva de datos la multinacional de grandes almacenes consiguió establecer numerosas predicciones sobre sus ventas, teniendo en cuenta distintos escenarios y factores, entre ellos el famoso huracán ***Katrina***, donde detectaron que las cervezas o los dulces eran de las provisiones que antes desaparecían del stock. Fuente: http://blogs.icemd.com/blog-la-gestion-del-big-data-en-la-inteligencia-de-negocio-/el-caso-walmart/

[20] Práctica a la que se le está acuñando el término de **analítica jurisprudencial**.

[21] El procesamiento de lenguajes naturales es un campo dentro de la ciencia –cuyo origen se vincula al científico británico Alan Turing–, ligada a la inteligencia artificial, y que a grandes rasgos tiene como finalidad el estudio de las interacciones entre los dispositivos informáticos y el lenguaje humano.

[22] <<Hoy probamos a fondo... Jurimetría>>. *Legaltechies*. 22 mayo 2018: https://legaltechies.es/2018/05/22/hoy-probamos-a-fondo-jurimetria/, se trata de un artículo sobre el funcionamiento de ***Jurimetría***, una interesante herramienta desarrollada por ***Wolters Kluwer*** que está comenzando a ser incorporada en muchos despachos de abogados.

ramas procesales. Las posibilidades no serán ilimitadas, pero puede ofrecer cuantiosas ventajas:

- Establecer tácticas procesales en aquellas áreas donde el jurista no cuente con demasiada experiencia;
- Trazar porcentajes, a raíz de los fundamentos analizados de aquellas sentencias relacionadas con determinadas materias; lo que sin duda supone una de las mayores bazas de estas herramientas, ya que son numerosas las ocasiones donde los profesionales pueden haber pasado por alto ciertos fundamentos, lo que ayudaría a sentar mayores precedentes a corto plazo;
- Ofrecer a los clientes, a partir de datos objetivos, una imagen realista de los resultados o las posibles opciones que podrán esperarse (el tiempo que podría durar un litigio, la probabilidad de que un recurso sea estimado, las ganancias que podrían obtenerse, el fallo más probable, etc.), según el litigio que se trate o el organismo que sea competente para conocer sobre la cuestión;
- Establecer porcentajes de éxito y ayudar a mejorar la calidad de los servicios prestados por el despacho o profesional.

A pesar de tratarse de un proceso aún en desarrollo, cada día más empresas están integrando estas nuevas tecnologías en sus modelos de negocio, obteniendo la información que resulta más relevante de aquellos datos con los que ya cuentan en su posesión para barajar posibles escenarios que puedan serles propicios, a la par que le otorgan un valor añadido a su marca personal.

Será cuestión de tiempo que estos programas acaben resultando imprescindibles –mucho más que las **bases de datos** que se suelen manejar en la actualidad– para que los profesionales desarrollen sus actividades de la manera más eficiente posible.

Aun así, se trata de un terreno en el que el sector legal todavía no está plenamente convencido, en base a los posibles que podría incurrirse al basar nuestras decisiones en torno a un algoritmo informático al no tener en cuenta ciertos condicionantes (como puede ser el **factor humano** a la hora de defender un caso u otro dependiendo de la experiencia del abogado al desarrollar su actividad en salas).

Y tampoco debemos olvidar los riesgos que este tipo de tecnologías pueden entrañar para las libertades y derechos fundamentales de aquellas personas físicas que sean titulares de los datos que puedan ser objeto de cualquier tratamiento automatizado.

2.3. Elaboración de perfiles

Una vez que esos datos hayan sido filtrados por el proceso análisis que hemos explicado en el punto anterior –posiblemente la tarea más ardua en todo tratamiento de datos–, las empresas podrán disponer de un abanico información sumamente sustancial para su modelo de negocio. Información que permitirá establecer ciertos patrones o elaborar una serie de perfiles de consumidores[23], ya sean propios o '*en potencia*' a partir de su creación. Se trata de pronosticar el comportamiento de los potenciales consumidores con el fin de tomar decisiones al respecto.

En la actualidad, esta actividad suele ser desarrollada por muchas organizaciones; de hecho, hay empresas cuya actividad principal consiste en la elaboración de perfiles, especialmente en el sector de la **mercadotecnia digital** cuando realizan campañas publicitarias mediante el envío de correos electrónicos (***e-mail marketing***).

Sin embargo, al hablar de la elaboración de perfiles debemos tener en cuenta que esta actividad no siempre se encuentra amparada a nivel legal, y aquí conviene señalar lo dispuesto por la normativa vigente en materia de protección de datos, tanto a nivel nacional (**artículo 18** de la **LOPDGDD**) como comunitario (**artículo 22** del **RGPD**) por la que no se permite el tratamiento de datos personales por medios automatizados, como es la elaboración de perfiles, que puedan producir efectos jurídicos sobre los interesados, o que pudiera afectarle de manera significativa en atención a las particularidades específicas de cada persona.

Igualmente, el **Considerando 63** del Reglamento Europeo hace referencia al derecho que posee el titular de los datos de carácter personal a conocer aquellos datos que sean objeto de tratamiento y así le conciernan; y además, que estos datos le sean

[23] El **artículo 4.4** del **RGPD** define la **elaboración de perfiles** como "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*".

comunicados las posibles consecuencias que implique cualquier tratamiento de datos personales cuando estos se lleven por medios automatizados.

Aunque por regla general se establezca la prohibición de los tratamientos automatizados sobre datos personales, incluía la elaboración de perfiles, la normativa comunitaria prevé a la par una serie de excepciones concretas en las que el responsable del tratamiento podrá ampararse para proceder a dicho tratamiento. Estas las encontramos en el **artículo 22.2** del **RGPD**:

- Cuando el tratamiento implique la toma de decisiones automatizadas que sean imprescindibles para la celebración de un contrato entre el responsable del tratamiento y el interesado;
- Cuando el interesado en el tratamiento haya prestado su consentimiento expreso (recordemos que no cabe el consentimiento tácito);
- Cuando así lo establezca el derecho de la Unión o el derecho de los Estados miembros donde que resulten de aplicación al responsable del tratamiento.

En cualquier caso, el responsable del tratamiento tendrá el deber de demostrar que ese tratamiento automatizado es indispensable, que la causa que llevó a la elaboración de perfiles es completamente legítima, y que además adoptará las medidas técnicas y organizativas necesarias que asegure la confidencialidad, la integridad y la disponibilidad de la información, garantizando de este modo la privacidad de los interesados en el tratamiento.

Sin embargo, estas excepciones no son óbice para que el interesado pueda ejercer cualquier de los derechos que le son propios, cuando los efectos jurídicos que se desprendan de cualquier tratamiento automatizado afecten a su esfera personal de manera significativa, y siempre que dicho tratamiento sea esencial para llevar a término una misión de interés público encomendada al responsable del tratamiento.

2.4. Ventajas e inconvenientes

Después de conceptualizar lo que entendemos por ***big data***, y tras desarrollar los procesos a los que se ve sometida la información relativa a los interesados en el tratamiento podemos entender las oportunidades que ofrecen este conglomerado de tecnologías emergentes:

- Un entorno más eficiente a la hora de tomar decisiones con una mayor agilidad;
- Un mayor ahorro en los costes, si bien este factor no se percibirá completamente a corto plazo;
- Elaborar mejores estrategias en el ámbito de la mercadotecnia digital a raíz de la elaboración de perfiles, creación de variables, etc.
- Mejorar el rendimiento del modelo de negocio, puesto que gracias a esta suerte de '**realidad 2.0**', la globalización digital ha permitido que el contacto con los usuarios y consumidores sea mucho más directo a la hora de recibir sus consultas, quejas y recomendaciones;

No obstante, todavía hay un cierto halo de incertidumbre en la acumulación masiva de datos y en cuánto puede repercutir esta tecnología en nuestra privacidad y en aquellos datos de carácter personal que nos conciernan. Al igual que el ***big data*** ofrece numerosas ventajas en el día a día de la sociedad, también cuenta con un contrapeso negativo:

- Uno de los principales puntos débiles que afecta a esta tecnología queda íntimamente relacionado al concepto de **anonimización**[24], un proceso que originariamente se estableció para borrar todo rastro de información personal sobre cualquier conjunto de datos. Este proceso, por un lado, ayudaba a mejorar la capacidad de análisis de datos, manteniendo su utilidad; y por otro, se mantenía la privacidad de las personas, cuyos datos eran objeto de tratamiento. Pero el auge del *big data* ha permitido que con el aumento de la capacidad para obtener información también facilite la reidentificación de aquellos sujetos que ya fueran anonimizados anteriormente, o bien mediante el reconocimiento de datos que en su momento no tenían la consideración de carácter personal.
- El hecho de hablar de una práctica que supone buscar y analizar '*cantidades masivas*' de datos es algo que ya de por sí pone en entredicho dos principios básicos de la protección de datos como son la minimización de datos (solo deben ser recogidos los datos estrictamente necesarios, **artículo 5.1.*c)*** del **RGPD**) y la

[24] GIL GONZÁLEZ, E. *Big data, privacidad y protección de datos*. 1ª ed. Madrid: Boletín Oficial del Estado (BOE), 2016, pgs. 78-79.

limitación de la finalidad (es decir, que esos datos que vayan a ser objeto de tratamiento no lo sean ulteriormente para una finalidad incompatible para la que fueren recabados originalmente, **artículo 5.1.*b)*** del **RGPD**).

- Anteriormente hablábamos de la ventaja que supone la agilización de toma de decisiones, pero a su vez implica someter esas decisiones a un desarrollo automatizado, permitiendo que sea un algoritmo informático el encargado de tomar esas decisiones[25], de las que se desprenderían determinados efectos jurídicos sobre las personas físicas.
- En cuanto al aspecto normativo, hay que tener en cuenta que a pesar de hacerse hincapié en la necesidad de contar con el consentimiento expreso del interesado a la hora de solicitar sus datos de carácter personal, algo que el RGPD ha ayudado a fortalecer; en la práctica se demuestra que la gran mayoría de usuarios no suelen tener en cuenta las políticas de privacidad ni los términos y condiciones de uso de las entidades que operan en el entorno digital[26] a la hora de adquirir sus productos o de hacer uso de sus servicios.

Estos son algunos de los desafíos que la normativa en materia de protección de datos tendrá que afrontar. Un terreno que se presenta arduo en el plano legislativo, pero que habrá que tratarse con sumo cuidado, ponderando siempre distintos intereses, y procurando que las personas físicas no sea vean desprotegidas ante el desconocimiento de las nuevas tecnologías o por los actos fraudulentos que determinados responsables puedan llevar a cabo en entornos digitales.

3. OSINT, ¿qué es la inteligencia?

3.1. Concepto de inteligencia

Queda claro que el *big data* supone un verdadero punto de apoyo para las organizaciones a la hora de expandir su modelo negocio. No solo las grandes

[25] Tal como ocurre en el sector bancario, donde la concesión de un préstamo puede depender del riesgo crediticio de la misma persona que vaya a solicitarlo.
[26] Una práctica bastante habitual en los usuarios que crean sus perfiles en redes sociales.

multinacionales, también las pequeñas y medianas empresas han empezado a entender la importancia de los datos que tratan.

Pero además del tratamiento de datos, también merece especial consideración la búsqueda de información y los medios empleados para su captación y los posteriores procesos analíticos a los que se verá sometida toda esa información inicialmente acumulada.

Hablamos de unos procedimientos que permiten compilar una gran cantidad de datos, obtenidos a partir de fuentes dispares y múltiples. A este tipo de proceso se le conoce como **inteligencia de negocio**, cuyo concepto fue definido por el investigador alemán del **IBM *Hans Peter Luhn*** como "*aquella capacidad para captar las interrelaciones de unos hechos planteados de manera que nos permita encauzar la acción hacia aquella meta que buscamos*"[27]. En este proceso de captación cuenta con un amplio espectro de disciplinas[28], pero cabe destacar una figura que poco a poco está tomando notoria relevancia en la búsqueda de información en entornos digitales.

Se trata de la **inteligencia de fuentes abiertas** (a la que nos referiremos a partir de este punto con el acrónimo **OSINT**[29]), un sistema que permite recabar información a través de cualquier medio que pueda considerarse gratuito y "*de público acceso*" a los usuarios: por redes sociales, en foros, *blogs*, diarios digitales, etc. Es decir, una búsqueda que puede ejecutarse mediante el mero uso de un navegador de *Internet*.

No obstante, la inteligencia **OSINT** no solo hace alusión a los recursos que puede proporcionar *Internet*; los periódicos, gacetas, revistas o manuales también constituyen una valiosa fuente de conocimiento e información –y tienen cabida en esta inteligencia de fuentes abiertas–, si bien es cierto que hoy en día, el omnipresente

[27] LUHN, H.P. <<A Business Intelligence System>>. *IBM Journal of Research and Development*. Oct. 1958, vol. 2, núm. 4, 314-319. Fuente: http://altaplana.com/ibm-luhn58-BusinessIntelligence.pdf, <<*The ability to apprehend the interrelationships of presented facts in such a way as to guide action towards a desired goal.*>>

[28] <<Intelligence Threat Handbook. Intelligence Colletction Activities and Disciplines>>. *Federation of American Scientists*. Abril 1996. Fuente: https://fas.org/irp/nsa/ioss/threat96/part02.html, el portal web de la *Federation of American Scientists* detalla con gran precisión ese catálogo de disciplinas de **inteligencia**.

[29] Acrónimo referido a su traducción en inglés ***Open-Source Intelligence***, un concepto que originariamente se usaba –y se sigue usando– en el ámbito militar, el cual ha adquirido una mayor relevancia en la lucha contra el terrorismo.

Internet nos proporciona la facilidad de encontrar o disponer de esos mismos recursos a golpe de *click*.

