LEFEBVRE

DESAFÍOS DE LA PROTECCIÓN DE DATOS EN 2022

INDICE

Ya puedes tener tus datos bajo control

LEFEBVRE

CENTINELA

Protección de Datos

Centinela Protección de Datos es un completo gestor documental diseñado para la correcta y sencilla implantación de un sistema de protección de datos personales en la empresa.

Una **guía eficaz** que te ayudará en la planificación, implantación y mantenimiento del sistemade protección de datos que llegado el caso te permitirá atestiguar todo el trabajo realizado durante el proceso.

- ☑ Adaptado a la ISO 19600
- ☑ Incluye el Memento Protección de Datos
- ☑ Permite la realización de evaluaciones de impacto y la confección del manual de política de protección de datos de la Organización

MÁS INFORMACIÓN EN EL 91 210 80 00

PRÓLOGO

2022 es un año que requiere atender, quizás más que nunca, a la Historia de la protección de datos personales. Desde el punto de vista legislativo esta comenzó en nuestro país hace treinta años. Fue en 1992 cuando se publicó Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (la famosa y derogada LORTAD).

Durante estas últimas tres décadas se ha producido una importante (r)evolución del derecho fundamental a la protección de datos personales que actualmente sigue avanzando en su europeización a través de la aplicación del Reglamento General de Protección de Datos (RGPD). Y el 28 de enero de cada año, día en el que se abrió a la firma el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, es una oportunidad para reflexionar sobre el pasado, presente y futuro de la protección de datos personales.

En concreto, en el marco de esta (r)evolución, cada vez estamos más inmersos en su europeización. Un claro ejemplo es la pandemia en la que desgraciadamente todavía seguimos inmersos. 2020 fue el año en el que se planteaba si el RGPD prohibía o permitía el tratamiento de datos relativos al COVID-19. A comienzos de 2022, aunque todavía se suscitan algunas dudas, lo que ha quedado claro es que el RGPD establece los requisitos de licitud del tratamiento, así como las bases de legitimación y condiciones a aplicar en casos como este.

La europeización es, precisamente, uno de los principales desafíos del derecho fundamental a la protección de datos en el momento actual. Desde las bases de legitimación del tratamiento, que ahora solo están en el RGPD, pasando por cuál es la autoridad competente en el caso de algunos tratamientos o hasta dónde llegarán las sanciones administrativas que imponen estas autoridades, son algunos de los retos a los que, a corto y medio plazo, tendremos que prestar atención.

Las obligaciones para las empresas derivadas de la normativa o pronunciamientos judiciales de la Unión Europeas, tales como los canales de denuncia, la regulación en materia de Inteligencia Artificial (IA) o en el caso de las redes sociales, son ejemplos de cuestiones que van a requerir atención con la finalidad de evitar fricciones entre el derecho fundamental a la protección de datos personales y otros derechos de la persona. Incluso cabría plantearse si la

protección de datos llegará a ser también un derecho de los robots.

Avanzaremos hacia nuevos conceptos y derechos como podría plantearse, por ejemplo, a partir de la "Teoría de modular de la privacidad de datos" ("Theory Modular Data Privacy"). Estos avances se producirán también ante el desafío de dar respuesta a interrogantes, tales como el valor económico de los datos personales que da lugar a su monetización.

El alcance del concepto de datos personales u otras cuestiones tales como los conceptos de responsable y encargado del tratamiento, que fueron interpretados por el ya extinto Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, seguirán siendo objeto de extensos debates jurídicos y darán lugar a la publicación de guías, directrices, sentencias, etc.

La atención se centrará también, sin duda, en aquellos casos en los que se traten categorías especiales de datos, tales como los datos relativos a la salud o afiliación sindical, o en otros casos como la geolocalización. Son tratamientos en los que la intromisión en la intimidad de la persona puede ser mayor o tener mayor incidencia. E incluso se siguen suscitando cuestiones sobre cuáles son los límites a los derechos a la intimidad y protección en ámbitos como el tributario.

Igualmente, nuevos desarrollos como la red social Clubhouse, que es una red social de chat de audios, pone de manifiesto el complejo escenario ante el que nos encontramos en materia de protección de datos por lo que se refiere a en dónde se tratan los datos personales. Es una cuestión de difícil solución que durante los próximos años seguirá planteando numerosos casos que para las organizaciones pueden implicar costosas decisiones, no solo en términos económicos, sino de elección de servicios digitales que les permitan asegurar el cumplimiento en materia de protección de datos personales. Y para los usuarios saber también a quién le dan sus datos personales.

Y los desafíos no acaban aquí, porque en breve podríamos asistir a la adopción de varias normas relevantes, aunque complejas, con implicaciones en materia de protección de datos, tales como la Ley de Inteligencia Artificial, la Ley de Mercados Digitales o la Ley de Servicios Digitales.

Este ebook es una publicación significativa y sobresaliente que nos invita a reflexionar, en particular en una fecha tan señalada, sobre temas clave en materia de protección de datos.

Miguel Recio Gayo
Doctor en Derecho. Profesor asociado de la Universidad CEU San Pablo y abogado de CMS Albiñana & Suárez de Lezo

GEOLOCALIZACIÓN Y DERECHOS FUNDAMENTALES

Julián García Marcos

1. Introducción: cuestiones terminológicas

Siempre conviene comenzar a escribir sobre una institución jurídica definiéndola. Y mucho más si hablamos de una herramienta tan compleja y de aplicaciones tan variadas como es la "geolocalización".

De la mano del Profesor Batucas Caletrio[1] podemos entender la geolocalización como "*la tecnología que permite ubicar un dispositivo en un punto espacial a partir de la transmisión de sus coordenadas de posicionamiento*".

Aparentemente la definición es sencilla. Ahora bien, jurídicamente, la forma en la que se ha introducido esta herramienta en nuestro ordenamiento no ha hecho sino confundir a los operadores jurídicos.

El art.588 quinques b) LECr. -**EDL 1882/1**-[2] alude a dispositivos o medios técnicos de seguimiento y localización.

En su primer apartado habla de que "el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización" determinando, eso sí, con precisión el medio empleado.

1. Intimidad Personal, protección de datos y geolocalizacion, Batucas Caletrio. Derecho Privado y Constitución ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82 http://dx.doi.org/10.18042/cepc/dpc.29.02.
2. "Cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización. 2. La autorización deberá especificar el medio técnico que va a ser utilizado. 3. Los prestadores, agentes y personas a que se refiere el art.588 ter e están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos por los que se ordene el seguimiento, bajo apercibimiento de incurrir en delito de desobediencia. 4. Cuando concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, la Policía Judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese en el mismo plazo. En este último supuesto, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso".

Y en el apartado tercero del mismo precepto habla de "no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización".

En la Exposición de Motivos de esta Ley se decía, únicamente, que "la reforma aborda también la regulación de la utilización de dispositivos técnicos de seguimiento y localización" razón por la cual la primera reflexión que puede hacerse a la luz de la redacción de este artículo es que nuestro legislador, a la hora de acometer la reforma que en nuestro ordenamiento operó la L 13/2015 de 5 octubre -**EDL 2015/102048**-, pensaba únicamente en lo que la Fiscal Ana Villagómez Muñoz define como "*aparatos que permiten determinar la posición de una persona o un objeto en un plano geográfico y temporal, determinados, tanto en tiempo real como mediante un estudio posterior de los datos recabados por el dispositivo utilizado*"[3].

Sin ánimo de exhaustividad, dentro de este amplio concepto nos podemos referir a distintas técnicas definidas, todas ellas, como modalidades dinámicas de localización:

- El sistema más comúnmente usado para el seguimiento y localización es el sistema GPS (Sistema de Posicionamiento Global) el cual suministra información sobre la posición y velocidad de un cuerpo 24 horas al día y con cobertura en todo el mundo,

- Cuando hablamos de "baliza policial" aludimos a un dispositivo electrónico oculto que genera información sobre localización y que, a través de las señales que emite por radiofrecuencia, sea o no a través de canales cerrados, permite realizar un seguimiento remoto de determinado objeto a través de un dispositivo receptor.

- Podrían incluirse dentro de este amplio concepto los dispositivos de descarga de localización (Qlog).

Todos ellos son instrumentos que permiten determinar la posición de una persona u objeto en un plano. Y envían señales para permitir ubicarla.

Volviendo, no obstante, al art.588 quinques nuestra Ley no sólo habla de instrumentos o "dispositivos".

Cuando nuestra Ley rituaria habla de **"medios de seguimiento y localización"** la doctrina entiende que alude a todos aquellos mecanismos aptos para recabar datos relacionados con la ubicación de una persona, normalmente vinculados con la operativa de proveedores de servicios de telecomunicaciones.