Hemos mencionado también el carácter gratuito de esta tecnología, ya que además de las redes sociales y páginas web de acceso público, desde Internet también se puede acceder a bases de datos gratuitas y de **código abierto**, desde las que tanto particulares como empresas pueden hacer uso para el almacenamiento de la información (*MongoDB*, *MariaDB*, *PostgreSQL* o *SQLite* son algunas de las más conocidas a nivel global), mejorando a su vez la trazabilidad de los datos en el modelo de negocio de toda organización.

Esto es algo en lo que la normativa comunitaria se está esforzando progresivamente por establecer en el ámbito empresarial, vista la importancia que han adquirido los datos de carácter personal para las grandes tecnológicas como Amazon, Apple, Google o Facebook, constituyendo a día de hoy su activo más valioso.

3.2. Modalidades de fuentes abiertas

Como señalamos al comienzo de este apartado, la inteligencia cuenta con un amplio catálogo de disciplinas: **MASINT** (obtención de información aplicada sobre dispositivos de reconocimiento electromagnético), **SIGINT** (búsqueda mediante la interceptación de señales acústicas), **FININT** (información obtenida en base a índices financieros), **TECHINT** (mediante métodos de carácter técnico, por ejemplo, informáticos o químicos) o **IMINT** (captación de imágenes por cualquier medio: satélite, videovigilancia, infrarrojos, fotográfica, etc.), entre otras. Estas, son algunas de las más destacadas, siendo su espectro más amplio, pero conviene al menos hacer mención a 3 que se encuentran vinculadas en mayor medida a la tecnología **OSINT** por su relevancia en entornos digitales:

- **HUMINT** (*Human Intelligence*): Se refiere a la obtención de información a través de fuentes humanas, es decir, la obtención de información sobre personas humanas mediante otras personas humanas. La práctica más conocida asociada a este término, y originaria, sería el espionaje.
- ***CYBINT** (Cyber Intelligence):* Es la denominada **ciberinteligencia**, aquella para cuya obtención se parte de aquella información que pueden encontrarse en el

ciberespacio; es decir, mediante la utilización de dispositivos informáticos interconectados en la red, ya provengan de sistemas protegidos o inseguros. Aunque es un término que suele estar estrechamente vinculado con la ciberseguridad, no implica necesariamente que se trate exclusivamente de una inteligencia desarrollada en el marco de la defensa contra amenazas de carácter cibernético; el mero hecho de contrastar una misma información en distintos medios, o el intercambio contenidos en red con otros usuarios, al margen de que hubiera implicaciones legales o éticas, conlleva el desarrollo de una actividad de este tipo de inteligencia.

- **SOCMINT** (*Social Media Intelligence*): Se trata más bien de un subtipo de inteligencia, ya que bien podría situarse dentro de la ciberinteligencia, e implica la obtención de información necesariamente a través de las redes sociales (también denominadas con la abreviatura **RRSS**), como *Facebook*, *Twitter*, *Instagram*, *LinkedIn*, *YouTube*, entre otras muchas.

  Posiblemente sea uno de los tipos de inteligencia con mayor impacto en la actualidad, debido a la cantidad de pesquisas que se pueden obtener sobre otras personas en estos entornos digitales.

  Un buen ejemplo del posible uso que se le puede dar a las redes sociales como medio de búsqueda de información podemos encontrarlo en la película ***Searching***[30], en la cual un padre decide investigar la desaparición de su hija a través de su portátil, analizando todo rastro digital que esta hubiera podido dejar en la red.

  Todas estas disciplinas parten de esa convergencia[31], la posibilidad de acceder a una amplia información disponible a cualquier usuario mediante fuentes abiertas que permita su compilación y analizarla para aquellos fines que consideremos pertinentes, con ciertas concesiones. Esto ha permitido convertir a Internet en un

[30] ***Searching***. Dirigida por Aneesh CHAGANTI. EE.UU.: Stage 6 Films, 2018. Disponible en ***Movistar+***: http://www.movistarplus.es/ficha/searching?tipo=E&id=1604292

[31] JIMÉNEZ VILLALONGA, R. <<Tipos de Inteligencia>>. *Grupo de Estudios sobre Seguridad Internacional*. 26 noviembre 2018. Disponible en: http://www.seguridadinternacional.es/?q=es/content/tipos-de-inteligencia, para un estudio más profundo y detallado de la materia, el Grupo de Estudios sobre Seguridad Internacional de la **Universidad de Granada** ha compilado una descripción más amplia sobre estas disciplinas emergentes sobre los procesos de inteligencia en medios digitales.

> sistema de vigilancia inexpugnable, nada escapa al ojo del Gran Hermano del siglo XXI: todo aquello que se publique queda registrado y almacenado en algún punto del vasto páramo digital sin necesidad de que se despoje al usuario de esa información que ha podido hacer pública.

Debido a esto, entendemos las implicaciones que constituyen el entendimiento y el manejo de la inteligencia **OSINT**. Esta cuenta con un doble reverso, el cual puede ser beneficioso o perjudicial, según la finalidad que se persiga o el sujeto que haga uso de la misma.

Actividades tan cotidianas como buscar un correo electrónico, encontrar amigos en las redes sociales o descargar contenido audiovisual para su posterior consumo son actividades **OSINT** habituales y es información que se encuentra al alcance de cualquier usuario. Así, podemos dividir el proceso de obtención de información mediante fuentes abiertas en distintas etapas:

- Encontrar aquellas fuentes de información más destacadas.
- Escudriñar la información que nos interesa.
- Tratar la información recabada que nos llevará a su posterior análisis.
- Proceder al análisis de la información y extraer aquellos datos que realmente resulten de utilidad práctica.
- Procesar la información para alcanzar un resultado específico y viable.
- Obtener del proceso una información que pueda exteriorizarse de forma útil que nos permita obtener el fin que se perseguía en un origen.

Por ello, a la hora de desarrollar procesos mediante inteligencia **OSINT**, es conveniente conocer algunas herramientas necesarias para cumplir con estas etapas con la mayor eficiencia.

Estas herramientas pueden proporcionar información de muy útil y de diversa índole: constatar si un determinado nombre de usuario se encuentra disponible, o si por el contrario se ha registrado en más de una plataforma; identificar si ante posibles brechas de seguridad en un sistema, estas hayan dado como resultado la filtración de determinados datos (correos electrónicos, teléfonos personales, contraseñas, etc.); escanear los puertos abiertos de un sistema, identificar fuentes de información sobre geolocalización, establecer mapas de redes inalámbricas, cotejar las expresiones más

habituales de una determinada web, o investigar si un determinado usuario tiene un mismo perfil en distintas *webs* o redes sociales, son algunas de las funcionalidades que pueden ofrecer el uso de este material tecnológico.

En cuanto a dichas herramientas **OSINT**, podemos destacar un par de ejemplos que son muy socorridos a nivel global.

Por un lado tenemos **MALTEGO**, cuya finalidad principal es la recopilación de información basada en la **minería de datos**, posiblemente sea una de las mejores herramientas del mercado en este campo, aunque cuenta con una versión gratuita[32], con ciertas limitaciones respecto a la cantidad de resultados que podemos obtener. Se trata de una herramienta con una mecánica bastante intuitiva, ya que una vez tratada y procesada la información esta es representada visualmente mediante gráficos.

Además, permite consultas sobre datos personales de usuarios (como una dirección de correo electrónico, un número de teléfono, afiliación a determinadas organizaciones, etc.) y posibilitando encontrar sus perfiles en redes sociales. Este último apartado puede servir de mucha utilidad a las empresas a la hora de elaborar perfiles.

Como hemos dicho, cuenta con una versión gratuita, pero pese a su limitación sirve de mucha utilidad, demostrando hasta qué punto podemos tener comprometida nuestra privacidad.

Por otro lado, anteriormente los usuarios también contaban con otra herramienta referente para la inteligencia **OSINT** llamada **WhoIS**, un protocolo **TCP/IP**[33] que actuaba como un consultorio mediante un sistema de petición-respuesta.

A través de la interfaz que proporcionaba en el buscador de su web podíamos realizar consultas sobre cualquier dominio existente en *Internet* y encontrar información sobre el mismo: sus datos de contacto del titular (o de la entidad que registró dicho dominio), su dirección postal, teléfono de contacto, correo electrónico, el nombre del servidor donde se alojaba ese dominio, las fechas de creación, actualización y

[32] Si resulta de interés, adjunto enlace de descarga para la versión **Maltego CE**, de uso gratuito: https://www.paterva.com/web7/downloads.php. Eso sí, será necesario registrarse en la Comunidad y dar algunos datos personales; podemos entender que igual no es tan '*gratuito*'.

[33] El acrónimo **TCP/IP** hacen referencia al **Protocolo de Control de Transmisión** / **Protocolo de Internet** (***Transmission Control Protocol*** / ***Internet Protocol***) que a grandes rasgos conforma el sistema de comunicación y transmisión de paquetes de datos entre sistemas operativos a través de la red. Es la base sobre la que se fundamenta ***Internet***.

expiración del dominio, así como cualquier otro dato que fuera necesario para localizar dicho dominio en la red.

Se trataba de una herramienta desarrollada por la **ICANN**[34], cuya información quedaba contenida y almacenada en su base de datos, quedando entonces al alcance de todos aquellos usuarios que quisieran hacer uso de la misma.

No obstante, el 25 de mayo de 2018 se materializó la obligatoria aplicación del **RGPD**, y con ella este tipo de aplicaciones han dejado de tener aplicabilidad en la red.

Un paso ciertamente lógico con la llegada del Reglamento, puesto que acceder de manera pública a datos de carácter personal de los titulares de estos dominios (como decíamos anteriormente, podían tratarse de datos pertenecientes tanto a personas físicas como jurídicas) sin el consentimiento expreso de los mismos supone no menos que una contrariedad al *íter* y a los principios fundamentales marcados por la nueva normativa vigente en materia de protección de datos.

Por ello, la **ICANN** aún sigue en proceso para establecer un nuevo modelo de protocolo, con el objetivo de que puedan seguir operando como lo han hecho hasta la fecha, pero adecuándose a lo establecido por la normativa comunitaria.

A pesar de este nuevo panorama legislativo, y salvando algunas excepciones, los usuarios todavía pueden hacer uso de ciertas directrices y herramientas para poder recabar información de otras personas a través de las fuentes abiertas.

También sería importante hacer un breve inciso en el camino, para comentar que la inteligencia de fuentes abiertas, por su propia definición, está estrechamente vinculada al ***Open Data*** (o **dato abierto**), una corriente que persigue el libre uso de toda aquella información que se encuentre disponible públicamente[35], siempre que se atribuya la autoría originaria de la misma. Es decir, información de libre acceso para los usuarios y que pueda ser susceptible de modificación o libre difusión entre los mismos para cualquier finalidad que persigan, con ciertas concesiones.

---

[34] **ICANN** es el acrónimo de la ***Internet Corporation for Assigned Names and Nunmbers***, una organización sin ánimo de lucro que opera a nivel internacional y se dedica asignar dominios (páginas *web*) a todas aquellas persona, física o jurídica, que lo solicite. Es una entidad que trata de velar por la operatividad en la red.

[35] <<¿Qué son los datos abiertos?>>. *Open Data Handbook*. Disponible en: http://opendatahandbook.org/guide/es/what-is-open-data/, a fin de divulgar el **conocimiento abierto**, la *Open Knowledge Foundation* ofrece una definición más completa sobre el ***open data*** en el enlace aportado (también en **español**).

Ciertamente se trata de una filosofía que recuerda a la ya iniciada por **Lawrence Lessig** cuando fundó la entidad ***Creative Commons***, que buscaba el libre acceso a la cultura y al intercambio de la misma en el entorno digital, de acuerdo a la licencia que se le hubiera establecido a un contenido u otro.

No obstante, es importante incidir que el dato abierto puede entrar en colisión con los datos de carácter personal, en cuanto que el acceso a estos últimos se encuentran limitados al consentimiento de su titular. Por tanto, sería conveniente que cualquier dato personal que pretenda convertirse en público o abierto, sea tratado de manera que pierda todo rastro del titular del mismo (anonimización), o bien tratarlos sin aquellos atributos que identifican a su titular, pero sin desvincularlos del mismo (seudonimización).

También conviene no confundir esta corriente denominada ***Open Data*** con el movimiento del ***Software Libre***, el cual busca facilitar a los usuarios de *softwares* la posibilidad de analizarlos, modificarlos según su conveniencia y distribuirlo libremente, sin verse limitado por las restricciones que impone el mercado y las licencias de *softwares* privados.

Si bien es cierto que se encuentran ciertas semejanzas en base a los valores éticos que ambos promulgan de compartir el conocimiento de manera libre y altruista con todo usuario que así lo desee –el nuevo mito del Prometeo tecnológico–, no está relacionado con los datos *per se*.

Podemos sintetizar que el ***open data*** es un movimiento que en la práctica se extiende tanto en el sector público como privado, si bien es cierto que para las instituciones públicas tiene una mayor incidencia de acuerdo con el principio de transparencia potenciado tras la irrupción del **RGPD**.

La globalización y la irrupción de las nuevas tecnologías han conseguido que la sociedad haya avanzado a un panorama donde la transparencia juega un rol fundamental dentro del tratamiento de datos, especialmente debido a factores como la incursión de medio que computan en la nube; pero que a su vez siguen conllevando una serie de riesgos para la privacidad de las personas físicas, que se han visto acentuados con el *Internet de las cosas*, permitiendo la interacción de los usuarios con aquellos objetos y/o dispositivos habituales en su día a día.

Es cierto que este tipo de fenómenos han traído ciertos beneficios, aligerándonos la carga de aquellas tareas que podamos realizar en nuestra vida cotidiana, conectando estos dispositivos mediante *Internet*, permitiendo su actualización ininterrumpida y mejorando la capacidad de redireccionamiento al poder configurarlos a través de la red.

Pero por otro lado, esto también puede dar lugar a una serie de riesgos para la privacidad de las personas físicas, implicando la exposición de nuestros hábitos y preferencias, los cuales podrían ser obtenidos y procesados por organizaciones dirigidas a elaborar perfiles y ofreciendo de esta manera unos productos o servicios personalizados en función de las necesidades del consumidor.

También puede conllevar otra serie de problemáticas legislativas, debido a la inexistencia de unos estándares establecidos que permitan atestiguar que estos dispositivos con las medidas de seguridad oportunas en los procesos de fabricación.

Esto que algo que se contrapone directamente a dos principios fundamentales en la protección de datos, como son la privacidad desde el diseño (***privacy by design***) y por defecto (***privacy by default***).

A su vez, la irrupción de las **NNTT** aplicadas a estos dispositivos también puede recopilar datos mediante señales inalámbricas, todo ello sin nuestro consentimiento, lo que a su vez contradice los deberes de información (**artículo 12.3** del **RGPD**) por parte del responsable –o encargado– del tratamiento y en la obtención del consentimiento expreso del interesado en cuanto a la licitud del tratamiento de sus datos personales (**artículo 6.1.*a)*** del **RGPD**).

Es por esto que el nuevo marco legislativo internacional debe buscar una vía que garantice unos niveles de seguridad básicos para los usuarios.

4. Monitorización

4.1. Concepto

Otro punto clave en este trabajo de investigación recae sobre la **monitorización** a la que podemos vernos sometidas las personas físicas a través de nuestra interacción con las nuevas tecnologías. Se trata de una serie de procesos establecidos tanto por

personas físicas como jurídicas, los cuales permiten analizar o vigilar a los usuarios en su día a día, recabando a su vez datos de los mismos mediante el uso de aplicaciones, o bien mediante la observancia que puede proporcionar los sistemas de videovigilancia, ya sea en entornos públicos o privados.

No obstante, cuando hablamos de tratamientos en los que intervienen un sistema de monitorización cabe diferenciar la finalidad que puede perseguirse. Pues dicha finalidad ayudará a hacernos una idea de lo sensible que puede ser ese tratamiento, los posibles riesgos –así como su tipología– que pueden derivarse del mismo, y las medidas que por tanto corresponderán aplicar.

No es lo mismo someter a los afectados a un sistema de videovigilancia, el cual puede legitimarse en la seguridad ciudadana, o en la salvaguarda de personas o bienes, que la observación reiterada y sistemática de determinados usuarios para analizar sus patrones, lo cual puede llevar a la elaboración de perfiles por parte del responsable del tratamiento con la que rentabilizar su modelo de negocio.

Los riesgos pueden variar en función del tratamiento que se pretenda realizar, lo que significa que deberá realizarse una gestión eficaz del riesgo que lleve asociada dicha monitorización, estableciendo las medidas necesarias para reducir o minorar los eventuales riesgos que implique el tratamiento y garantice las libertades y derechos fundamentales de aquellos sujetos sometidos a una constante monitorización.

A continuación, iremos desglosando cada uno de los entornos digitales donde los usuarios desarrollan su día a día, las formas en que estos pueden ser monitorizados en cada uno de ellos, y los riesgos a los que quedan expuestos.

4.2. Monitorización en entornos digitales

4.2.1. Páginas webs, foros y redes sociales

Podríamos decir que *Internet* ha resultado ser la herramienta más eficiente para monitorizar a los usuarios y obtener una ingente cantidad de información, tanto personal como no personal. Más aún cuando hablamos de las **RRSS**, un instrumento que –para la mayoría de personas– a día de hoy supone una extensión de nuestra propia persona: interactuamos con conocidos y terceros; vertemos nuestras opiniones y sentimientos respecto a determinados temas (lo que a su vez puede exponer

determinadas creencias o ideologías al ojo público); compartimos nuestras canciones, series o películas favoritas; publicamos *stories* de nuestros viajes de vacaciones, etc.

Y es ente punto donde la tecnología **OSINT** puede encontrar su mayor utilidad, ya que gracias a la elevada participación de sus usuarios y la inmediatez con la que llegan interactuar unos entre otros para conversar sobre acontecimientos destacables puede arrojar cierta información relativa a esos mismos usuarios de una manera prácticamente accesible para toda clase de público, datos que pueden convertir a las redes sociales en el objeto perfecto para el empleo de técnicas de tecnología **OSINT**, puesto que pocas personas suelen tener conocimiento de los mecanismos de privacidad con los que dichas redes cuentan.

En estos términos, podríamos empezar centrándonos en una red social que se adecua perfectamente a las necesidades que requiere la tecnología de fuentes abiertas, como es ***Twitter***. Se trata de una **RRSS** fundada en 2006, cuya mecánica se basa en el envío y recepción de mensajes breves[36], contando con un máximo de 280 caracteres (si bien en su origen el límite se encontraba en los 140 caracteres máximos). Estos mensajes pueden ser publicados en abierto para toda la comunidad integrante de la red –cabe mencionar que los perfiles pueden ir asociados tanto a personas físicas como a personas jurídicas u otras organizaciones–, o bien ir dirigidos a uno o varios usuarios expresamente.

La finalidad de esta **RRSS** no deja de ser otra que la interacción entre todos los usuarios que integran su comunidad, difundiendo noticias de actualidad, eventos, opiniones, así como cualquier otro tipo de contenido meramente divulgativo.

Actualmente ***Twitter*** cuenta aproximadamente con 330 millones de usuarios activos[37], una tercera parte de los que posee ***Instagram***, y hasta una séptima parte del total de los perfiles con los que cuenta ***Facebook***; no obstante, sigue siendo una de las herramientas más necesarias para el sector del *marketing* digital debido a su interacción en tiempo real con los demás usuarios, lo que la convierte en el canal de

[36] Esta técnica se denomina ***microblogging***.

[37] CLEMENT, J. <<*Number of mothly active Twitter users worldwide from 1st quarter 2010 to 1st quarter 2019 (in millions)*>>. *Statista*. 14 agosto 2019. Fuente: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

comunicación idóneo para las marcas, organizaciones y otras entidades[38] que cuentan con cierta influencia en entornos digitales; lo que a su vez permite que dicha red sea un excelente conductor para el desarrollo de técnicas de monitorización a través de la tecnología **OSINT**.

Como ya desarrollamos en el punto anterior, la inteligencia de fuentes abiertas permite compilar información procedente de numerosas fuentes de acceso público que posteriormente se somete a un análisis con la finalidad de crear un patrón para la toma de decisiones. Y aunque a la hora de obtener información por estos medios los responsables del tratamiento han de cumplir necesariamente con el deber de información para con los titulares de dichos datos, en la práctica vemos como incluso las grandes multinacionales ni siquiera cumplen con estos preceptos básicos, como es el caso de ***Twitter*** que recientemente comunicó haber sufrido ciertos problemas de seguridad en el seno de su sistema de información, lo que les ha permitido utilizar datos de sus usuarios para llevar a cabo campañas publicitarias personalizada, sin haber sido informados previamente de dicha actividad y sin obtener debidamente su consentimiento[39].

No obstante, este tipo de técnicas no son objeto únicamente de marcas u otras entidades corporativas. En lo relativo a la seguridad de la información, los organismos públicos también cumplen una función esencial para la defensa de los derechos y libertades de las personas físicas aun cuando hablamos de entornos digitales, sobre todo cuando se trata de prevenir actos relacionados con el terrorismo. Aquí podríamos destacar la constante labor desempeñada por los Cuerpos y Fuerzas de Seguridad del Estado, siendo un caso bastante sonado su interacción con la comunidad de ***Twitter*** a raíz del atentado sufrido en Barcelona los días 17 y 18 de agosto 2017[40], donde un

[38] Habitualmente, las empresas y las marcas que cuentan con un perfil en cualquier red social, estas suelen ser gestionadas por ***Community Managers*** o **CM** (sus siglas en inglés), profesionales del *marketing* digital que se encargan del mantenimiento y el desarrollo de la comunidad *online* de la marca o entidad a la que representa en el entorno digital. Una de sus funciones principales es aumentar dicha comunidad y captar subscriptores y potenciales clientes.

[39] ALONSO, R. <<*Twitter ha estado usando datos de sus usuarios para publicidad sin tener permiso*>>. *ABC Redes*. 8 agosto 2019. Fuente: https://www.abc.es/tecnologia/redes/abci-twitter-estado-usando-datos-usuarios-para-publicidad-sin-tener-permiso-201908080938_noticia.html

[40] CAMPOS, C., MARTÍN PLAZA, A. <<*Atentado en Barcelona y Cambrils. El día después de los atentados en Cataluña: cuatro detenidos y un huido*>>. *RTVE*. 18 agosto 2017. Fuente: http://www.rtve.es/noticias/20170818/atentado-barcelona-directo/1599220.shtml

furgón atravesó el paseo de la Rambla (día 17), cobrándose la vida de 15 personas y dejando más de un centenar de heridos; al día siguiente se produciría otro atropello en la localidad tarraconense de Cambrils (día 18), donde se cobró la vida de una mujer y quedaron 6 heridos. Posteriormente, este acto fue reivindicado por el **Estado Islámico**[41].

En este caso, la intervención de los Cuerpos y Fuerzas de Seguridad a través de la red no fue tanto para llevar a cabo una función investigadora, sino más bien buscaba como objetivo el reducir la alarma social entre la comunidad, además de tratar de entorpecer la difusión del ilícito perpetrado por la organización terrorista a través de cualquier medio digital. Por ello, pidieron la colaboración ciudadana para no difundir fotografías o vídeos de la situación de la ciudad durante el trágico suceso[42], idea de la que se hizo eco a través de los medios de comunicación[43].

No obstante, ni ***Twitter*** ni el resto de redes sociales son las únicas herramientas de las que se sirven las autoridades policiales para la prevención e investigación de hechos ilícitos, también suelen recabar información mediante la monitorización de páginas web en sí y de foros.

Concretamente, son en foros integrados por una comunidad plural, como por ejemplo ***4Chan*** –una comunidad de origen angloparlante, pero cuyo mayor grueso comparte afición por la cultura asiática–, donde las autoridades suelen realizar una actividad de monitorización intensiva sobre sus hilos, puesto que es habitual encontrar en este entorno digital material de dudosa legalidad, muchas veces relacionado con la violencia extrema y con la pornografía infantil.

---

[41] También denominado ***Daesh*** o **ISIS**.

[42] POLICIA NACIONAL <<*Por respeto a las víctimas y a sus familias, por favor, NO compartas imágenes*...>>. *Twitter*. 17 agosto 2017, 17:45. Fuente: https://twitter.com/policia/status/898209070993338368. Fue una iniciativa que se hizo viral en la comunidad de *Twitter* al inundar la red de fotos de gatos a fin de no extender el pánico ni crear un estado de alarma social.

[43] LÁZARO, M. <<*Por qué Twitter se ha llenado de gatos tras el atentado de Barcelona*>>. *Huffington Post*. 18 agosto 2017 Fuente: https://www.huffingtonpost.es/2017/08/17/por-que-twitter-se-ha-llenado-de-gatos-tras-el-atentado-de-barce_a_23080797/. Se trató de un movimiento surgió como una suerte de réplica a la iniciativa originada por los usuarios belgas a raíz del atentado de Bruselas del 22 de marzo de 2016, donde la comunidad llenó la red social con fotos de patatas fritas que englobaba un doble significado: como símbolo gastronómico de la ciudad afectada, y de resistencia frente a la adversidad. Fuente: https://www.huffingtonpost.es/2016/03/22/atentados-bruselas-patatas-fritas_n_9521522.html

De hecho, un caso reciente que se acabó tornando mediático fue el de ***Bianca Michelle Devins***, una adolescente estadounidense aficionada a los videojuegos y miembro de dicha comunidad que fue asesinada y decapitada por un conocido de la propia víctima, el cual acabó compartiendo varios stories en su perfil de ***Instagram*** con imágenes de la cabeza decapitada de la joven Bianca. Estas imágenes no tardaron en acabar circulando por ***4Chan***, y fue aquí donde las autoridades policiales prosiguieron con la investigación hasta dar con su asesino[44].

Sin duda, esta labor ejercida por las fuerzas policiales se encuadra en el marco de la monitorización con una clara finalidad investigadora y preventiva, a través del empleo de las nuevas tecnologías mediante la búsqueda en fuentes que podemos considerar plenamente accesibles para el usuario medio –conviene no confundir que sea una fuente plenamente accesible a cualquier persona mediante cualquier dispositivo tecnológico, a que sean fuentes fácilmente accesible–.

No obstante, tampoco podemos decir que todos los organismos públicos hagan uso de las tácticas basadas en la tecnología **OSINT** para, en principio, prevenir actos que atenten directamente contra nuestros derechos fundamentales.

Para aquellos profesionales dedicados a la protección de datos personales no nos es ajeno, a la luz de los hechos más recientes tras la llegada de la nueva **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales**, que en su **Disposición Final Tercera**, segundo apartado (en relación con el **artículo 58 *bis*** de la **Ley Orgánica 15/1985, de 19 de junio, del Régimen Electoral General**) "*Los partidos políticos* [...] *podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral*".

Una cuestión que la **AEPD** acabó resolviéndose de manera ágil, y favorable para los interesados o afectados por el tratamiento de sus datos personales, a través de la **Circular 1/2019, de 7 de marzo**, con unos criterios de interpretación restrictiva sobre

[44] KHRON, R. *<<17-Year-Old e-Girl Bianca Devins was killed by jealous family friend>>. eBaum's World*. 15 julio 2019. Fuente: https://www.ebaumsworld.com/articles/e-girl-bianca-michelle-devins-murdered-by-her-incel-orbiter/86016368/

aquellos datos que puedan ser efectivamente objeto de tratamiento, desplegados en su **artículo 5**[45].