Estaríamos hablando, a título meramente ejemplificativo, de la localización GSM (Sistema Global de Comunicaciones Móviles), un servicio ofrecido por las empresas operado-

3. Otras medidas de investigación limitativas de derechos reconocidos por el art.18 CE -EDL 1978/3879- referencia concreta a los dispositivos de seguimiento y localización. Curso: "La interceptación de las comunicaciones telefónicas y telemáticas" En: Estudios jurídicos-Ministerio Fiscal, 2016.

ras de telefonía móvil que permite establecer, con cierta precisión, donde se encuentra físicamente un terminal móvil en un momento determinado.

Esta imprecisión terminológica no sólo trasciende doctrinalmente, sino que tiene su proyección en la práctica habitual de Juzgados y Tribunales.

En fecha de 1 de julio de 2019 el Juzgado de Instrucción nº 4 de Ávila dictó auto en el que acordaba expedir oficios a las compañías operadoras de servicios de telefonía móvil a fin de que remitieran a la Comandancia de la Guardia Civil los datos de geolocalización de varios números de telefonía móvil en determinados periodos de tiempo. Se estaba investigando un delito de quebrantamiento de medida cautelar. La primera cuestión que la Audiencia Provincial se plantea es determinar el precepto que ampara la solicitud policial de localización de un terminal móvil, ya sea el art.588 quinquies b) que sostenía la resolución impugnada o el art.588 ter j) que consideraba el Ministerio Fiscal concluyendo que el precepto que amparaba la solicitud formulada era el art.588 ter j), en la medida que se interesaba la localización de un terminal móvil.

Cierto que el recurso del Ministerio Fiscal fue desestimado por motivos diversos pero, entiendo, que es el confuso encabezamiento del precepto el que, en definitiva, puede llevar a los operadores jurídicos a confundir los fundamentos de cada una de las medidas de investigación.

Pudiera pensarse, para terminar, que el legislador aprovecharía el Anteproyecto de Nueva Ley de Enjuiciamiento Criminal para poner fin a tanta confusión.

Mas nada más lejos de la realidad. De hecho la primera de las cuestiones que cabe reprochar al Anteproyecto -si es que pretendía solventar este problema- es su escasa precisión terminológica.

Y es que mientras que el art.396.1 del Anteproyecto se refiere a "medios técnicos de seguimiento y localización", el art.396.2 alude a "dispositivos", el art.399 vuelve a mencionar los "dispositivos" o el art.400 los "medios técnicos".[4]

2. Potencialidad lesiva de la geolocalización: los derechos fundamentales que se pueden ver limitados en el proceso penal por estas medidas de investigación

Ya hablemos de "dispositivos" o ya hablemos de "medios" lo que es evidente es que la L 13/2015 de 5 octubre de modificación de la Ley de enjuiciamiento criminal -**EDL 2015/169144**- para el fortalecimiento de las garantías procesales y la regulación de las me-

4. Las medidas de investigación tecnológica en el anteproyecto de ley de enjuiciamiento criminal de 2020. Una aproximación preliminar Julián García Marcos, Javier Ignacio Zaragoza Tejada Revista Aranzadi Doctrinal,ISSN 1889-4380, Nº. 2, 2021.

didas de investigación tecnológica se vio obligada a introducir en nuestra Ley procesal una detallada y novedosa regulación de ambos. Y en su Exposición de Motivos destacaba que solo mediante su regulación "*se podrá evitar la incidencia negativa que el actual estado de cosas está proyectando en relación con algunos de los derechos constitucionales que pueden ser objeto de limitación en el proceso penal*".

Vale la pena detenerse, al menos someramente, en cuales son estos derechos fundamentales que nuestro legislador veía tan necesario proteger a la luz de la carencia que, en esas fechas, habían puesto de manifiesto las instituciones supranacionales respecto a nuestros instrumentos normativos.

a.- si los "medios" o datos de geolocalización aparecen vinculados a procesos comunicativos [5] es factible considerar (sobre todo si pensamos en ello desde un punto de vista "dinámico"[6]) que gozan de la super-protección que el art.18.3 de la Constitución Española -**EDL 1978/3879**- otorga a las comunicaciones[7]. En consecuencia ya desde antiguo se viene asumiendo que sólo cabe el desvelo de estos datos previa autorización judicial[8].

b.- Ahora bien, tanto si estos datos aparecen desvinculados de cualquier tipo de comunicación (obviando a aquellos sectores doctrinales que defienden que entre "aparatos" puede generarse una comunicación, en sentido estricto, desligada de intervención humana y la distinción antes mencionada) como si hablamos, exclusivamente, de "ubicación" geográfica son la intimidad (art.18.1 CE) y el derecho a la protección de datos personales (art. 18.4 CE -**EDL 1978/3879**-) los derechos que pueden verse concernidos.

Sin que podamos obviar, en este sentido, por su trascendencia, que el Convenio Europeo de Derechos Humanos en su artículo 8 reconoce que "*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*" y que "*no podrá haber injerencia de la autoridad públi-*

5. El art.3.1.f) L 25/2007, de 18 octubre, de conservación de datos -EDL 2007/159198- relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones entiende que son datos que los operadores de telefonía han de conservar, conforme a sus prescripciones, los datos necesarios para identificar la localización del equipo de comunicación móvil, esto es: 1.º La etiqueta de localización (identificador de celda) al inicio de la comunicación y 2.º Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.
6. Cuando introduzco este matiz estoy pensando en la diferenciación que hizo entre datos "dinámicos" y "estáticos" la STS 7/2014 de 22 enero -EDJ 2014/7521- (que venía a decir: "ese listado (de llamadas) no puede estimarse desprovisto de protección constitucional. De hecho, en función de su consideración estática -listado de llamadas obrante en los archivos de las operadoras, expresivo de comunicaciones ya concluidas y que no estaban siendo objeto de intervención judicial-, o dinámica -listado de llamadas generado durante conversaciones que ya son objeto de una medida de injerencia-, su régimen jurídico es diverso y el grado de protección también lo es") Ahora bien, esta distinción entre datos dinámicos y estáticos ha perdido bastante fuerza a partir de la entrada en vigor de la reforma operada en la LECRIM por la LO 13/2015 -EDL 2015/169144-).
7. Art.18.3 CE -EDL 1978/3879-: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".
8. Art.588 ter j) 1 LECRIM -EDL 1882/1-: "Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial"

ca en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

i.- Con respecto al derecho a la intimidad[9] en la ya vetusta STC 70/2002 de 3 abril 2002 -EDJ 2002/7116- el Tribunal Constitucional reconoce que la intimidad es un derecho fundamental digno de protección pero, al mismo tiempo, susceptible de ser limitado previa resolución judicial o, subsidiariamente, en los casos de necesaria y urgente intervención policial, previo balance de proporcionalidad.

El Tribunal Constitucional asevera que "*lo intervenido* (unas hojas manuscritas y dobladas, sin sobre, en el interior de una agenda que portaba el detenido) *pertenecía al ámbito de la intimidad*" concluyendo que dicha incautación se trataba "*de una diligencia practicada en el curso de la investigación de un delito (...) y orientada a la averiguación del mismo y a la recogida de instrumentos, efectos y pruebas del mismo. Por tanto, concurre un fin constitucionalmente legítimo. En segundo lugar, (que) existe habilitación legal para la actuación de la policía, (..., art.282 LECrim -**EDL 1882/1**-). En tercer lugar, si bien la actuación no se realiza previa autorización judicial, podemos afirmar que estamos en uno de los supuestos excepcionados de la regla general, pues existen y pueden constatarse razones para entender que la actuación de la Guardia Civil era necesaria. (...). A lo que ha de añadirse, por último, que la actuación policial respeta el principio de proporcionalidad, pues se trata de una medida idónea para la investigación del delito (de la agenda y de los documentos se podían extraer -como así fue- pruebas incriminatorias y nuevos datos para la investigación), imprescindible en el caso concreto (no existían otras menos gravosas) y ejecutada de modo tal que el sacrificio del derecho fundamental no resulta desmedido en relación con la gravedad de los hechos y las sospechas existentes*".

ii.- Con respecto al derecho a la protección de datos de carácter personal[10], más allá de su reciente configuración jurisprudencial, ya en la STC 96/2012 de 7 mayo 2012 -**EDJ 2012/98391**- se fijan criterios para su adecuada protección.

En este caso, en el seno de unas diligencias preliminares, ADICAE solicita que el Juzgado requiera a la sociedad BBVA para que entregue los listados diferenciados por productos financieros,

9. Art.18.1 CE -EDL 1978/3879-: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"

en fichero electrónico "Excel" o compatible, que contengan los datos personales (nombre y apellidos, DNI, dirección postal actualizada, y números de teléfono, fax y correo electrónico, si estuvieren disponibles), de los clientes personas físicas que, en toda España, hubieran contratado con dicha entidad bancaria productos financieros.