Esta situación no es ajena para los especialistas en privacidad. En los últimos años hemos sido testigos de cómo esta tecnología basada en la captación de datos a través de fuentes abiertas ha resultado trascendental para el devenir de este Nuevo Orden Mundial establecido.

Un escenario ejemplarizante lo tuvimos en 2018, cuando los medios de comunicación dieron a conocer el escándalo iniciado por la titánica red social ***Facebook*** y la empresa ***Cambridge Analytica***, a raíz de las elecciones presidenciales de Estados Unidos en 2016.

Cambridge Analytica (también denominada **CA**) fue una consultora británica especializada en la minería y análisis de datos, que acabó convirtiéndose en todo un referente sobre decisiones estratégicas en el marco de campañas electorales de carácter nacional en decenas de países a lo largo del mundo (Estados Unidos, Canadá, Reino Unido, Italia, Lituania, Ucrania, Rumanía, Antigua y Barbuda, San Cristóbal y Nieves, Argentina, Brasil, Colombia, México, Birmania[46], India, Indonesia, Libia, Malasia, Tailandia, Ghana, Kenia, Nigeria, Sudáfrica, Trinidad y Tobago, etc.) y que además llegó a ser un elemento decisivo en la victoria del movimiento de salida de la Unión Europea por parte del Reino Unido (movimiento que tomó el nombre de ***Brexit***), así como en la victoria de **Mauricio Macri** al alcanzar la Presidencia de la República Argentina en 2015, ya que la consultora colaboró con el gabinete del candidato[47] al llevar a cabo una campaña ofensiva contra la anterior presidenta Cristina F. de Kirchner.

Pero alcanzó una mayor trascendencia a raíz de la campaña electoral de Estados Unidos en 2016, al colaborar estrechamente con el entonces candidato electo

[45] Fuente: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-3423

[46] WAROFKA, A. <<*An Independent Assessment of the Human Rights Impact of Facebook in Myanmar*>>. *Facebook Newsroom*. 5 agosto 2018. Fuente: https://newsroom.fb.com/news/2018/11/myanmar-hria/. En 2018, ***Facebook*** emitió un informe donde desde la propia entidad admitieron públicamente que pudieron tener un papel clave en el conflicto étnico perpetrado contra la población *rohingya* en Birmania.

[47] JUÁREZ, S. <<*Cambridge Analytica y ejercito de trolls: confirman la manipulación en las elecciones 2015*>>. *Canal Abierto*. 31 julio 2018. Fuente: https://canalabierto.com.ar/2018/07/31/cambridge-analytica-y-ejercito-de-trolls-confirman-la-manipulacion-en-las-elecciones-2015/amp/

republicano **Donald Trump** en su campaña hacia la Presidencia. Su colaboración se basó en la captación de las cuentas de usuarios estadounidenses en ***Facebook***, principalmente de usuarios residentes en determinados estados (Florida, Michigan y Pennsylvania, sobre todo) que podían resultar decisivos para el bando republicano en el momento del escrutinio; y por lo general, la captación de los datos personales que realizaban a través de la red social se centraban en aquellos usuarios que denominaban '*votantes indecisos*'. Analizando los perfiles de estos votantes, y en base a las publicaciones que estos compartiesen, **CA** podía enviar una publicidad personalizada dirigida a este tipo de usuarios, consiguiendo de esta manera un efecto realmente significativo que pudiera materializarse en el momento de la votación.

No obstante, aunque estas operaciones se llevaron a cabo durante la campaña electoral entre 2015 y 2016, no fue hasta mediado de 2018 cuando las grandes editoriales internacionales –como el periódico americano *The New York Times* o el diario británico *The Guardian*– hicieron público el fraude perpetrado por ***Cambridge Analytica*** a raíz de las declaraciones emitidas por **Christopher Wylie**[48], un ex-empleado de la consultoría que, tras abandonar la compañía en 2014, informó a ***Facebook*** de la monitorización que efectuaba **CA** con los datos de sus usuarios de manera indebida, y sin contar con el conocimiento ni el consentimiento de los mismos.

Una vez filtrada esta información por los medios, en abril de 2018 el propio fundador de la red social, **Mark Zuckerberg** ofreció un comunicado donde se responsabilizó personalmente por la 'brecha de confianza'[49] que surgió entre ***Facebook*** y sus usuarios; lo que recientemente ha llevado a la **Comisión Federal de Comercio de Estados Unidos** (***Federal Trade Commission***) imponer a la gran red social una multa de

[48] CADWALLADR, C. *<<'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower>>. The Guardian*. 17 marzo 2018. Fuente: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[49] Este comunicado tuvo lugar en el seno de la comparecencia de Mark Zuckerberg ante el Comité de Comercio, Ciencia y Transporte y el Comité Judicial del Senado de Estados Unidos. Fuente: https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data

5.000 millones de dólares[50], por su *mala praxis* en el tratamiento de los datos personales de más de 87 millones de usuarios.

En cuanto a la consultora privada, en mayo de 2018, ***Cambridge Analytica*** se declaró en bancarrota como consecuencia del escándalo[51], echando el cierre a su andadura.

Para ilustrar de manera más gráfica el origen de este acontecimiento, conviene destacar que recientemente la plataforma de contenido en streaming ***Netflix*** puso a disposición de sus abonados el documental "**El Gran Hackeo**"[52], donde se hace hincapié en los peligros a los que se ven expuestos los usuarios debido al mal uso de las nuevas tecnologías y a la explotación de la información de carácter personal usando como trasfondo los sucesos ya conocidos sobre ***Facebook*-CA**.

4.2.2. Apps

Otro entorno digital donde la monitorización está adquiriendo cada vez mayor relevancia lo encontramos en los dispositivos móviles, instrumentos que a día de hoy se ha convertido prácticamente en una extensión de nuestras propia personas: nos comunicamos con nuestros más allegados y terceros mediante aplicaciones de mensajería instantánea, llevamos a cabo nuestras tareas profesionales y mandamos correos a través de los mismos, controlamos nuestras redes sociales y nuestra economía mediante aplicaciones, establecemos nuestros hábitos de vida y los dejamos registrados en nuestros dispositivos, y un sinfín de actividades que quedan circunscritas en nuestra esfera más privada e íntima.

Por ello es importante que los usuarios sean conscientes tanto de las ventajas que nos brindan estas nuevas tecnologías: la facilidad de acceder a la información a través de los navegadores, la brevedad para comunicarse con las demás personas gracias a la mensajería instantánea, la utilidad de los sistemas de geolocalización que nos

[50] REDACCIÓN BBC NEWS MUNDO <<*Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios*>> *BBC News*. 24 julio 2019. Fuente: https://www.bbc.com/mundo/noticias-49093124. Se trata de la multa más elevada impuesta a ***Facebook*** hasta la fecha.

[51] LUMB, D. <<*Cambridge Analytica is shutting down following Facebook scandal*>>. *Engadget*. 2 mayo 2018. Fuente: https://www.engadget.com/2018/05/02/cambridge-analytica-is-shutting-down-following-facebook-scandal/

[52] ***The Great Hack***. Dirigida por Karim AMER y Jehane NOUJAIM. EE.UU.: Netflix, 2019. Disponible en ***Netflix***: https://www.netflix.com/title/80117542

permiten llegar a nuestro destino por las rutas más efectivas, etc.; así como de los riesgos a los que nos vemos expuestos por el uso indebido de las mismas, que pueden materializarse tanto en lo que respecta a la privacidad de las personas:

- El mal empleo que hagamos de nuestros datos, o bien el mal uso que terceros quienes gestionen nuestros datos de forma inapropiada o para fines cuestionables–;
- La posible revelación de información relativa a nuestros ámbitos más íntimos;
- La obtención de información de carácter personal por entidades u organización cuyo objetivo sea la elaboración de perfiles para ofrecer a sus usuarios productos o servicios personalizados de acuerdo a sus hábitos o sus gustos;
- La posibilidad de verse afectados por fraudes o cualquier otra amenaza a través de los medios digitales (*ransomware*, *phishing*, *malware*, *spam*, etc.);
- Otro tipo de amenazas realmente gravosas son aquellas que pueden involucrar a los menores de edad, sujetos susceptibles de una mayor protección, y es que en los entornos digitales estos pueden llegar a ser víctimas de conductas ilícitas como el *sexting* o por delitos de tráfico de pornografía infantil;

O bien que afecten a aquellos aspectos relacionados con el estado de la salud de las personas:

- La adicción o dependencia de estos dispositivos, una conducta que cada vez tiene un mayor incremento en las generaciones más jóvenes, llegando a causar un cierto grado de aislamiento social para con las demás personas en entornos físicos o trastornos de ansiedad;
- Las dolencias físicas que podemos sufrir al adoptar a largo plazo posturas molestas debido al uso reiterado de los dispositivos móviles;
- E incluso la posibilidad de causar accidentes de tráfico mortales por no prestar atención a lo que ocurre a nuestro alrededor.

Como decimos, es necesario advertir a los usuarios no solo del mal uso que estos pueden ejercer sobre sus datos cuando dicha información quede contenida en sus dispositivos móviles, sino también de las posibilidades que las aplicaciones que tengan instaladas en estos dispositivos no cuenten con las medidas de seguridad necesarias para garantizar los derechos fundamentales de las personas físicas, bien por sus

posibles fallas, o porque durante el desarrollo de una aplicación no se hubieran tenido en cuenta los principios de **privacidad desde el diseño** (*privacy by design*) y **por defecto** (*privacy by default*).

No es inusual encontrarnos en la actualidad con aplicaciones que incurren en ilícitos relacionados con la falta privacidad de los usuarios que las instalan en sus dispositivos inteligentes, que varían desde herramientas que pueden manipular nuestras fotografías para determinar, en base a un algoritmo, cómo será nuestro rostro a la vejez hasta a aplicaciones destinadas al uso culinario[53].

Aunque sin duda, uno de los casos más recientes y sonados a nivel nacional fue el procedimiento sancionador iniciado por la **AEPD** contra la **Liga de Fútbol Profesional** debido a que esta última desarrolló una aplicación[54] con la que sus usuarios podían seguir el minuto y resultado de los partidos en directo.

No obstante, dicha aplicación infringía el principio de transparencia (**artículo 5.1** del **RGPD**), pues al proceder a su instalación no se informaba debidamente a los usuarios que la misma autorizaba los permisos necesarios para activar los micrófonos de los dispositivos móviles, cuya última finalidad sería tener constancia de los bares y locales que emitían partidos de **LaLiga** de manera fraudulenta, sin abonar las cuotas correspondientes.

La cuestión radica en que al tener activada la aplicación durante la emisión de los partidos, ésta capta la acústica de la posición donde se encuentra el usuario, reconociendo así su emisión. A este tratamiento se añade que la aplicación cruza tal información con las coordenadas de geolocalización del dispositivo y se trasladaban a

[53] KAINTURA, P. <<*Hackers discover microphone hidden in Lidl's kitchen robot*>>. *TechGrits*. 15 junio 2019. Fuente: http://www.techgrits.com/hackers-discover-microphone-hidden-in-lidls-kitchen-robot-video/. Recientemente, unos usuarios aficionados a las nuevas tecnologías adquirieron un robot de cocina distribuido por la cadena alemana de supermercados ***Lidl*** y decidieron alterar un software que lleva incorporado para así poder jugar al videojuego clásico ***Doom*** a través de su pantalla táctil. No obstante, durante su investigación, hallaron que este modelo de robot llevaba incorporado además un micrófono oculto en su interior. Posteriormente el **CMO** (*Chief Marketing Officer*) francés de la franquicia informó que este se incorporó para futuras actualizaciones en caso de que fuera compatible con ***Alexa***, por lo que hasta la fecha su utilidad era nula; no obstante, al tratarse de un dispositivo que no se actualizaba desde 2017, sería muy probable que se viese afectado a ciertas vulnerabilidades en cuanto a su seguridad. Para mayor información, adjunto un artículo donde se amplía la noticia sobre esta aplicación.

[54] Resolución de la AEPD (Proc. Nº PS/00326/2018). Fuente: https://www.aepd.es/resoluciones/PS-00326-2018_REC.pdf. También denominada como *app* **LaLiga**

su base de datos con aquellos locales dedicados al sector de la hostelería que cuentan con sus licencias de emisión, por lo que si no figuraba en esta se procedía a la inspección de este local.

Posteriormente, **LaLiga** aclaró que la activación del micrófono por parte de la aplicación no se realizaba de manera reiterada, sino en momentos puntuales durante cada uno de los partidos, y que las señales de audio captadas no se recopilaban en ningún servidor sino que se compilaban en algoritmos matemáticos[55] –un funcionamiento similar al de la aplicación de rastreo musical ***Shazam***–.

No obstante, a pesar de esta matización la **AEPD** entendió que el tratamiento no era ilícito por que se hiciera uso del micrófono de los dispositivos, sino porque este tratamiento no se comunicaba de manera correcta a sus usuarios, siendo preciso que cada vez que la aplicación activara dicha función se notificara al usuario de la misma cada vez que se procediese a recopilar esa información, así como de la posibilidad de revocar su consentimiento en cualquier momento (**artículo 7.3** del **RGPD**).

Todo ello desembocó en la imposición de una sanción de 250 mil euros, la cual sigue en proceso de recurso, ya que como responsables del tratamiento (**LaLiga**) entienden que no se cometió ninguna irregularidad en base a la legislación vigente, pues la *app* advertía al usuario en 3 ocasiones –durante el proceso de instalación– sobre la función del micrófono en sus **Condiciones Legales**[56]. Igualmente, **LaLiga** ya comunicó que esta funcionalidad dejaría de estar activa tras acabar la temporada 2018-19.

Dejando a un lado este caso ampliamente mediático, y centrándonos algo más en la escasa jurisprudencia que hay en la actualidad sobre esta materia tan novedosa referida a la monitorización a través del uso de aplicaciones telefónicas, también podemos hacer mención a la **Sentencia de la Audiencia Nacional** de 6 de febrero de 2019, contra **Telepizza** en relación con el proyecto ***Tracker***[57].

---

[55] OTTO, C. <<*Sanción histórica a la LaLiga: 250.000 € por 'espiar' con tu móvil en busca de piratería*>>. *El Confidencial*. 12 junio 2019. Fuente: https://www.elconfidencial.com/tecnologia/2019-06-11/aepd-laliga-app-sancion-multa-proteccion-datos-pirateria_2064138/

[56] MORELL RAMOS, J. <<Si aceptas, la *app* de #*LaLiga* hace uso de tu micro y geolocalización [...]>>. *Twitter*. 10 junio 2018, 11:01: https://twitter.com/Jorge_Morell/status/1005736734255210496

[57] SAN (Sala de lo Social) de 6 de febrero de 2019 (caso 13/2019, Proc. 318/2018), asunto Federación de Servicios de Comisiones Obreras y Federación Estatal de Servicios, Movilidad y Consumo de la Unión General de Trabajadores contra Telepizza, S.A.U, y el Ministerio Fiscal. Fuente: https://www.ccoo-servicios.es/archivos/28079240010000000258201928079240014 12.PDF

Este proyecto se basaba en el desarrollo de una aplicación móvil, la cual se diseñó para tener geolocalizados a sus trabajadores, a través de sus dispositivos móviles personales, mientras realizaban los repartos a domicilio. Al tratarse de una aplicación que el trabajador debía instalar en su propio dispositivo, el responsable del tratamiento estableció un pequeño incremento salarial para dichos empleados de **5'50 euros** mensuales de compensación por el terminal, más unas variables en función de los datos usados (cuya horquilla oscilaba entre **1'40** y **2'90 euros mensuales**, dependiendo si el contrato era de 24 horas mensuales o de jornada completa).

La cuestión que suscitó esta sentencia no fue la finalidad del tratamiento que buscaba dicha aplicación, ya que podría ampararse en el interés legítimo de **Telepizza** que, como responsable del tratamiento, puede buscar una mayor eficacia y mejora en la promoción de sus productos y servicios; sino que esta medida fue establecida por parte de la empresa, imponiendo en el contrato la condición unilateral de que el trabajador debía poner su dispositivo a disposición de la empresa dispositivo móvil con el objetivo de mantenerlos geolocalizados durante sus horas de reparto; estableciendo además un régimen disciplinario distinto para aquellos trabajadores que se mostrasen disconformes con la medida, quedando el mismo al margen del régimen ya establecido en convenio.

Una cuestión que para la Audiencia Nacional sin duda supuso un abuso de derecho por parte de la franquicia en el ejercicio de su potestad organizativa y empresarial, atentando contra la privacidad de los empleados por tratarse de una medida desproporcionada, cuando una opción similar y menos intrusiva hubiera sido establecer un sistema de geolocalización en la flota de vehículos, cuya titularidad pertenece a la empresa.

Igualmente, la sentencia también se pronunció sobre la falta de ética del responsable del tratamiento por ignorar deliberadamente el derecho de información tanto a los trabajadores, ya que no se les proporcionaba una información detallada del sistema ***Tracker*** ni de su mecánica; como a los representantes sindicales (tal como establece el **artículo 64.5** del **Estatuto de los Trabajadores**), motivo por el que tanto Comisiones Obreras como la Unión General de Trabajadores decidieron impugnar esta medida.

En definitiva, estamos siendo testigos de un crecimiento paulatino del uso indiscriminado de aplicaciones para ejercer una labor de monitorización, en ocasiones exhaustiva y que no siempre se corresponde de manera justificada con la finalidad inicialmente perseguida, algo que la normativa debe evitar y por lo que el legislador ha de adaptarse de manera efectiva, dada la velocidad a la que avanzan las nuevas tecnologías.

4.2.3. Deep web, dark web y darknet

Pese a que el acceso a *Internet* es insondable en su extensión, siendo la *web*[58] el medio de acceso habitual para la población mundial a la hora de buscar o divulgar información, sin embargo no es la única modalidad de acceso. Es aquí donde entra en escena un concepto que en los últimos años ha empezado a tener mayor peso en lo que respecta a la privacidad de las personas físicas y que actualmente resulta especialmente complejo delimitar su seguridad o, aún más, regular su uso por parte de la comunidad internauta. Se trata de la ***Deep Web***.

Lo primero que debemos preguntarnos es, ¿*qué es la deep web*? Una forma breve de definirla sería como "*toda aquella información contenida en Internet a la que no podemos acceder públicamente a través de la web*".

Como decimos, se trata de una definición breve, pero no sencilla; y es que si lo que entendemos como *web*[59] puede suponer algo más del 5 por ciento de todo lo que compone *Internet*, la *deep web* vendría a ser ese 95 por ciento restante, el cual se compone de datos a los que no se puede acceder a través de motores de búsqueda convencionales (como ***Google***, ***Yahoo!*** o ***Mozilla***).

Por lo general, este tipo contenido no dejan de ser meras páginas *webs* cuyo acceso queda restringido por proveedores que mediante una subscripción de los titulares de las *webs* quedan protegidas; así como cualquier archivo que tengamos alojado en una nube, los mensajes de nuestras propias cuentas de correos, o incluso aquellas páginas

[58] Abreviación de ***World Wide Web***, que podemos definir como el sistema más usual de acceso a *Internet*, por el cual se transmiten multitud de tipos de datos a través del **Protocolo de Transferencia de Hipertextos** (o **HTTP**), que conforman los enlaces que nos dirigen a una determinada página *web*.

[59] También denominada '***Clearnet***' o '***Surface Web***', que vendría a ser la idea que todo el mundo tiene de lo que es Internet en sí, a cuyo contenido puede tener acceso la comunidad a través de cualquier navegador habitual.

que creamos de manera temporal cuando consultamos nuestra banca *online*, realizamos una compra por ***Amazon*** o bien cuando reservamos una plaza en cualquier buscador de vuelos.

A su vez, dentro de la *deep web* encontramos una fracción que queda velada deliberadamente para los motores de búsqueda, la cual se conoce como ***Dark Web***. Si hemos enunciado que la *deep web* supone el 95 por ciento de todo lo que abarca realmente *Internet*, la *dark web* abarca apenas un 0'1 por ciento de la anterior.

Esta parte más reducida se caracteriza por su contenido no indexable; es decir, la información contenida en ella se mantiene en direcciones IP encriptadas y con dominios propios, por lo que únicamente se pueden acceder a estas mediante navegadores especialmente diseñados para su búsqueda denominados ***darknets*** (como por ejemplo ***TOR***, uno de los navegadores más conocidos para sumergirse en la *dark web*, cuyo dominio es ***.onion***).

Como decíamos inicialmente, el concepto de la *deep web* ha ido adquiriendo en los últimos años una mayor relevancia en lo tocante a la privacidad de los usuarios, pues se trata de un espacio donde el internauta puede moverse con una mayor libertad, puesto que el cifrado de sus comunicaciones hace su rastreo resulte más complejo para terceros –lo cual no quiere decir que sea imposible–, lo que podría crear en el usuario medio una cierta expectativa razonable de anonimato.

No obstante, este concepto también se ha ido percibiendo con ciertas connotaciones negativas, en gran parte debido al supuesto uso que se la ha dado a esta zona tan difusa de la *web*. No es raro asociar esta parcela de *Internet* con actos ilícitos, tales como la venta ilegal de armas y sustancias estupefacientes, el tráfico de *bitcoins*, la pornografía infantil, la posibilidad de ser víctimas de un *ransomware*, la contratación de asesinos a sueldo, o la supuesta existencia de ***red rooms***[60], etc.

Al margen de que algunos de estos ilícitos puedan ser verídicos en mayor o menor medida, no dejan de ser actos que hemos podido encontrarlos incluso en páginas o

[60] COX, J. <<*The 'real' dark web doesn't exist*>>. *Vice*. 31 agosto 2015. Fuente: https://www.vice.com/en_us/article/vvbw8b/the-real-dark-web-doesnt-exist. Las ***red rooms*** o habitaciones rojas son páginas donde presuntamente se pueden ver, o incluso participar en streaming en la tortura o el asesinato de personas, algo que posteriormente se acabó desmintiendo. No obstante, se trata de una leyenda urbana que se ha consolidado en el imaginario de la comunidad internauta.

redes sociales convencionales, como fue el caso de los atentados que tuvieron lugar en la localidad neozelandesa de *Christchurch* en marzo de 2019 y que fue retransmitido en directo en ***Facebook*** por el propio terrorista[61].

A pesar de toda esta faceta negativa, el uso de la dark web también puede suponer un medio alternativo para muchos ***hacktivistas*** –esto es, *hackers* que llevan a cabo acciones con una finalidad política, generalmente relacionada con las protestas a favor de los DDHH– a la hora de transmitir cierto contenido de carácter divulgativo, debido a la dificultad que implica acceder a determinada información en algunos países con políticas muy restrictivas en cuanto a las libertades de los usuarios, como puede ser el caso de China, Emiratos Árabes, Irán o Rusia.

Sin embargo, el empleo de esta herramienta con motivos políticos no solo se da en regímenes autoritarios, también puede darse en naciones democráticas, tal como ocurrió en 2013 cuando **Edward Snowden** llevó a cabo las revelaciones sobre la red de vigilancia mundial entre varias agencias de inteligencia internacionales[62].

Anteriormente hemos hecho mención a la expectativa razonable de anonimato que puede asumir un usuario al navegar en la *deep web*, dado que las páginas que albergan esta parte de *Internet* se encuentran reforzadas con direcciones IP encriptadas. Ciertamente, esta situación eleva la dificultad del rastreo de determinadas actividades, pero esto no implica que no sea posible monitorizar a los cibernautas en este terreno, y mucho menos cuando se trata de investigar actos ilícitos.

[61] PONS, P. <<*Facebook restringe las retransmisiones en directo tras la matanza de Nueva Zelanda*>>. *La Vanguardia*. 15 mayo 2019. Fuente: https://www.lavanguardia.com/tecnologia/20190515/462263858254/facebook-restringe-retransmissiones-directo-live-matanza-nueva-zelanda-redes-sociales-tecnologia-portada.html. El 15 de marzo de 2019 un individuo produjo un tiroteo masivo en dos mezquitas de la ciudad de *Christchurch*, siendo su objetivo civiles musulmanes, dejando un recuento de medio centenar de víctimas mortales. Su retransmisión en directo por ***Facebook*** llevó a que la propia red social restringiese su cobertura, además de invertir en mejores medios para la detección y análisis de imágenes y vídeos. Para mayor información sobre este suceso adjunto un enlace con un artículo del diario **La Vanguardia** sobre dicha decisión:

[62] MACASKILL, E., DANCE, G. <<*NSA Files Decoded: Edward Snowden's surveillance revelations explained*>>. *The Guardian*. 1 noviembre 2013. Fuente: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded. El diario británico ***The Guardian*** elaboró un exhaustivo artículo con algunos de los documentos clasificados de la **NSA** (la **Agencia de Seguridad Nacional de los Estados Unidos de América**).

En España contamos con grupos de operaciones dedicados a la persecución delitos informáticos, integrados por especialistas de la Guardia Civil (denominado como **Grupo de Delitos Telemáticos**) así como por la Policía Nacional (la **Brigada de Investigación Tecnológica**) que realmente tienen cierta presencia en páginas y foros ubicados en la *deep web*, buscando constantemente indicios de toda clase actos ilícitos, como los ya mencionados. A pesar de la encomiable labor de las Fuerzas y Cuerpos de Seguridad del Estado y de sus esfuerzos por tratar de monitorizar estas redes en la inmensidad de *Internet*, lo cierto es que las autoridades policiales siguen sin contar con los medios necesarios para actuar con plena eficacia en esta área.

A todo esto cabe añadir la escasa jurisprudencia con la que contamos en materia de delitos informáticos a través de la *deep web*, aunque los pocos resultados que podemos encontrar son bastante significativos: delitos relativos a estafas[63] y falsificación de documentos oficiales, al tráfico de drogas[64] y otras sustancias estupefacientes, así como a la difusión de material pornográfico infantil[65].

Todas estas sentencias coinciden en el hecho de que ninguna hace referencia a la labor concreta que las autoridades realizaban a través de la *dark web*, ya que para la obtención de indicios en estos actos se hizo necesario recurrir a medios de carácter

[63] SAP (Madrid), de 23 de mayo de 2017 (núm. 321/2017, Proc. 6587/2017), por la que una mujer de nacionalidad rumana fue condenada por estafa y falsedad en documento oficial, puesto que su actividad consistía en la sustracción de datos numéricos y códigos de verificación procedentes de tarjetas del *Royal Bank of Scottland*, cuyos titulares eran todos de nacionalidad irlandesa. Se trata de una práctica habitual entre *hackers* en la *dark web*; no obstante, la investigación pudo llevarse a cabo a través de la colaboración de las entidades gestoras de pagos, ***Redsys*** y ***Ceca***, que efectuaron el pago de las compras fraudulentas. Fuente: **CENDOJ** (http://www.poderjudicial.es/search/indexAN.jsp#).

[64] SAP (Santa Cruz de Tenerife), de 3 de octubre de 2018 (núm. 294/2018, Proc. 1900/2018), donde un individuo resulto condenado por un delito contra la salud pública, al adquirir sustancias estupefacientes a través de la *dark web* y realizando su compra mediante *bitcoins*. A pesar de que no puede rastrearse la dirección IP de los usuarios al usar buscadores *darknet* como ***TOR***, las autoridades policiales pudieron seguir el rastro a través de los mensajes intercambiados entre las partes implicadas en dicha red. Fuente: **CENDOJ** (http://www.poderjudicial.es/search/indexAN.jsp#).