El Tribunal Constitucional reconoce, a este respecto, que "los datos solicitados a la entidad demandante están protegidos por el art.18.4 CE -**EDL 1978/3879**-, que "*consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona*" y, en consecuencia debe analizar si la medida acordada por el juez limita el derecho fundamental a la protección de datos de carácter personal y, en caso afirmativo, si dicha injerencia es constitucionalmente legítima. Y para llevar a cabo este análisis viene a exigir "*que la medida limitativa del derecho fundamental esté prevista por la Ley, que sea adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo*". Sólo cabe limitar la concreta facultad de disposición y control de los datos personales en atención a derechos y bienes de relevancia constitucional y, por tanto, esta limitación ha de estar justificada, ser proporcionada y, además, establecerse por Ley, pues el derecho fundamental a la protección de datos personales no admite otros límites.

3. Evolución jurisprudencial: de la intrascendencia constitucional a la super-protección

Centrada, de esta manera, la materia objeto de nuestro análisis, esto es, puesta de manifiesto la indefinición terminológica de nuestra Ley rituaria y sentadas las bases para entender que no cabe una injerencia en los derechos fundamentales atinentes a la geolocalización de personas sin la correspondiente ponderación legal y, en su caso, autorización judicial, entremos a analizar tanto los antecedentes de cada una de estas medidas como la situación en que, actualmente, nos encontramos al respecto.

a.- Con respecto a los **dispositivos técnicos de geolocalización** hemos de mencionar, cuando menos, el caso Estados Unidos contra

10. Art.18.4 CE -EDL 1978/3879-: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Antoine Jone[11], jurisprudencia norteamericana que sirve de germen para el cambio normativo que con respecto a estos instrumentos de investigación se produjo y el asunto del Tribunal Europeo de Derechos Humanos de Uzun contra Alemania.

En el primero de ellos la Corte Supremo Norteamericana entra a analizar si la conexión de un dispositivo GPS a un "jeep" con el fin de "seguir" a un objetivo durante cuatro semanas con el fin de contrastar las sospechas que tenían frente a su usuario se hizo o no con cumplimiento de las prescripciones judiciales fijadas en la resolución habilitante.

Con respecto al segundo Omar Bouazza Ariño[12] analiza cuidadosamente el supuesto de hecho y las conclusiones que alcanza el Tribunal en su sentencia.

Durante una investigación dirigida por el Fiscal General Federal alemán contra el Sr. Bernard Uzun y un presunto cómplice por haber participado en un atentado terrorista el Sr. Uzun y su cómplice destruyeron los transmisores instalados en el coche del presunto cómplice. El Fiscal decidió instalar un sistema de geolocalización por satélite en el coche del cómplice del Sr. Uzun. La vigilancia duró dos meses, hasta que el Sr. Uzun fue detenido. El Tribunal Constitucional Alemán en la Sentencia de 12 de abril de 2005 entiende "proporcionado" este medio de investigación, dada la gravedad de los delitos. Añade que las garantías procesales contempladas en la ley eran suficientes para proteger la intimidad de la persona pero invita al legislador alemán a que valore si, con la evolución de la técnica, pudiera resultar conveniente una legislación más garantista.

El Tribunal Europeo de derechos humanos considera que la medida estaba justificada y fue proporcional al fin perseguido y a la naturaleza del delito descartando que se viole el art.8 del Convenio Europeo de Derechos Humanos -**EDL 1979/3822**-. Y llega a esta conclusión dado que dicha medida estaba prevista en el Código Procesal alemán, perseguía un fin legítimo (se investigaba un caso de terrorismo en que estaba en juego la seguridad pública) y los tribunales alemanes habían reforzado el control judicial en la utilización de este tipo de medidas no obstante reconocer que el hecho de que las autoridades alemanas hayan recopilado sistemáticamente información del Sr. Uzun a través del sistema GPS supone una injerencia en el derecho al respeto de la vida privada del demandante.

11. Un análisis detallado del supuesto puede hallarse en LA LOCALIZACIÓN DEL SOSPECHOSO MEDIANTE DISPOSITIVOS DE SEGUIMIENTO Y SU APLICACIÓN EN EL PROCESO PENAL. PRUEBA ILÍCITA. Trabajo de fin de grado de CRISTINA MAÑAS MARIN que puede consultarse en https://biblioteca.cunef.edu/files/documentos/TFG_Cristina_Ma%C3%BIas.pdf.
12. Notas de Jurisprudencia del Tribunal Europeo de derechos humanos, Revista de Administración pública ISSN 0034-7639 num. 184 Madrid enero-abril (2011) pags. 193-207.

En nuestro ordenamiento, hasta fechas bien recientes, el uso de geolocalizadores apenas ha tenido incidencia en nuestros tribunales y ha sido considerada siempre como una herramienta propia de la actividad investigadora de la Policía Judicial[13]. En la STS 562/2007 -**EDJ 2007/80222**- el recurrente invocan la "*vulneración de su derecho (...) a la intimidad que concretan en el hecho de haber colocado (en una embarcación) una baliza de seguimiento sin autorización judicial*". Responde nuestro Tribunal Supremo que "*se trata (...) de una diligencia de investigación, legítima desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiriera en un derecho fundamental que requeriría la intervención judicial*". En la STS 906/2008 -**EDJ 2008/272898**- el Tribunal Supremo afirma que si la localización (SITEL o Sistema de Intervención Telefónica) "*permitiera conocer el lugar exacto en el que el comunicante se encontraba podría hablarse de una afectación a la intimidad*", pero que, cuando como en este caso, esa ubicación sólo puede concretarse con una aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal, en modo alguno "*puede considerarse afectado, al menos de forma relevante, el derecho a la intimidad del sometido a la práctica de la diligencia*". En la STS 798/2013 -**EDJ 2013/214599**- (posterior, incluso, a la STEDH Uzun contra Alemania) se decía que "*el uso de radiotransmisores para la localización de embarcaciones en alta mar por la policía (...) (no) supone una inferencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional*". Finalmente, en la STS 610/2016 -**EDJ 2016/113582**- (posterior a la entrada en vigor de la reforma que en la LECRIM opera la L 13/2015 de 5 octubre -**EDL 2015/169144**-) en la que se plantea la vulneración del derecho a la intimidad por "*la instalación en el vehículo que utilizaba el recurrente de un dispositivo GPS o baliza de seguimiento por parte de la autoridad policial sin previa y preceptiva autorización judicial*" se concluyó, como hacía la Instancia, que "no se había vulnerado el derecho a la intimidad con tal intensidad que hubiese sido necesaria la previa autorización judicial". La situación cambia, radicalmente, a partir de la STS 141/2020 -**EDJ 2020/553012**-.

En este caso, ante una condena por delito contra la salud pública, el recurrente alega que el auto que autorizaba la instalación y uso por los agentes de policía de un dispositivo de localización global de navegación por satélite (GNSS) en el vehículo habitualmente utilizado por el acusado, era nulo de pleno derecho. Argumenta que el oficio de la Guardia Civil, dirigido al Juzgado de instrucción, era manifiestamente insuficiente para justificar la injerencia en el derecho fundamental a la intimidad.

13. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, JULIÁN GARCÍA MARCOS. Pags. 285 a 325. INVESTIGACIÓN TECNOLÓGICA Y DERECHOS FUNDAMENTALES. Coord. JAVIER IGNACIO ZARAGOZA TEJADA, 2017. Ed. Aranzadi.

En este caso nuestro Tribunal Supremo, tras una profusa enumeración de antecedentes jurisprudenciales (en los cuales, como ya hemos visto, se llegó a negar que la colocación de una baliza afectara a derecho fundamental alguno) llega a la conclusión de que "el conocimiento por los poderes públicos, en el marco de una investigación penal, de la ubicación espacio-temporal del sospechoso, encierra una injerencia de menor intensidad que otros actos de investigación perfectamente imaginables" lo que, entiende, "no puede llevarnos a banalizar el acto de intromisión estatal que la utilización de un GPS representa en el círculo de derechos fundamentales de cualquier ciudadano".

Y a pesar de que el legislador haya guardado silencia al respecto en la reforma operada en la Ley de Enjuiciamiento Criminal por la LO 13/2015 -**EDL 2015/169144**- concluye que los "principios de proporcionalidad, necesidad y excepcionalidad siguen actuando como presupuestos de legitimidad, cuya concurrencia ha de quedar expresamente reflejada en la resolución judicial habilitante" siendo que en el caso concreto nada de esto sucedió.

Y, como queda reflejado en la Sentencia, no hablamos ya, en este momento, de existencia/inexistencia de auto que autorizara la colocación de la "baliza" sino de la suficiencia en la ponderación realizada.

Teniendo en cuenta que el principal motivo por el que se atiende al recurso del condenado es que la resolución habilitante se apoyaba, esencialmente, en una "confidencia" policial le habría bastado al Tribunal Supremo acudir a su propia Jurisprudencia (STS 373/2017 de 24 mayo -**EDJ 2017/135139**-[14]) para legitimar su discurso.
No obstante nuestro Tribunal Supremo menciona recientes Sentencias en las que rechaza que la colocación de una baliza interfiriera en un derecho fundamental que requeriría la intervención judicial y, posteriormente, tomando como punto de partida la antes mencionada STEDH Uzun contra Alemania exacerba, desde mi punto de vista, sin excesivo razonamiento, la protección que ha de brindarse al derecho a la intimidad.