[65] STS (Sala de lo Penal), de 19 de diciembre de 2018 (núm. 667/2018, Proc. 4554/2018), sentencia en la que un individuo fue condenado como autor de un delito de distribución de pornografía, que entre 2011 y 2014 llegó a ser coadministrador de varios foros de la dark web dedicados a la producción y distribución de pornografía infantil, obteniendo con su detención materiales informáticos con información relevante sobre enlaces a páginas ilegales, contactos con pedófilos y productores de material pornográfico infantil, así como innumerables carpetas con millones de archivos de este tipo. Hay que advertir que esta sentencia surge en el marco de una investigación internacional coordinada entre el **FBI** y la **EUROPOL** (**Operación *Downfall* 2**), la cual se realizó mediante el uso de darknets, y de la que llegó a obtenerse una dirección IP, procedente del condenado de dicha sentencia. Fuente: **CENDOJ** (http://www.poderjudicial.es/search/indexAN.jsp#).

analógico (como el rastreo de direcciones IP a través de la navegación en *webs* convencionales, etc.).

No obstante, todas comparten una causa común: el error humano. Y es que en muchas ocasiones, sus infractores suelen ser descubiertos por no tomar las cautelas necesarias en estas redes, o bien por no poseer los conocimientos necesarios sobre su funcionamiento.

Si a ello le sumamos que incluso es posible encontrar defectos en las *darknets* que causen una brecha en su seguridad, bien por fallos de encriptación en su aplicación, o bien por la creación de puertas traseras en los mismos navegadores por parte de sus desarrolladores con las que se permita a las autoridades policiales establecer un cierto control[66], esto podría poner en entredicho la expectativa razonable de anonimato que ofrece la *dark web* para los internautas más incautos al demostrar las vulnerabilidades con las que cuenta la red en sí, pero sobre todo por el desconocimiento de muchos usuarios, factores que pueden ayudar a las autoridades a llevar a cabo este tipo de operaciones.

Por todo lo expuesto, queda demostrado que incluso en los rincones más ocultos de *Internet* pueden encontrarse errores en su arquitectura que permitan a las autoridades competentes realizar una mejor actividad de monitorización sobre determinados contenidos[67], a pesar de todas las implicaciones negativas que puedan recaer sobre el derecho a la privacidad de los usuarios sobre sus comunicaciones en el entorno digital.

---

[66] EDWARDS, A. <<*FBI bids to extradite Irishman, 28, on suspicion of being 'largest child-porn dealer on planet'*>>. *Daily Mail Online*. 5 agosto 2013. Fuente: https://www.dailymail.co.uk/news/article-2384773/Eric-Eoin-Marques-largest-child-porn-dealer-planet-extradited-FBI.html. A mediados de 2013, se descubrió que el dominio ya inactivo ***Freedom Hosting***, debido a determinadas vulnerabilidades en sus sistemas, quedó comprometido. Esto permitió al FBI introducir un código en el navegador *darknet* **TOR *Browser Bundle*** para localizar la dirección IP del usuario responsable del dominio anteriormente mencionado, el cual también era sospechoso de distribuir pornografía infantil. Este hecho hizo que la comunidad internauta comenzase a cuestionarse hasta qué punto podía quedar garantizado su anonimato en la *deep web*.

[67] VERDÚ, D. <<*Golpe a la delincuencia de la Deep Web*>>. *El País*. 12 noviembre 2014. Fuente: https://elpais.com/politica/2014/11/12/actualidad/1415794086_687302.html. En 2014, la **Europol** en coordinación con varias autoridades internacionales (entre ellas, el **Grupo de Delitos Telemáticos** de la Guardia Civil) llevaron a cabo la operación ***Onymous***, dedicada a combatir el tráfico de drogas y la falsificación de documentos oficiales a través de la *dark web*, llegando a cerrar más de 400 dominios donde se desarrollaban estas actividades ilícitas. En relación con dicha operación, adjunto un artículo del diario **El País**, que desarrolla como se llevó a cabo la operación.

Por ello, es necesario que la comunidad internauta comprendan el funcionamiento de estas redes, haciendo de las mismas un uso más responsable.

4.2.4. Plataformas streaming

Para finalizar con este apartado, vamos a hacer referencia a un sector que en los últimos 4 años ha tenido un mayor impacto en la comunidad digital y en el modo de entender la cultura del consumismo.

Hablamos de la reproducción de contenidos audiovisuales por *streaming*; esto es, la posibilidad de consumir películas, documentales, series o cualquier otro producto similar desde nuestros *smart TV's*, ordenadores o dispositivo móvil a través de su conexión a *Internet*.

Se trata de una tecnología que nos ha facilitado la posibilidad de acceder a este tipo de contenido a nuestra libre elección a través de proveedores que, mediante una suscripción monetaria (ya sea mensual o anual), nos ofrecen este servicio a la carta y poniendo a disposición del consumidor un repertorio casi ilimitado de material audiovisual, ahorrándonos la publicidad comercial de la televisión convencional y dándonos el control de lo que queramos ver y cuando lo queramos ver.

Pero, ¿*qué tiene que ver esta tecnología con la monitorización de los usuarios*? ¿*Y en qué medida afecta a la privacidad de las personas*? A primera vista, podría decirse que no existe una relación entre la posibilidad de ver películas o series y que estas nos condicionen personalmente. No obstante, la cuestión pendula en torno a los resultados que pueden arrojar las reproducciones de determinados contenidos según un cierto tipo de usuario.

En la actualidad existen multitud de proveedores de contenido audiovisual en streaming, siendo los más populares a nivel global ***Netflix***, **HBO**, ***Hulu*** o ***Amazon Prime Video***, mientras que en España también contamos con entidades como ***Filmin*** o ***Movistar+***. Pero en este caso nos detendremos en el gigante americano ***Netflix***, una empresa que inició su andadura mediante el alquiler de DVD por correo postal y acabó consolidándose como uno de los gigantes de los servicios en *streaming*.

Lo que nos interesa de este servicio es que permite que una misma cuenta pueda editar más de un perfil, de manera que esa misma cuenta pueda ser compartida por

varias personas. Esto posibilita a ***Netflix*** obtener datos de una mayor cantidad de usuarios, amplificando de esta manera el desarrollo de su algoritmo.

La mecánica de este algoritmo se basa en las reproducciones que cada perfil realiza sobre el catálogo del servicio, analizando la película o serie que ve, su género, su año de estreno, los interpretes que figuran o el director que la realiza, la fecha y hora en que se ha reproducido, etc. Todos estos factores permiten que algoritmo conozca con mayor precisión nuestros gustos, algo que posteriormente se materializa con mediante pequeños detalles en la interfaz de la aplicación, siempre en función de la afinidad con cada usuario: por ello, si ***Netflix*** percibe que lo que más consumimos son thrillers, será este tipo de género el que figure sobre todo entre nuestras sugerencias y que los fotogramas de las series o películas sean más oscuras y apagadas; si por el contrario, consumimos más comedias, las sugerencias aparecerán con imágenes más desenfadas.

Explicado así, está claro que esto no es nada nuevo, pues a fin de cuentas no deja de ser una empresa que busca su máximo beneficio, pero si tomamos conciencia de que se trata de un algoritmo que se centra siempre en la experiencia individual de cada consumidor[68], y que este se aplica sobre cada perfil que forma parte de una cuenta, entonces podemos hacernos una idea de cuantísima información recopilan de nosotros, generando *big data* constantemente gracias a los metadatos que va almacenando sobre cada usuario.

Se trata de un sistema que aprende a partir de la experiencia del usuario[69], lo que sigue demostrando que los medios tecnológicos avanzan exponencialmente. Sin embargo, este avance también puede llevar aparejado otros riesgos que afecten de

[68] IZQUIERDO, A. <<*2.000 comunidades de gustos y 27.000 micro-géneros, la base del sistema de recomendación de Netflix*>>. *Xataka*. 31 enero 2019 (actualizado 16 febrero 2019). Fuente: https://www.xataka.com/streaming/2000-comunidades-gustos-27000-micro-generos-base-sistema-recomendacion-netflix

[69] CASTILLO, C. DEL <<*La paradoja de Black Mirror: Netflix guarda tus datos sobre qué elegiste en cada opción de su último capítulo interactivo*>>. *El Diario*. 13 febrero 2019. Fuente: https://www.eldiario.es/tecnologia/paradoja-Black-Mirror-Netflix-Bandersnatch_0_867563950.html.
Uno de los últimos eventos más recientes que volvió a poner en el centro del debate la importancia de los datos personales para la multinacional ***Netflix*** fue el estreno de ***Bandersnatch***, un episodio especial de la serie británica '***Black Mirror***', en el cual era el usuario el que decidía que acciones iba a llevar a cabo el protagonista, como si de un libro de '*Elige tu propia aventura*' se tratase. Estas decisiones se almacenan y pasan a formar parte de la base de datos de la entidad. No obstante, la propia entidad acabó aclarando que estos datos quedan disasociados en el proceso, por lo que no tendrían la consideración de carácter personal, lo cual les permite explotarlos como mejor consideren, por ejemplo vendiéndolos.

una u otra manera a distintas facetas personales, como podría ser la relativa a la salud física[70].

No obstante, quizás el problema no sea tanto que este tipo de tecnologías tan intrusivas puedan suponer un riesgo para nuestra privacidad, sino que en caso de que así fuera, *¿habría consecuencias significativas*? *¿Y qué perjuicios podría causar si llegasen a materializarse tales riesgos*? Es por esto por lo que el plano legislativo debe tratar de adecuarse a los acontecimientos tecnológicos que se van desarrollando con el paso del tiempo.

5. Consideraciones legales

5.1. Incidencia en la privacidad y vulneración de la intimidad

En este punto sería conveniente preguntarnos, *¿es consciente la sociedad de la creciente importancia que se le está otorgando a sus datos personales con el auge tecnológico que estamos viviendo*?

En las dos últimas décadas *Internet* se ha consolidado como el medio de comunicación principal entre las personas, la herramienta de búsqueda idónea que nos permite encontrar cualquier producto, cualquier contenido, en definitiva cualquier tipo de información a golpe de *clic*. Hemos sido testigos de un avance tecnológico que ha traído consigo grandes beneficios para la comunidad: comunicarnos en cuestión de segundas con cualquier persona al otro lado del planeta, automatizar determinadas tareas domésticas –lo que a efectos de ahorro económico ha supuesto un logro–, abrir la puerta a la cultura de una manera exponencial, etc.

No obstante, este desarrollo digital también ha dado lugar a determinados riesgos en lo relativo a la privacidad de las personas, tanto en aquellos aspectos más habituales que pueden darse en nuestro día a día, o en el marco de una relación laboral (medios de geolocalización, monitorización, videovigilancia, etc.), como por las consecuencias

[70] MEHTA, I. <<*Netflix tests tracking your 'physical activity' to improve video quality*>>. *The Next Web*. 31 julio 2019. Fuente: https://thenextweb.com/apps/2019/07/31/netflix-is-testing-changing-playback-quality-based-on-your-physical-activity/. Recientemente, un usuario de Twitter experto en seguridad descubrió que la *app* móvil de ***Netflix*** le solicitaba permiso para acceder otras aplicaciones que median su actividad física.

que, debido al empleo de estas nuevas tecnologías, pueden entrañar para nuestra salud (problemas de ansiedad, depresiones, aislamiento social, etc.).

En definitiva, después de analizar todos estos medios y técnicas que tanto organizaciones como autoridades tienen a su disposición para captar información, es difícil no tener la sensación de encontrarnos constantemente en un proceso de monitorización, y sin embargo no ser plenamente conscientes de esta **vigilancia digital**, indistintamente de que su ejecución pueda suponer un beneficio o un perjuicio sobre nuestras libertades y derechos más fundamentales, según el caso.

Pero a pesar de todo ello, *¿debería permitirse esta forma de control*? Ante todo es conveniente tratar de apagar los fuegos que estas conspiraciones *orwellianas* puedan causar; hay que ser conscientes de que el Estado, en la medida que a este le compete, tienen el deber de hacer uso de estas tecnologías para la observancia del bien común. Lamentablemente, vivimos tiempos donde la seguridad se ha vuelto un pilar básico de la sociedad, y la lucha contra el crimen y el terrorismo en entornos digitales es una cuestión de primer orden en toda agenda gubernamental. Tal y como explicamos en páginas anteriores[71], se tratan de medidas que la comunidad asumimos como necesarias, un precio que debemos estar dispuestos a pagar por vivir en una sociedad civilizada.

En cuanto a la adopción de este tipo de actuaciones por entidades y organizaciones privadas, la cuestión puede tornarse controvertida. Hemos visto que no son pocos los casos en que grandes empresas hacen uso de distintos sistemas de vigilancia y rastreo, tanto sobre sus empleados como sobre los consumidores de sus productos o servicios. Podemos entender que se tratan de contextos que obedecen a distintos causas legitimadoras: la necesidad de cumplir con una obligación adoptada por las dos partes en el marco de una relación contractual, llevar a cabo una misión realizada en pos del interés público que haya sido otorgada al responsable del tratamiento (como los sistemas de cámaras de Londres[72] o el proyecto ***Skynet*** desarrollado por China[73]), o

[71] En relación con los atentados terroristas perpetrados en las ciudades de Barcelona (páginas 39 y 40) y *Christchurch* (página 51).

[72] LESSIG, L. *El Código 2.0*. 1ª ed. Madrid: Traficantes de Sueños, 2009, pg. 335. Inicialmente, las autoridades londinenses idearon este sistema para regular el tráfico de la ciudad y controlar que los no residentes que circulasen por las zonas más céntricas pagasen su correspondiente impuesto. Se trata de un sistema que acabó convirtiéndose en una base de datos que contenía información sobre todos los

simplemente la satisfacción del interés legítimo que motiva al responsable a llevar a cabo dicho tratamiento.

Todas estas circunstancias pueden dar lugar, en mayor o menor medida, a la legitimación del tratamiento, tal como establece el **artículo 6** del **RGPD**, siempre que cumpla con determinados requisitos. A fin de cuentas, cuando decidimos contratar la instalación de un sistema de alarma o videovigilancia, cuando queremos crearnos una cuenta en una red social o cuando instalamos una *app* que registre nuestra frecuencia cardiaca, horas de sueño y/o kilómetros recorridos, estamos aceptando implícitamente las **Condiciones Generales de Uso** para el tratamiento que va a llevar a cabo el responsable, puesto que en caso de no aceptarlas sería técnicamente imposible que pudiera realizarse la prestación del servicio.

De este modo, es importante que a la hora de aceptar dichas condiciones el responsable cumpla con el **deber de información** (**artículos 12** a **14** del **RGPD**), es decir, debe informar al usuario de todos aquellos aspectos relativos al tratamiento y que vayan a incidir sobre sus datos de carácter personal de manera concisa, inteligible, transparente y en un lenguaje claro y sencillo, de manera que el interesado posteriormente pueda conceder un consentimiento informado mediante un acto afirmativo, del cual se desprenda una voluntad claramente "*libre, específica e inequívoca*" por el que acepte el tratamiento (**considerando 32** del **RGPD**).

Ahora bien, distinto sería que esta facultad de monitorización asumida por el responsable acabase usándose a la postre de una manera indiscriminada sobre todo aquel afectado por el tratamiento, o incluso sobre toda la población global, algo que sin duda no pasó inadvertido para la opinión pública tras la filtración de **Edward**

---

coches de la ciudad con una indicación expresa de la hora y el lugar concreto de la circulación de los mismos.

[73] ÁLVAREZ, R. <<*20 millones de cámaras equipadas con inteligencia artificial hacen que China sea el verdadero Gran Hermano*>>. *Xataka*. 26 septiembre 2017 (actualizado 9 febrero 2018). Fuente: https://www.xataka.com/privacidad/20-millones-de-camaras-equipadas-con-inteligencia-artificial-hacen-que-china-sea-el-verdadero-gran-hermano. Se trata de un proyecto masivo desarrollado por las autoridades policiales chinas a principios de 2015 con el objetivo de aumentar la seguridad de la nación. Este sistema queda compuesto por más de 20 millones de cámaras instaladas a lo largo de todo el país, y además de monitorizar las zonas públicas, también cuentan con un *software* que emplea un sistema de **inteligencia artificial** por el que es capaz de emplear técnicas de reconocimiento facial. Además, resulta anecdótico el nombre que le dieron al proyecto, ya que ***Skynet*** también fue el nombre que se le dio a la entidad ficticia de la saga fílmica ***Terminator***, una inteligencia artificial que se sublevó contra los seres humanos.

Snowden sobre la red de vigilancia mundial que llevaron a cabo varias agencias de inteligencia internacionales[74].

Por ello, es conveniente saber delimitar aquella parcela personal de cada individuo donde no se vea expuesto a cualquier injerencia por parte del Estado o terceras entidades, realizar un triple juicio ponderado de **idoneidad** –que la medida pueda conseguir el propósito que se persigue–, **necesidad** –que el objetivo del tratamiento no pueda alcanzarse mediante una medida menos intrusiva– y de **proporcionalidad** –que la medida elegida sea equilibrada y si de esta pudieran más beneficios para el interés común que perjuicios sobre los valores que entran en conflicto con el tratamiento–. Y es que no debemos olvidar que infringir una expectativa razonable de privacidad, siempre que esta fuera plenamente legítima y razonable, podría suponer un quebranto sobre el derecho fundamental de las personas físicas a la protección de sus datos.

5.2. Identidad digital.

S i hay algo que busca promover el nuevo **Reglamento General de Protección de Datos** es velar por el derecho a la privacidad de las personas físicas, garantizando el ejercicio de sus derechos y libertades.

No obstante, en lo que respecta a la actividad de la comunidad en los entornos digitales, somos consciente de que no hay nada que escape a *Internet*, es el ojo que todo lo ve. Tanto los motores de búsqueda como las redes sociales almacenan todo tipo de información sobre cada uno de nuestros actos (fotos, mensajes, aficiones o preferencias, etc.), por lo que muchos usuarios hemos asumido que no contamos con una noción de privacidad en sentido estricto en la red.

Tanto los organismos públicos como las organizaciones privadas hacen uso de las nuevas tecnologías para tener un mayor conocimiento de las actividades que llevamos a cabo en nuestro día a día, ya sea para analizar nuestros perfiles ideológicos o políticos para así captar o modificar nuestra intención de voto, o para recoger datos

[74] Sobre este apartado ya hablamos anteriormente en la página 51, por lo que nos remitiremos a la misma.

sobre nuestras aficiones personales con el objetivo de ofrecernos productos o servicios que se adecuen a los usuarios en función de sus intereses.

Por todo esto, es importante analizar si la **dirección IP** debe tener la consideración de dato personal. Se trata de un código hexadecimal compuesto por una serie de dígitos numéricos que se asigna a cada dispositivo tecnológico que tenga la posibilidad de acceder a *Internet* (como puede ser un ordenador o un *smartphone*), es un elemento que sirve para identificar la identidad de nuestro dispositivo en la red.

Con esta definición, podría decirse que tal dato numérico no identifica expresamente a la persona que está navegando por la red, o que al menos no hace plenamente identificable al usuario que se encuentra tras esta dirección.

No obstante, si nos paramos a examinar el primer enunciado del **artículo 4** del **RGPD**, de este podemos extraer que "*se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea* [...]", lo que da peso a la teoría de que ese código numérico que se le asigna a un dispositivo podría facilitar a su vez la identidad del usuario en cuestión.

A pesar de ello, en la práctica son muchas las compañías prestadoras de servicios de red *online* las que aseguran que ese proceso de identificación requiere de medios muy específicos y costosos, además de que no serían suficientes para identificar completamente a los usuarios por sus datos identificativos más básicos, como serían el nombre y los apellidos.

Aun así, en los últimos años tanto la jurisprudencia nacional como internacional se ha pronunciado respecto a este asunto, posicionándose en todo caso con lo expuesto por el vigente **Reglamento Europeo**, siguiendo así mismo el criterio que fundamentó la **AEPD** en su **Informe jurídico 327/2003**[75], donde entiende que "*aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red*" sí que podría identificarse a un usuario desde el momento en que

[75] Informe jurídico 327/2003, sobre la consideración de "*carácter de dato personal de la dirección IP*": https://www.aepd.es/informes/historicos/2003-0327.pdf

éste inicie sesión (también denominado ***log-in***) a través de un navegador en cualquier página donde tenga una cuenta personal.

Ese dato tendrá la consideración de carácter personal, pudiendo el proveedor de servicios de *Internet* (Orange o Vodafone, por ejemplo) "*identificar al usuario con el que tiene un contrato de acceso a Internet*" a través de su dirección IP; y a partir de la captación de este elemento se podrían relacionar con "*otros datos de carácter personal* [...] *que permitan identificarlo, especialmente si se utilizan medios* [...] *para recoger información adicional sobre el usuario, tales como cookies con un identificador único* [...] *que permite su identificación*".

Junto al criterio de la autoridad de control nacional, decíamos que también la jurisprudencia se ha posicionado sobre esta cuestión. La Sala de lo Contencioso del Tribunal Supremo concretó en su Sentencia de 3 de octubre de 2014[76] que la dirección IP de un dispositivo electrónico debe ser reconocida como dato personal (**fundamento Jurídico cuarto**), puesto que a partir de la misma los proveedores pueden identificar –bien directamente o de manera indirecta– la identidad de un usuario determinado. Por lo que en este tipo de supuestos, sería necesario que el responsable del tratamiento obtenga el consentimiento del usuario que sea titular o propietario de este código para proceder a su tratamiento.

En cuanto a la jurisprudencia internacional, el Tribunal de Justicia de la Unión Europea también encontró acomodo en esta perspectiva con su Sentencia de 19 de octubre de 2016[77] (**incisos 47** y **49**, **primera cuestión prejudicial**), pues entiende que "*una*

[76] STS (Sala de lo Contencioso) de 3 de octubre de 2014 (núm. 3896/2014, Proc. 6153/2011), por la que la organización de Productores de Música de España (*Promusicae*) interpuso recurso de casación contra la Resolución del Director de la AEPD, dictada a 2 de julio de 2009, por la que se negaba a dicha organización la exención del deber de informar a los usuarios de redes **P2P** sobre el tratamiento de sus datos, en defensa de los derechos de propiedad intelectual de sus productores y editores. Fuente: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=7195354&links=&optimize=20141023&publicinterface=true. Se trata de una resolución estrechamente vinculada a la STJUE Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 29 de enero de 2008 (Asunto C-275/06), ya mencionada anteriormente, en la página 12.

[77] STJUE (Sala Segunda) de 19 de octubre de 2016 (C-582/14), en la que el Sr. Patrick Beyer solicitaba la prohibición de que la República Federal de Alemania conservase su dirección IP con motivo de una serie consultas en varios sitios *web* de acceso público, ya que este tipo de información tiene la consideración de dato personal, y su recogida y utilización solo está autorizada (según el derecho alemán) a efectos de facturación. Fuente: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=1314731

dirección IP dinámica registrada por un proveedor [...] *con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye* [...] *un dato personal* [...] *cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona*".

De esta manera, la jurisprudencia confirma que los proveedores de servicios de red en línea pueden contar con los medios necesarios para "*identificar, con ayuda de otras personas, a saber, la autoridad competente* [...] *al interesado sobre la base de las direcciones IP conservadas*" por los cauces que la Ley establece, tal como ocurren en el caso de España.

No obstante, nuestra normativa también establece que estos proveedores podrán conservar determinadas categorías de datos (como aquellos relativos a la conexión y desconexión de los usuarios) durante "*un máximo de 2 años o un mínimo de 6 meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos* [...]"[78].

Por tanto, llegados los casos y según las circunstancias que se den, es posible llegar a considerar la dirección IP de un dispositivo electrónico con capacidad para acceder a la red como un dato de carácter personal, en tanto que haya posibilidad de asociarla a otros datos que puedan identificar o hagan plenamente identificable a un usuario, siempre que el responsable del tratamiento lo haga por las vías que establece la normativa a tal efecto, recabando previamente el consentimiento del titular de los datos que va tratar; ya que en caso contrario, se vería en la situación de afrontar elevadas sanciones por no respetar los derechos fundamentales de los afectados, especialmente si esos datos van a ser usados para tratamientos masivos o su uso sea destinado a la elaboración de perfiles por medios automatizados.

Igualmente, tampoco hay que olvidar que la nueva normativa en protección de datos recoge una serie de derechos adaptados a la sociedad digital, garantizando el acceso universal de los mismos a *Internet*, a la posibilidad de ejercer nuestro derecho al olvido tanto en motores de búsqueda como en redes sociales, a la educación y la seguridad a

[78] **Artículo 5.1** de la **Ley 25/2007**, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Fuente: https://www.boe.es/buscar/pdf/2007/BOE-A-2007-18243-consolidado.pdf

través de medios digitales, especialmente cuando se trata de velar por sujetos susceptibles de una mayor protección como son los menores de edad, entre otros.

Incluso se hace expresa referencia a derechos concernientes a las personas físicas en el desarrollo de sus funciones dentro del ámbito laboral, entre los que destacan: la **desconexión digital** del trabajador en lo que se refiere a sus funciones puramente profesionales en los tiempos de descanso y/o vacaciones; o la garantía de que su intimidad quedará preservada, especialmente frente a tratamientos de videovigilancia, grabaciones o sistemas de geolocalización en el lugar de trabajo.

Aun así, es cuestión de tiempo que este catálogo de derechos se vaya ampliando, no tanto en el sentido de crear nuevos derechos, sino por dotarlos de un sentido que se amolde a las necesidades que la sociedad va adquiriendo a través del uso de las nuevas tecnologías.

V. CONCLUSIONES

A raíz de lo expuesto, es importante remarcar que necesitamos políticas públicas que protejan a los ciudadanos de cualquier tratamiento abusivo sobre aquellos datos que les conciernan, garantizando así el derecho fundamental a mantener parte de su vida en privado, fuera del alcance de terceras personas o entidades ajenas a su esfera más íntima y personal.

Llegados a este punto, ¿*cabría plantearse en ese tipo situaciones cualquier juicio de proporcionalidad entre la finalidad que pueda perseguir un responsable del tratamiento y los medios empleados por el mismos, si estos se superponen a la privacidad de las personas*? Como hemos visto, a pesar de que en la mayoría de tratamientos, estos se suelen realizar mediante técnicas de seudonimización que de por sí pueden preservar nuestra identidad y nuestros datos personales, el mero hecho de que estos tratamientos se realicen en entornos digitales ya lleva aparejado a su vez el riesgo a que los mismos puedan verse afectados por actos ilícitos, pues el empleo de los mismos en las manos equivocadas pueden acabar repercutiendo sobre los afectados de manera significativa.

Por ello es crucial que los internautas sean conscientes del grado de responsabilidad que conlleva su actuación en *Internet* –tanto en su superficialidad como en los niveles más profundos de la red–, evitando cualquier mal uso o abuso sobre las mismas, puesto que una mala actuación podría inferir de manera perjudicial sobre los derechos y las libertades del resto de la comunidad.

En definitiva, tras la investigación realizada, hemos demostrado que aunque no contemos con una extensa jurisprudencia en esta materia tan novedosa como es la relativa al **Derecho Digital**, tampoco podemos negar la evidencia de que en los últimos años hemos comenzado a asentar los cimientos necesarios que ayuden a vertebrar eficientemente la regulación de la sociedad digital.