Decía la Circ 4/2019 de 6 marzo -**EDL 2019/6833**- de la FGE que "uno de los factores que influyen de manera determinante en el juicio de ponderación que exige el principio de proporcionalidad es el de la duración de la medida". Y en Uzun contra Alemania se decía "the applicants observation via GPS, in the circunstances (for 3 months collected and store data) and

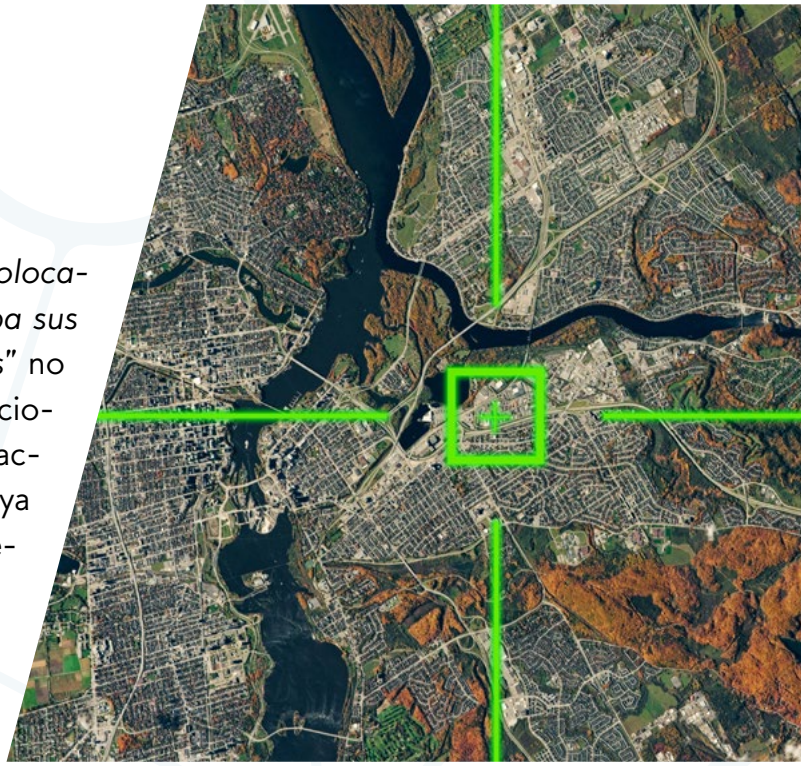
14. "la mera referencia a informaciones "confidenciales" no puede servir de fundamento único a una solicitud de medidas limitadoras de derechos fundamentales (entradas y registros, intervenciones telefónicas, detenciones, etc.), y, en consecuencia, a decisiones judiciales que adoptan dichas medidas, salvo supuestos excepcionalísimos de estado de necesidad (peligro inminente y grave para la vida de una persona secuestrada, por ejemplo)".

the processing and use of data (...) amounted to an interference with private life" (esto es, la observación de los demandantes via GPS por tres meses y recopilando y procesando datos (...) constituye una interferencia en la vida privada) y que "cannot be said to have been subjected to total and comprehensive surveillance" (esto no supone ser objeto de una total y omnicomprensiva vigilancia) ya que "surveillance was carried out for a relatively short period of time (...) affected him essentially only at weekends" (la vigilancia había sido llevada a cabo durante un breve periodo de tiempo y, sobretodo, los fines de semana).

En el caso de referencia, el que dio lugar a la STS 141/2020 -**EDJ 2020/553012**-, no queda plasmado, en absoluto, si la intensidad de la injerencia en la intimidad del investigado fue más allá de la mera colocación del dispositivo de localización global de navegación por satélite (GNSS) en el vehículo habitualmente utilizado por el acusado, se perpetuó (o no) en el tiempo o se proyectó sobre aspectos de la vida privada del condenado. Simplemente se considera que la colocación de la baliza es una injerencia en la intimidad del condenado per se y la fundamentación del Juez de Instrucción debía haber respetado la "*proporcionalidad, necesidad y excepcionalidad (...) como presupuestos de legitimidad*" de la medida. Algo que, teniendo en cuenta el origen de la información suministrada, no hizo.

Lo que es evidente es que a raíz de los postulados (y aseveraciones) de esta Sentencia nuestro Tribunal Supremo ha sido uniforme en su interpretación de la cuestión que nos ocupa.

En la STS 530/2020 de 21 octubre 2020 -**EDJ 2020/693731**-, en un supuesto en donde se ponía en tela de juicio la validez de los datos obtenidos de un balizamiento acordado por las autoridades alemanas, se destaca "*la absoluta imprescindibilidad de la autorización judicial para que los datos obtenidos, como elementos de investigación o de prueba, puedan ser utilizados en la causa*" añadiendo que "*cuando los dispositivos se hayan instalado en otro país y se continúe la intervención en territorio español, debe ponerse en conocimiento de la autoridad judicial, en la forma y a los efectos previstos en las normas de cooperación internacional*" mientras que en la STS 291/2021 de 7 abril -**EDJ 2021/547693**- en donde, de nuevo, se consideraba por el recurrente que el auto habilitante, que acordó la colocación en el vehículo de un aparato de geolocalización a fin de controlar sus desplazamientos, no estaba sustentado en indicios fundados, sino en meras conjeturas policiales, que justificaran la invasión del espacio reservado a toda persona que con tal medida se producía, el Tribunal Supremo tacha de inaceptable la pretensión considerando que "*la vigilancia sobre el coacusado (...) buscaba descubrir la existencia de otros miembros de la organización y*



la forma de actuación, lo que implica que la colocación del dispositivo en el vehículo que facilitaba sus desplazamientos, cumplía los requisitos legales" no sin antes aclarar que "los principios de proporcionalidad, necesidad y excepcionalidad siguen actuando como presupuestos de legitimidad, cuya concurrencia ha de quedar expresamente reflejada en la resolución judicial habilitante".

A la vista de los términos en los que se está expresando, recientemente, el Tribunal Supremo no parece que pueda esperarse una "*rebaja (de) las exigencias necesarias para la utilización de esta técnica de investigación en relación con otras, como las intervenciones telefónicas, haciendo depender casi en exclusiva la legalidad de su uso del juicio de proporcionalidad*" y que aunque "*la autorización judicial será siempre necesaria (...) su justificación podrá ser acorde a esta menor afectación*" aspecto que destacaba la Fiscalía General del Estado en su Circ 4/2019 de 6 marzo -**EDL 2019/6833**-, en relación con la jurisprudencia del TEDH apoyándose, fundamentalmente, en que "a pesar de la limitación de la intimidad que a través de los dispositivos técnicos de seguimiento y localización se produce, se trata, por regla general, de intromisiones de baja intensidad".

De hecho, y quizá inspirado en esta STS 141/2020 de 13 mayo -**EDJ 2020/553012**-, el Anteproyecto de nueva Ley de Enjuiciamiento Criminal sujeta la utilización de medios (y dispositivos) de localización a la preceptiva resolución del Juez de Garantías que deberá conceder la misma en base al principio de proporcionalidad. Obvia, sin embargo, la referencia a los principios de necesidad y de idoneidad, principios a los que, por remisión a las disposiciones generales relativas a las intervención de las comunicaciones, sí que inspiran el artículo 588 quinques y tampoco sujeta dicha autorización a una tipología concreta.

b.- Es la misma Circ 4/2019 de 6 marzo -**EDL 2019/6833**- de la FGE en su apartado 3.2 la que introduce los **"medios" de localización** cuando asegura que "la recopilación sistemática de datos de posicionamiento afecta también al derecho a la protección de datos personales del investigado (Art.18.4 CE -EDL 1978/3879-), con una incidencia directa, además, en el derecho a la intimidad".

Ello nos lleva, necesariamente, a analizar la trascendencia constitucional que pueden llegar a tener los servicios ofrecidos por las empresas operadoras de telefonía móvil para establecer, con cierta precisión, donde se encuentra físicamente un terminal móvil en un momento determinado[15].

i.- Dentro de estos medios ya hemos mencionado, anteriormente, los datos de localización que pueden ser considerados como datos de tráfico (art. 3.1.f) de la L 25/2007, de 18 octubre -**EDL 2007/159198**-, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones) los cuales se generan como consecuencia de la realización de una llamada o de la remisión de un mensaje de texto.

De acuerdo con lo dispuesto en la citada L 25/2007, de 18 octubre -EDL 2007/159198- las operadoras de telefonía almacenan estos datos durante un periodo de 12 meses pudiendo ser cedidos en virtud de mandamiento judicial y persecución de delitos graves y de acuerdo con el art.588 ter j) LECr. -EDL 1882/1- "los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial".

ii.- Al lado de los citados datos de localización-datos de tráfico estarían los datos de localización distintos a los de tráfico, los datos "stand by", que posibilitarían una comunicación si se realizaran las actuaciones conducentes para ello.

Cuando nuestro teléfono móvil conecta con una red G.S.M.[16] la localización se almacena en unas bases de datos denominadas H.L.R (Home Location Register) que se van actualizando a medida que vamos transitando por distintas antenas B.T.S[17]. Teniendo en cuenta el escaso periodo de tiempo en que estos datos permanecen en el sistema toma especial interés lo que se ha venido a llamar "aseguramiento inmediato" cuyos antecedentes se encuentran en el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 y que se regula en nuestra LECRIM en el art. 588 octies[18].

15. El nuevo papel de la telefonía móvil en el proceso penal: ubicación y perfiles de desplazamiento, JULIO PEREZ GIL (coord) en EL PROCESO PENAL EN LA SOCIEDAD DE LA INFORMACIÓN PARA INVESTIGAR Y PROBAR EL DELITO. Editorial LA LEY. 2012.
16. GSM son las siglas de Global System for Mobile communications (Sistema Global para las comunicaciones móviles) y es un tipo de red que se utiliza para la transmisión móvil de voz y datos.
17. En el contexto de la telefonía móvil, una estación base (en inglés: Base Transceiver Station (BTS) dispone de equipos transmisores/receptores de radio, en la banda de frecuencias de uso (850/900 /1800/1900 MHz) En GSM y (1900/2100Mhz) en UMTS que son quienes realizan el enlace con el usuario que efectúa o recibe la llamada (o el mensaje) con un teléfono móvil (https://es.wikipedia.org/wiki/Estaci%C3%B3n_base).
18. "El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos

Al respecto de la investigación con los datos que hemos denominado "stand by" (incluso esta Sentencia podría entenderse referida a los primeros, los datos de localización-datos de tráfico) vale la pena detenerse en la posición que el Tribunal Supremo mantuvo en su STS 777/2012 de 17 Octubre 2012 -EDJ 2012/237512- en la que salía al paso de los reproches que los recurrentes planteaban con respecto a lo que, entonces, denominaban "rastreo de datos". Nuestro Tribunal Supremo reconocía que "este cruce de datos será extremadamente útil en la investigación de una serie de delitos, de importante impacto social, y que pueden verse facilitados en su esclarecimiento a través de esta nuevas técnicas en el cruce de conectividades" y que "obviamente por ello no se ven afectados, ni han de incidir, ni en el invocado derecho constitucional a la intimidad, ni al secreto de las comunicaciones". El Tribunal Supremo rechaza la posibilidad de que esta técnica vulnere la intimidad (tal como se planteaba por las defensas) pues "lo único que pretende es conseguir, en un radio de acción prefijado, la activación de unos mecanismos de comunicación, traducidos en números, de donde pueda inferirse la localización de unos terminales de donde inducir la presencia de unos pocos sospechosos que respondan a la utilización más certera de un material que se ha conseguido por otros medios probatorios (...) remitiéndose a la línea seguida por la antes mencionada Sentencia 906/2008, de 19 diciembre -EDJ 2008/272898- de acuerdo con la cual "*esa ubicación sólo puede concretarse con una aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal,* ***en modo alguno puede considerarse afectado, al menos de forma relevante, el derecho a la intimidad del sometido a la práctica de la diligencia***" y negando, finalmente, la posibilidad de que este tipo de rastreo pueda considerarse puramente prospectivos.

Es verdad que esta postura ha sido, posteriormente, matizada. Y no cabe la menor duda de que, actualmente, recabar estos datos de las operadoras de telefonía afecta a derechos fundamentales de la persona, ya sea la intimidad (almacenamiento masivo de datos de localización o "cruzado" de datos con otras bases) o el derecho a la protección de datos personales.

Y así lo ha reconocido el Tribunal Supremo en su más reciente STS 723/2018 de 23 enero 2019 -**EDJ 2019/501813**- cuando considera legítimo el acceso a "*los datos relativos a los teléfonos móviles que se conectaran en un determinado momento a una concreta antena de telefonía, con la finalidad de cruzarlos con los de otras antenas, instaladas todas ellas en zona*" en virtud de resolución judicial y con una adecuada y justificada ponderación de la proporcionalidad.

Por la relevancia que el acceso a estos datos de localización que hemos denominado "stand by" pueden tener para el derecho a la protección de datos debe destacarse la recien-

te LO 7/2021, de 26 mayo, de protección de datos personales -**EDL 2021/17526**- tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales en cuyo artículo 7.2 se obliga a "*las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública*".

Si bien de esta manera, de la misma forma que ocurría con el art. 22.2 de la ya derogada Ley Orgánica de protección nº 15/1999 de protección de datos de carácter personal -**EDL 1999/63731**- [19], los Agentes de la Policía Judicial contaban con habilitación legal para utilizar datos con fines de investigación delictiva el artículo 515.1 del Anteproyecto de nueva Ley de Enjuiciamiento Criminal faculta, únicamente, al Fiscal, previo dictado de un Decreto (con el contenido del artículo 515.2 del Anteproyecto) a requerir a los responsables del tratamiento, ya sean personas públicas o privadas, la cesión de datos personales incluidos en archivos o registros, siempre que el conocimiento de los mismos sea indispensable para el descubrimiento del hecho investigado[20].

iii.- Como tercera categoría dentro de los "medios" de localización estarían los **datos de localización que los operadores ofrecen como Servicio de Valor Añadido (S.V.A.)** [21]

En este caso se hace referencia a aquellos que se almacenan como consecuencia de las prestaciones que ofrece un servicio tras ser contratado, suscrito y activado pudiendo situar con precisión el aparato sobre un mapa.

Para acceder a estos datos sería precisa autorización judicial conforme a lo dispuesto en el art. 588 sexies a) 1 LECr. -**EDL 1882/1**- [22]

19. "la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales".
20. Las medidas de investigación tecnológica en el anteproyecto de ley de enjuiciamiento criminal de 2020. Una aproximación preliminar Julián García Marcos, Javier Ignacio Zaragoza Tejada Revista Aranzadi Doctrinal, ISSN 1889-4380, Nº. 2, 2021 (ya mencionado).
21. Estos SVA se definen en el art. 2 Dir 2002/58/CE -EDL 2002/29506- como "todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación". En la propia Directiva se utilizan como ejemplos recomendaciones sobre tarifas menos costosas, orientación vial, información sobre tráfico, previsiones meteorológicas o servicios de información turística.
22. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos".

4. Conclusiones

En resumen, las nuevas técnicas de investigación basadas en la geolocalización, ya sean las apoyadas en la utilización de dispositivos técnicos o las basadas en los datos que se generan por los dispositivos electrónicos afectan de forma relevante a los derechos fundamentales. Y aunque desde diversos sectores doctrinales, desde la propia Fiscalía o desde las instituciones supranacionales se ha defendido la menor intensidad en la ingerencia lo que es cierto es que nuestro Tribunal Supremo ha ido evolucionando hacia la super-protección de la intimidad siendo, actualmente, necesario que sea el Juez Instructor el que, valorando previamente la necesidad, la utilidad y la proporcionalidad supervise la utilización de cualquier medida de esta naturaleza. Ello sin perjuicio de la reciente habilitación que, al respecto, la reciente LO 7/2021, de 26 mayo -**EDL 2021/17526**- que podría posibilitar, en casos concretos, que sean las Fuerzas Policiales las que, dependiendo del caso, accedan sin la venia judicial a aquellos datos que, sin afectar a la intimidad, sean objeto de cobertura a través de la protección de datos de carácter personal.

ADMISIÓN O NO POR LA EMPRESA DE LAS DENUNCIAS ANÓNIMAS

ElDerecho.com

El 17 de diciembre entra en vigor la **directiva europea 2019/1937** que obliga a todas las sociedades con más de 249 empleados y a las administraciones públicas con poblaciones superiores a 10.000 habitantes a implementar en su sistema un canal de denuncias para velar por la buena praxis empresarial. Así, cualquier trabajador, directivo o agente externo con algún tipo de vínculo laboral (proveedores, colaboradores, comerciales, etc.) puede hacer uso de esta herramienta para denunciar conductas inmorales, situaciones irregulares y otros delitos o faltas de las que deseasen informar.

Según el texto de la directiva europea, el procedimiento natural de todas las denuncias efectuadas será el siguiente: emisión de la denuncia, admisión a trámite, actuaciones del responsable y resolución de la denuncia. Las denuncias pueden ser anónimas o nominativas y, en ambos casos, aportar la siguiente información para ser admitida a trámite: exposición de los hechos denunciados con detalles y datos que faciliten su análisis, explicación sobre la manera de la que se tuvo conocimiento de los hechos denunciados, personas o entidades contra las que se dirige la denuncia acotando al máximo el número de implicados para facilitar su individualización (nombre, cargo, departamento, etc.), enumeración de testigos si los hubiera y otro tipo de informaciones que puedan facilitar la investigación y resolución de los hechos denunciados. La principal diferencia, por tanto, entre las denuncias anónimas y las nominativas es que las segundas requieren la identificación del emisor mediante el nombre, los apellidos, DNI, teléfono y correo electrónico. Así, todas las denuncias emitidas que no se acojan a esas condiciones no serán procesadas.