Además, poco a poco, las autoridades de control han ido aportando material de verdadero valor para el ámbito legislativo mediante innumerables resoluciones, informes jurídicos y guías de uso sobre diversas materias respecto a numerosas cuestiones: sobre el uso de las *cookies*, si los *pixeles* y balizas *web* pueden equipararse

a las primeras[79]; la consideración de dato personal en relación con la dirección IP de un dispositivo electrónico, etc. Una labor que actualmente siguen desarrollando, a pesar de contar con pocos medios para el desarrollo de sus funciones y con un cuerpo en cierta medida escaso[80].

Espero que con este trabajo de investigación haya conseguido arrojar algo de luz sobre unas cuestiones que en los últimos tiempos ha suscitado cierta inquietud tanto para los usuarios que forman parte de esta comunidad como para los organismos públicos encargados su salvaguarda, y que también ha supuesto grandes quebraderos de cabeza para otras entidades (públicas y privadas). Igualmente, confío en haber aportado un punto de vista pragmáticamente jurídico, y que este ayude en mayor o menor medida a discernir que la legislación y la tecnología pueden y deben estar obligadas a entenderse en esta nueva sociedad.

Siempre se ha dicho que el derecho es cambiante en consonancia con la historia, su sociedad y los acontecimientos que se desprenden de cada época; y el avance que se ha configurado en los últimos años, tanto a nivel social como tecnológico así lo demuestra.

[79] Fuente: https://www.aepd.es/resoluciones/PS-00371-2016_REC.pdf

[80] ROMERO, P. <<*Reglamento Europeo – Mar España, directora de Protección de Datos: Las pymes me tienen preocupada*>>. *Diario El Público*. 20 de mayo de 2018. Fuente: https://www.publico.es/sociedad/reglamento-europeo-mar-espana-directora-proteccion-datos-pymes-me-preocupada.html

VI. BIBLIOGRAFÍA

- ALDEA, M. <<*e-Privacy*: La UE propone normas más estrictas para las comunicaciones electrónicas>>. *Écija Blog*. 18 enero 2017. Disponible en: https://ecija.com/e-privacy-la-ue-propone-normas-mas-estrictas-las-comunicaciones-electronicas/
- ALONSO, R. <<*Twitter* ha estado usando datos de sus usuarios para publicidad sin tener permiso>>. *ABC Redes*. 8 agosto 2019. Disponible en: https://www.abc.es/tecnologia/redes/abci-twitter-estado-usando-datos-usuarios-para-publicidad-sin-tener-permiso-201908080938_noticia.html
- ÁLVAREZ, R. <<20 millones de cámaras equipadas con inteligencia artificial hacen que China sea el verdadero Gran Hermano>>. *Xataka*. 26 septiembre 2017 (actualizado 9 febrero 2018). Disponible en: https://www.xataka.com/privacidad/20-millones-de-camaras-equipadas-con-inteligencia-artificial-hacen-que-china-sea-el-verdadero-gran-hermano
- CADWALLADR, C. <<'I made *Steve Bannon's* psychological warfare tool': meet the data war whistleblower>>. *The Guardian*. 17 marzo 2018. Disponible en: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump
- CAMPOS, C., MARTÍN PLAZA, A. <<Atentado en Barcelona y Cambrils. El día después de los atentados en Cataluña: cuatro detenidos y un huido>>. *RTVE*. 18 agosto 2017. Disponible en: http://www.rtve.es/noticias/20170818/atentado-barcelona-directo/1599220.shtml
- CASTILLO, C. DEL <<La paradoja de *Black Mirror*: *Netflix* guarda tus datos sobre qué elegiste en cada opción de su último capítulo interactivo>>. *El Diario*. 13 febrero 2019. Disponible en: https://www.eldiario.es/tecnologia/paradoja-Black-Mirror-Netflix-Bandersnatch_0_867563950.html
- CLEMENT, J. <<Number of mothly active Twitter users worldwide from 1st quarter 2010 to 1st quarter 2019 (in millions)>>. *Statista*. 14 agosto 2019. Disponible en: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/
- COX, J. <<The 'real' *dark web* doesn't exist>>. *Vice*. 31 agosto 2015. Disponible en: https://www.vice.com/en_us/article/vvbw8b/the-real-dark-web-doesnt-exist
- EDWARDS, A. <<FBI bids to extradite Irishman, 28, on suspicion of being 'largest child-porn dealer on planet'>>. *Daily Mail Online*. 5 agosto 2013. Disponible en: https://www.dailymail.co.uk/news/article-2384773/Eric-Eoin-Marques-largest-child-porn-dealer-planet-extradited-FBI.html

- FERNÁNDEZ BURGUEÑO, P. <<Si *Burger King* borrase los datos de todos [...]>>. *Twitter*. 10 mayo 2018, 18:27. Disponible en: https://twitter.com/pablofb/status/994614827032203265
- GIL GONZÁLEZ, E. *Big data, privacidad y protección de datos*. 1ª ed. Madrid: Boletín Oficial del Estado (BOE), 2016.
- IZQUIERDO, A. <<2.000 comunidades de gustos y 27.000 micro-géneros, la base del sistema de recomendación de *Netflix*>>. *Xataka*. 31 enero 2019 (actualizado 16 febrero 2019). Fuente: https://www.xataka.com/streaming/2000-comunidades-gustos-27000-micro-generos-base-sistema-recomendacion-netflix
- JIMÉNEZ VILLALONGA, R. <<Tipos de Inteligencia>>. *Grupo de Estudios sobre Seguridad Internacional*. 26 noviembre 2018. Disponible en: http://www.seguridadinternacional.es/?q=es/content/tipos-de-inteligencia
- JUÁREZ, S. <<*Cambridge Analytica* y ejercito de *trolls*: confirman la manipulación en las elecciones 2015>>. *Canal Abierto*. 31 julio 2018. Fuente: https://canalabierto.com.ar/2018/07/31/cambridge-analytica-y-ejercito-de-trolls-confirman-la-manipulacion-en-las-elecciones-2015/amp/
- KAINTURA, P. <<Hackers discover microphone hidden in *Lidl's* kitchen robot>>. *TechGrits*. 15 junio 2019. Disponible en: http://www.techgrits.com/hackers-discover-microphone-hidden-in-lidls-kitchen-robot-video/
- KHRON, R. <<17-Year-Old e-Girl Bianca Devins was killed by jealous family friend>>. *eBaum's World*. 15 julio 2019. Disponible en: https://www.ebaumsworld.com/articles/e-girl-bianca-michelle-devins-murdered-by-her-incel-orbiter/86016368/
- LÁZARO, M. <<*Por qué Twitter se ha llenado de gatos tras el atentado de Barcelona*>>. *El Huffington Post*. 18 agosto 2017. Disponible: https://www.huffingtonpost.es/2017/08/17/por-que-twitter-se-ha-llenado-de-gatos-tras-el-atentado-de-barce_a_23080797/
- LESSIG, L. *El Código 2.0*. 1ª ed. Madrid: Traficantes de Sueños, 2009.
- LUHN, H.P. <<A Business Intelligence System>>. *IBM Journal of Research and Development*. Oct. 1958, vol. 2, núm. 4, 314-319. Disponible en: http://altaplana.com/ibm-luhn58-BusinessIntelligence.pdf
- LUMB, D. <<*Cambridge Analytica* is shutting down following *Facebook* scandal>>. *Engadget*. 2 mayo 2018. Disponible en:

https://www.engadget.com/2018/05/02/cambridge-analytica-is-shutting-down-following-facebook-scandal/

- MACASKILL, E., DANCE, G. <<*NSA Files Decoded: Edward Snowden's surveillance revelations explained*>>. *The Guardian*. 1 noviembre 2013. Disponible en: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded
- MEHTA, I. <<*Netflix* tests tracking your 'physical activity' to improve video quality>>. *The Next Web*. 31 julio 2019. Disponible en: https://thenextweb.com/apps/2019/07/31/netflix-is-testing-changing-playback-quality-based-on-your-physical-activity/
- MORELL RAMOS, J. <<Si aceptas, la *app* de #*LaLiga* hace uso de tu micro y geolocalización [...]>>. *Twitter*. 10 junio 2018, 11:01. Disponible en: https://twitter.com/Jorge_Morell/status/1005736734255210496
- OTTO, C. <<Sanción histórica a la LaLiga: 250.000 € por 'espiar' con tu móvil en busca de piratería>>. *El Confidencial*. 12 junio 2019. Disponible en: https://www.elconfidencial.com/tecnologia/2019-06-11/aepd-laliga-app-sancion-multa-proteccion-datos-pirateria_2064138/
- PERETÓ, A. <<El caso *Walmart*>> *ICEDM Blog: La gestión del Big Data en la inteligencia de negocio*. 11 noviembre 2015. Disponible en: http://blogs.icemd.com/blog-la-gestion-del-big-data-en-la-inteligencia-de-negocio-/el-caso-walmart/
- POLICIA NACIONAL <<Por respeto a las víctimas y a sus familias, por favor, NO compartas imágenes...>>. *Twitter*. 17 agosto 2017, 17:45. Disponible en: https://twitter.com/policia/status/898209070993338368
- PONS, P. <<*Facebook* restringe las retransmisiones en directo tras la matanza de Nueva Zelanda>>. *La Vanguardia*. 15 mayo 2019. Disponible en: https://www.lavanguardia.com/tecnologia/20190515/462263858254/facebook-restringe-retransmisiones-directo-live-matanza-nueva-zelanda-redes-sociales-tecnologia-portada.html
- REDACCIÓN BBC NEWS MUNDO <<*Cambridge Analytica*: la multa récord que deberá pagar *Facebook* por la forma en que manejó los datos de 87 millones de usuarios>> *BBC News*. 24 julio 2019. Disponible en: https://www.bbc.com/mundo/noticias-49093124
- REDACCIÓN EL HUFFPOST <<Por qué están tuiteando patatas fritas contra los atentados en Bruselas>>. *El Huffington Post*. 22 marzo 2016. Disponible en:

https://www.huffingtonpost.es/2016/03/22/atentados-bruselas-patatas-fritas_n_9521522.html

- ROMERO, P. <<Reglamento Europeo – Mar España, directora de Protección de Datos: Las pymes me tienen preocupada>>. *Diario El Público*. 20 de mayo de 2018. Disponible en: https://www.publico.es/sociedad/reglamento-europeo-mar-espana-directora-proteccion-datos-pymes-me-preocupada.html
- VERDÚ, D. <<Golpe a la delincuencia de la *Deep Web*>>. *El País*. 12 noviembre 2014. Disponible en: https://elpais.com/politica/2014/11/12/actualidad/1415794086_687302.html
- WAROFKA, A. <<An Independent Assessment of the Human Rights Impact of *Facebook* in *Myanmar*>>. *Facebook Newsroom*. 5 agosto 2018. Disponible en: https://newsroom.fb.com/news/2018/11/myanmar-hria/
- <<*Facebook*, Social Media Privacy and the Use and Abuse of Data>>. *Senate Committee on the Judiciary, Senate Committee on Commerce, Science and Transportation*. 10 abril 2018. Disponible en: https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data
- <<Guía del Reglamento General de Protección de Datos para responsables de tratamiento>>. *Agencia Española de Protección de Datos*. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf
- <<Intelligence Threat Handbook. Intelligence Colletction Activities and Disciplines>>. *Federation of American Scientists*. Abril 1996. Disponible en: https://fas.org/irp/nsa/ioss/threat96/part02.htm
- <<Hoy probamos a fondo... Jurimetría>>. *Legaltechies*. 22 mayo 2018. Disponible en: https://legaltechies.es/2018/05/22/hoy-probamos-a-fondo-jurimetria/
- <<¿Qué son los datos abiertos?>>. *Open Data Handbook*. Disponible en: http://opendatahandbook.org/guide/es/what-is-open-data/
- Agencia Vasca de Protección de Datos (*Datuak Babesteko Euskal Bulegoa* en euskera): https://www.avpd.euskadi.eus/s04-5213/eu/
- Maltego CE, herramienta online gratuita: https://www.paterva.com/web7/downloads.php
- *Searching*. Dirigida por Aneesh CHAGANTI. EE.UU.: Stage 6 Films, 2018.
- *The Great Hack*. Dirigida por Karim AMER y Jehane NOUJAIM. EE.UU.: Netflix, 2019.

VII. FUENTES NORMATIVAS

- Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, de Protección de Datos Personales.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre la Privacidad y las Comunicaciones Electrónicas.
- Informe jurídico 327/2003, de la Agencia Española de Protección de Datos, sobre la consideración de carácter de dato personal de la dirección IP.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, sobre la Privacidad y las Comunicaciones Electrónicas.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la Protección de Datos Personales y a la Libre Circulación de estos Datos.

VIII. FUENTES JURISPRUDENCIALES

- STJUE (Sala Segunda) de 19 de octubre de 2016 (C-582/14, asunto Patrick Beyer contra *Bundesrepublik Deutschland*).
- STJUE (Gran Sala) de 29 de enero de 2008 (C-275/06, asunto Productores de Música de España contra Telefónica de España, S.A.U.).
- STS (Sala de lo Contencioso) de 3 de octubre de 2014 (núm. 3896/2014, Proc. 6153/2011).
- STS (Sala de lo Penal) de 19 de diciembre de 2018 (núm. 667/2018, Proc. 4554/2018).
- SAN (Sala de lo Social) de 6 de febrero de 2019 (núm. 13/2019, Proc. 318/2018, asunto Federación de Servicios de CC.OO. y Federación Estatal de Servicios, Movilidad y Consumo de la UGT contra Telepizza, S.A.U, y el Ministerio Fiscal).
- SAP (de Madrid) de 23 de mayo de 2017 (núm. 321/2017, Proc. 6587/2017).
- SAP (de Santa Cruz de Tenerife) de 3 de octubre de 2018 (núm. 294/2018, Proc. 1900/2018).
- Resolución de la AEPD (Proc. Nº PS/00326/2018).
- Resolución de la AEPD, R/00596/2017 (Proc. Nº PS/00371/2016).