Si la denuncia prosperase, el responsable o departamento encargado del Canal de Denuncias procederá a su admisión y tramitación abriendo un expediente y asignándole un número de referencia para facilitar su seguimiento.

Por el contrario, si la denuncia se rechazase por entenderse que no cumple con los requisitos exigidos, bien por la falta de pruebas físicas, testigos o porque la denuncia presentada no fuese contraria a la legalidad del convenio o los principios éticos de la actividad económica, se archivaría de manera inmediata.

Del mismo modo, el responsable debe elaborar un informe detallado mediante el cual comunique y justifique los motivos por los que la denuncia no ha sido tramitada y se ha procedido a su archivo.

Otro de los escenarios que podría presentarse es la petición del gestor del Canal de Denuncias de la modificación de la denuncia o aclaración de los hechos relatados si éste entendiese que la información redactada por el denunciante no es lo suficientemente descriptiva para iniciarse la investigación. En ese caso se otorgaría un plazo máximo al interesado para realizar los cambios exigidos y, de excederse la fecha límite, la denuncia pasaría a ser archivada.

Por último, tampoco serán admitidas a trámite denuncias que manifiesten conductas o situaciones de dudosa credibilidad u opiniones y valoraciones subjetivas del denunciante sin indicios de veracidad.

CERTIFICADO COVID E INTIMIDAD ¿COMPATIBLE?

El Reglamento sobre el certificado COVID digital de la UE entró en vigor el 1 de julio de 2021. Tal certificado digital conocido como Green Pass, tiene como objetivo acreditar digitalmente que una persona ha sido vacunada contra la COVID-19, se ha realizado una prueba cuyo resultado ha sido negativo o se ha recuperado de la COVID-19.

Tal documento permite garantizar la libre circulación entre los estados miembros, evitando posibles controles como cuarentenas o pruebas adicionales, además de permitir el acceso a lugares públicos y de ocio como cines, gimnasios, restaurantes o museos dependiendo de cada estado.

Los ciudadanos pueden obtener el certificado digital solicitándolo a las autoridades nacionales competentes en materia que son responsables de su expedición. En el caso de España, los ciudadanos, deben solicitarlo, con carácter general, en su Comunidad Autónoma. Adicionalmente, el Ministerio de Sanidad emite certificados de vacunación y recuperación, únicamente en formato electrónico, cuya información está recolectada en su sede electrónica.

La aplicación de este instrumento por parte de la población ha dado origen a diferentes reflexiones y debates jurídico-éticos y sociales. Lo explicamos:

En primer lugar, debemos tener en cuenta que cuando hablamos de "Green Pass" estaremos hablando de un certificado Covid digital en el marco europeo. Este certificado tendrá "fin médico" y, como hemos visto antes, facilitará la circulación transfronteriza.

A priori, no tenemos porque alarmarnos del uso de tal medio, sobre todo si pensamos a la discrecionalidad que se brinda a los Estados Miembros y a la legitimación del Reglamento Sanitario Internacional del año 2005. No obstante, queremos enfocarnos en las problemáticas que van surgiendo al margen de la utilización de tal medio así como a sus desafíos, desde un punto de vista de la protección de datos así como de las consecuencias que se pueden desarrollar desde un punto de vista penal:

La Comisión Europea ha señalado el Green Pass contendrá "la información clave necesaria, como nombre, fecha de nacimiento, fecha de expedición, información pertinente sobre la vacuna /prueba/recuperación de la enfermedad (dependiendo del caso por el cual se está solicitando el certificado digital) y un identificados único."

En relación al primer alcance cabe señalar que los requisitos que los Estados Miembros tienen que tener en cuenta para un correcto uso legal del Certificado Covid Digital (Green Pass) está íntimamente relacionado con el principio de proporcionalidad y de ponderación de riesgos, así como a la minimización de los datos personales, con el fin de que sea garantita la privacidad del ciudadano, dando preferencia a aquellas herramientas que recojan la menor cantidad de datos.

A tal respecto la AEPD ha señalado "*La utilización para estos fines de certificados acreditativos de la situación sanitaria en relación con el covid-19 implica la necesidad de contar con una base legal apropiada que se ajuste a los principios de eficacia, necesidad y proporcionalidad, atendiendo a la existencia de otras medidas de protección que puedan resultar menos invasivas, evitando efectos discriminatorios y estableciendo las garantías adecuadas. En ese sentido, debe tenerse en cuenta que la vacunación no es obligatoria, que hay colectivos que no pueden recibir la vacuna por razones médicas o de otro tipo y que, en último extremo, el proceso de vacunación se basa en unos criterios de priorización que suponen que parte de la población aún no haya podido acceder a la vacuna*".

Además, señala que: "*Los certificados solo incluirán la información limitada que sea necesaria, que no podrá ser conservada por los países visitados. A efectos de verificación, solo se comprueban la validez y la autenticidad del certificado, verificando quién lo ha expedido y firmado. Todos los datos sanitarios permanecen en el Estado miembro que expidió el certificado digital verde*".

En resumen el uso del Green Pass debe estar justificado y el tratamiento de datos personales debe contar con base legitimadora, sin olvidar que siendo datos de matiz sanitario son también datos de carácter especial y por su sensibilidad tienen una protección reforzada.

A tal aspecto no hay que olvidar que el Green Pass es un instrumento digital, y por ende, las problemáticas que pueden surgir serán relacionadas tanto con el alcance tecnológico como administrativo.

De hecho, los certificados funcionan a través de un documento que contiene un código QR que será comprobado por la persona encargada de la labor de control que tendrá que verificar su autenticidad.

Y desde el punto de vista penal... ¿Pueden falsificarse, utilizarse los datos para usurpar la identidad, o hacer negocio con ellos?

¡Ojo con el robo de datos, la usurpación de identidad y las falsificaciones!

En efecto, es suficiente pensar en que los ciberataques han aumentado mucho durante la pandemia, por medio de delitos como

el phishing hasta aplicaciones maliciosas, con el fin de robar datos personales de las víctimas y sacar provecho. En esta ocasión, el objetivo de los cibercriminales, o hackers, es el Green Pass, ya que es un instrumento que se va a utilizar en toda Europa y permite la libre circulación de los ciudadanos. En algunos estados miembros, como Francia e Italia, además, sirve para poder acceder a sitios de ocio así que su empleo es aún mas popular. Asimismo, cuantas más organizaciones almacenen o accedan a información personal, más expuestas estarán en caso de perdida o robo de datos.

Otro de los principales problemas que se está detectando es el robo o falsificación de tal documento. En el primer caso no hay que olvidar que la información sustraída es de tipo sensible ya que son datos que merecen especial protección. (Cabe destacar que a pesar del riesgo, cierto es que en Europa al tratarse un QR digital es más complicada su falsificación, sin embargo en EEUU el certificado se otorga en papel lo que ha provocado una oleada de ventas ilegales por un precio de entre 20 y 25 $).

Tal hecho se fundamenta en la naturaleza de los datos tratados, debido a que son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

Las acciones a ejercer, entonces, pueden abarcar desde el alcance administrativo, por medio de la sanción, desde el punto de vista civil, por medio de la petición de indemnización o resarcimiento por intromisión al derecho al honor, o desde el punto de vista penal dado que estaríamos ante un delito de falsificación de documento público que se recoge el art 392.1 y se castiga con la pena de seis meses a tres años de prisión, perseguible en cualquier caso de oficio.

¿Qué hacer para evitarlo?

Sin duda alguna, lo mejor que podemos hacer para evitarlo es:

1) Ante cualquier funcionamiento anómalo lo mejor es que lo pongamos en conocimiento de las autoridades cuanto antes.

2) Tener sumo cuidado con la aplicación del móvil, ser conscientes de a quién se lo enseñamos y por qué motivo y acceder a él siempre a través de la Aplicación Android o IOS que tengamos descargada en nuestro dispositivo, abriéndola única y exclusivamente cuando lo vayamos a mostrar y cerciorarnos de haberla cerrado después para que no quede abierta en segundo plano.

3) Acceder a la aplicación siempre mediante código, Face ID, o huella digital para garantizar que en el caso de pérdida o robo del dispositivo no sea fácil acceder a la información.

EL DELITO CONTRA LA INTIMIDAD Y LA RED SOCIAL FACEBOOK EN LA SECCIÓN #JURISPRUDENCIATUITATUIT

Escarlata Gutiérrez Mayo

¿Publicar en una red social que una persona ha estado en una casa de acogida, habiendo tenido el autor conocimiento de ello por ser parte en un procedimiento judicial, constituye un delito contra la intimidad previsto en el artículo 197.2 CP?

En este caso el acusado en 2017 publicó en la red social Facebook un documento donde aparecía que su expareja sentimental había estado residiendo en una casa de acogida durante unos meses. Todo ello con la finalidad de dañar, con su difusión indiscriminada a terceros, la imagen de quien había sido su pareja.

El acusado tuvo acceso a dicho documento por figurar aportado en un procedimiento judicial en el que el mismo era parte.

El Juzgado de lo Penal condenó al acusado a 1 año de prisión y multa como autor de un delito contra la intimidad previsto en el artículo 197.2 del CP. Sentencia que fue confirmada en apelación por la Audiencia Provincial.

Interpone el letrado del condenado recurso de casación por indebida aplicación del art. 197.2 entendiendo q no proceder su aplicación ya que la información que se difunde no tiene carácter secreto, pues no afecta a datos íntimos de la denunciante y el documento llegó al acusado legítimamente.

Señala el TS q es preciso analizar tres cuestiones para ver si procede la aplicación del tipo del art. 197.2 CP:

1. Si el documento de q la perjudicada estuvo en una casa de acogida, que ha sido obtenido.
por el acusado sin que haya realizado ningún acto de apoderamiento, encaja en el tipo.

2. Si esa información puede considerarse "dato reservado de carácter personal".

3. Si es necesario que esos datos se hallen incorporados a un registro automatizado o si, por el contrario, la protección penal se dispensa también a los archivos que todavía no automatizados.

Respecto de la primera cuestión, recuerda el TS que según reiterada jurisprudencia el apoderamiento de documentos exigido

en el art. 197 CP no puede considerarse estrictamente como apoderamiento físico de los mismos.

Basta con su aprehensión virtual, de manera que el sujeto activo del delito se haga con su contenido de cualquier forma técnica que permita su reproducción posterior, como, por ejemplo, mediante su fotografiado.

Aunque el relato de hechos probados no precisa el modo en el que el acusado tuvo acceso a ese documento, está claro que accedió a él y, a la vista de su contenido, lo utilizó mediante su difusión en la red social de Facebook con el fin de erosionar la privacidad de su expareja.

En segundo lugar ¿el contenido de ese documento tiene la naturaleza de "dato reservado de carácter personal o familiar"?

El letrado del acusado entiende que no, habida cuenta que no era un dato secreto.

Si bien el TS precisa que "dato reservado de carácter personal" es un concepto normativo que ha de interpretarse conforme a la legislación protectora de ese derecho de nueva generación consolidado al amparo del art. 18.4 CE, esto es, el derecho a la autodeterminación informativa, o lo que es lo mismo, el derecho a conocer y controlar lo que los demás conocen de uno mismo. De ahí que el concepto de "datos personales" no pueda ser indentificado a efectos penales como "dato secreto".

Desde esta perspectiva, es indudable q una información referida a lo q se ha llamado la "historia social" de una persona, en la que se recogen datos que no tienen por qué ser objeto de conocimiento público, tiene cabida en el concepto normativo de dato reservado de carácter personal.

En último lugar, no es necesario para aplicar el tipo del art. 197.2 CP que el acceso y consiguiente utilización de esa información se obtuviera directamente de un archivo automatizado.

Y es que la vigente LO 3/2018, 5 de diciembre abarca en su ámbito de protección tanto a los ficheros automatizados como a aquellos otros que no tienen este carácter, al ajustar su formato a un esquema convencional, no informatizado.

En el presente caso, es más que previsible que el documento al que

tuvo acceso el acusado y que utilizó mediante su difusión en la red estuviera incorporado a un registro o fichero automatizado. Pero, al margen de la altísima probabilidad de que así fuera, lo cierto es que el acusado digitalizó ese documento, condición indispensable para su acceso a la web. Y con su inclusión en Facebook autorizó el conocimiento y utilización de esos datos por terceros.

Por todo lo expuesto el TS desestima el recurso interpuesto, confirmando la resolución recurrida.

Muy interesante el VOTO PARTICULAR que formula a esta sentencia el Magistrado Antonio del Moral, quien entiende que el recurso tendría que haber sido estimado, ya q estos hechos no encajan en el delito previsto en el art. 197.2 por los siguientes motivos:

a) El dato se obtiene legítimamente.

b) El dato no se obtiene de un fichero, ya que un expediente judicial (de donde se obtiene el documento) no puede encuadrarse en este concepto.

c) Tanto el apoderamiento como el acceso requieren siempre una conducta activa: alguien se apodera o accede. Recibir una comunicación (de forma pasiva) por ser parte en el procedimiento judicial, como ha ocurrido en este caso, no puede equipararse a "apoderarse" ni a "acceder".

Si la información no se obtiene de un fichero al que se accede por iniciativa propia, sino que se recibe, debe resultar irrelevante que se digitalice luego. Resultando estos hechos atípicos penalmente.

Personalmente, siendo muy interesante el supuesto que se plantea en esta sentencia, comparto la posición del voto particular, resultando muy complicado encajar los hechos en el art. 197.2 por no tratarse de un acceso ilícito y por no poder considerarse un expediente judicial un fichero o archivo.

RETOS FUTUROS DE LA PROTECCIÓN DE DATOS RESPECTO LA ROBÓTICA Y LA INTELIGENCIA ARTIFICIAL

Javier Antonio Nisa Ávila

1. El futuro que ya llega

La sociedad en la actualidad está de camino hacia una nueva era interconectada, interoperable y con una delgada línea entre privacidad y publicidad entendido como datos públicos vendidos o recaptados. El futuro es un lugar donde se compartirá todo a tiempo real las 24 horas y sin descanso. El auge de los sistemas de información y comunicación bajo las tecnologías de la información y comunicación (TIC), así como el Internet Of Things (IOT) y el Internet Of Robot Things (IORT) nos prepara el escenario de una nueva sociedad donde existen cada vez más herramientas de explotación y control de datos.

Partiendo de esta base tenemos que revisar el significado del concepto trabajo y lo que ello significa en el ámbito jurídico teniendo en cuenta el momento de gran evolución que está sufriendo. Los contenidos que se suben a plataformas digitales se están convirtiendo en un nuevo estilo de vida donde cualquier tipo de producto o servicio se puede convertir en una nueva forma de extraer rendimiento económico. Por ello las empresas y particulares usan estas plataformas para promocionar productos, generar contenidos directos o indirectos que tienen como objetivo un beneficio económico o simplemente compartir una serie de conocimientos de forma altruista.

Las actuales plataformas de generación de contenidos son un nuevo sistema de desarrollo laboral y social en la nueva sociedad en red. La nueva generación de ciudadanos prosumers que usan las diversas plataformas tanto de redes sociales como de generación de contenidos ha supuesto una revolución social. Las actividades y contenidos que generan los diferentes tipos de usuarios en red se están convirtiendo en nuevo medio de vida que se está enmarcando un nuevo ámbito laboral. El desarrollo de contenidos de carácter lúdico o con fines lucrativos se está afianzando como una nueva profesión a desarrollar en un futuro cada vez más cercano. El carácter que está tomando los contenidos generados por prosumers y creadores puros

de contenido son un valor generado en torno a ellos que los convierte cada vez más en un futuro pilar preeminente en la economía mundial.

Pero ello parte de la base de la necesidad de una serie de plataformas o aplicaciones donde volcar contenidos o usarlas para diversos servicios. Partiendo de esta premisa la constante tecnificación de la empresa y su ritmo de incorporación de toda clase de nuevas tecnologías a sus productos y servicios incrementan la posibilidad de fuga del know-how.

La carencia en todas las instancias jurídicas actuales, tanto nacionales como supranacionales, nos brinda un panorama que permite constatar la existencia un legislador carente de los suficientes conocimientos técnicos. La deficiencia en conocimientos genera una deficiente legislación tecnológica desde un punto de vista técnico jurídico.

La realidad nos enmarca dentro de un problema que puede conllevar consecuencias jurídicas transversales a diversos campos que extralimitan el jurídico, comenzando por futuras repercusiones sociales de profundo calado. Por ello resulta más que nunca necesario analizar el panorama jurídico actual que conlleva dicho reto y proponer soluciones y prevendas para conseguir alcanzar un futuro empresarial eficiente entre los derechos y deberes existentes entre trabajadores, empresario y consumidores.

Todo ello nos lleva hacia un cambio de paradigma social, comercial y laboral al completo y sin vuelta atrás. La llegada de las nuevas tecnologías a la vida cotidiana y profesional nos encamina hacia una sociedad basada en una tecnificación que nos permite disfrutar de nuevos servicios de todo tipo. La sociedad en red, es una realidad y nos arroja cifras en las que actualmente se generan en torno a 6.826.667 de documentos por segundo en red. Pero esos archivos no sólo son documentos, si se analizan cuando los examinamos por dentro nos encontramos con una serie de datos que son los que conforman en su conjunto a un documento (World In-

ternet Users Statistics and 2019 World Population Stats, 2019).

No obstante los datos indicados sólo son una parte de la realidad de datos que se mueven. Los datos que podemos ver a simple vista son un contenedor de datos realmente donde encontrar como si de una matrioshka se trata más datos dentro de datos. Por ello en la nueva idea fuerza en la que se basa la nueva sociedad en red son los datos dentro de los datos. Todos esos documentos, archivos, fotografías, posts o datos que subimos a internet a modo de correo o comentario en una red esconden una serie de datos denominados metadatos.

Los metadatos son la piedra de roseta del siglo XXI que va a permitir interpretar muchos datos ocultos en todo lo que se sube a la red, voluntario o involuntario. La nueva sociedad en red basada en IOT e IORT es el punto de partida real de la explotación de datos mediando el data mining. Los metadatos o datos fantasma jurídicamente definidos junto con el Big Data son los dos grandes conceptos que lo recogen todo acerca de los ciudadanos que componen la sociedad en red

Por ello **uno de los campos a analizar debe ser la regulación jurídica de la explotación de los metadatos**. La pretensión del estudio jurídico de los metadatos es la de evitar que se usen como vía discriminatoria para los ciudadanos. La necesidad de protección y cumplimiento de los contratos de uso de plataformas digitales de contenidos, aplicaciones o cualquier otro sistema de intercambio de datos donde se firman unas condiciones de uso es que se establezcan una serie de obligaciones jurídicas reales que deban cumplirse. El ritmo de vida en la actualidad nos está llevando de forma constante a la reafirmación de una nueva era interconectada entre todos los ciudadanos de la sociedad en red. La posibilidad de compartir a tiempo real todo tipo de datos entre diferentes operadores de datos como pueden ser ciudadanos, empresas, gobiernos, etc. donde el tráfico de datos y de información fluye las 24 horas y sin descanso, es un reto jurídico a tener en cuenta. El afianzamiento de sistemas de información que usan las tecnologías de la información y comunicación (TIC), y las nuevas redes de comunicación de datos basadas en el Internet Of Things (IOT) y el Internet Of Robot Things (IORT) son un grave peligro para la finalidad protectora que tiene el derecho hacia los ciudadanos. El futuro nos arrastra inevitablemente hacia una sociedad donde cada vez más herramientas de explotación y control de datos se van a imponer como herramientas de uso diario, con asunción de necesidad vital. Los algoritmos serán la pieza clave donde sustentar todo el sistema tecnológico, creando una red neuronal basadas en diferentes algoritmos que permitan una recreación y captura de datos como nunca ha sucedido.
Los algoritmos por ello son el eje principal a través del cual se vertebran todos los da-

tos del tráfico total de red. Los algoritmos se alimentan de los metadatos generados por usuarios, ciudadanos, consumidores, usuarios prosumers y usuarios creadores de contenido entre otros para mapear la vida de las diferentes sociedades mundiales.

Pero uno de los principales problemas que nos encontramos a la hora de abordar el análisis de los algoritmos es la necesidad de adquisición de conocimientos y el sistema de gestión de los mismos respecto a cómo por parte de los legisladores se encuentra regulado. La situación actual jurídicamente se encuentra desbordada y lo que deberían ser dos campos entrelazados jurídicamente y regulados de forma armonizada entre sí, se convierte en una prioridad a legislar a futuro. La necesidad de adquirir aptitudes legisladoras que permitan que las herramientas descritas no se conviertan en un sistema de recaptación y análisis de datos libres sin control ni conocimiento para los usuarios, es una realidad fáctica que resulta necesaria abolir del negacionismo colectivo. Para ello la didáctica jurídica como concepto es más necesaria que nunca. El futuro más cercano nos está precipitando de forma cada inmediata a una nueva moneda de cambio, los datos privados y empresariales. El Data Mining es la "ciencia" que va a permitir este cambio de paradigma como herramienta metodológica asociado al principal concepto contenedor; el "Big Data". El Big Data se encuentra íntimamente asociado a los algoritmos, puesto que el Data Mining es la metodología, los metadatos son la fuente de alimentación y los algoritmos se vislumbran como la nueva herramienta que permitirá exprimir ante la nueva fiebre del oro que se avecina con todos datos vinculados a usuarios de diferentes aplicaciones. La capacidad de aislar datos con una mayor proyección de explotación económica de los que no lo son genera una necesidad regulatoria que se suma a las ya citadas. El futuro sistema económico se basará en herramientas con capacidades vinculadas a sistemas de inteligencia artificial y robótica, lo que va a suponer un reto jurídico.

El posicionamiento de contenidos que estos algoritmos ejecutan tras realizar tareas de Data Mining dentro del concepto "madre" de Big Data, debería tener una total ausencia de sesgos de cualquier tipo y construir un sistema mundial que permita con absoluta certeza que ningún ciudadanos va a ser discriminado o favorecido respecto a otro por los datos vertidos en red o los analizados en estas.

Pero el principal problema se basa en la inexistencia de regulación jurídica respecto al concepto algoritmo.

Las plataformas y aplicaciones usan a los algoritmos para realizar estudios de Data Mining personalizando el perfil de cada ciudadano de forma poco clara y transparente. Por ello existe una vis discriminatoria en relación a las clausulas contractuales estándar actuales respecto a la realidad de datos que se explotan.

Pero la realidad es que el principal problema lo tenemos en lo que protección de datos se refiere de forma genérica, por los diversos frentes legales abiertos derivados de la explotación de datos basados en algoritmos que usan metodología de Data Mining para analizar datos y metadatos. Los metadatos son datos no visibles y se encuentran alrededor de todos los datos esenciales y necesarios para el desarrollo de los objetivos de las plataformas digitales; son el principal objetivo de análisis jurídico en lo que a la discriminación de contenidos en plataformas se refiere. Los datos que se encuentran ocultos son los llamados elementos meta o conocidos como metadatos, que no son otra cosa que datos automatizados o generados por programas o algoritmos, enmarcado todo ello bajo el concepto jurídico de datos fantasma o ghostdata. Los metadatos o jurídicamente denominados ghostdata y son el pilar fundamental sobre el que se basa el futuro transaccional comercial de las plataformas digitales. La capacidad que tienen los ghostdata de recrear a tiempo real la vida de los usuarios de las plataformas digitales es tan precisa que debe ser regulada jurídicamente con urgencia y bajo supervisión continua.

Asimismo nos cabe resaltar que nos estamos refiriendo exclusivamente a datos dentro de transacciones informatizadas, en forma de archivo, email, documento, fotografía, etc, cualquier acción que se realice en una red o aplicación. Por ello si partimos de esa base como luego se verá, el RGPD no protege a los ciudadanos ni usuarios, sean empresas o personas físicas. **El RGPD aunque establece al ciudadano como sujetos pasivo a ser protegido no establece mecanismos efectivos para cumplir dicha pretensión**. Los sujetos pasivos se encuentran con la existencia de algoritmos que leen correctamente los metadatos generados por aplicaciones, páginas web o diferentes aparatos electrónicos lo que supone poder llegar a conocer muchos datos importantes a nivel de datos privados de un usuario.

Por lo que se refiere a la metodología empleada a lo largo de todos los capítulos si la examinamos más a fondo y la desglosamos teniendo en cuenta los elementos investigados se ha usado una metodología dialéctica y fenomenológica respecto al análisis socio-jurídico. El uso de la metodología dialéctica junto con la jurídico-proyectista pretende poner énfasis en los supuestos de hecho opuestos dentro del análisis efectuado de forma simultánea lo que supone al mismo tiempo, la búsqueda de una trascendencia jurídica en base a la finalidad de la investigación y respecto a la fusión de diversos conceptos jurídicos contrarios pero con el único objetivo que nos ayude a aclarar la estructura actual y certera existente aunque sea de forma indirecta entre los conceptos analizados aunque parezcan contrarios. (Míguez Passada, 2014). La metodología fenomenológica que usamos junto a una metodología hipotético-deductiva impulsado por un método inductivo-comprensivo para los aspectos sociales que interactúan con la legislación pretende mediante un análisis general partiendo de ciertos casos particulares ser

capaz de construir a través del método inductivista un sistema lo suficientemente eficiente como para ser considerado apto para aplicarse a las leyes de un modo científico con la finalidad de ponerlas a prueba para localizar mediante un razonamiento alcanzar una predicción sobre lo no contenido expresamente en la norma pero pretendido por el legislador (Fuster Guillen, 2019). Por último para el ámbito más puro del derecho, entendido como derecho natural aplicable a todos los ámbitos investigados, se aplica de forma transversal para todos los campos, como metodología principal apoyada en las anteriores, un método hipotético-deductivo para el ámbito de interpretación legal y creación legislativa el cual a través de la observación del fenómeno estudiado se encuentre mediante la creación de una hipótesis jurídica coherente una explicación científica al fenómeno descrito en los objetivos previos mediando la deducción de las posibles consecuencias o propuestas ejecutadas desde la propia hipótesis con la finalidad de encontrar los supuestos de hecho para el constructo jurídico más elemental del objeto investigado (Klimovsky, 1971).

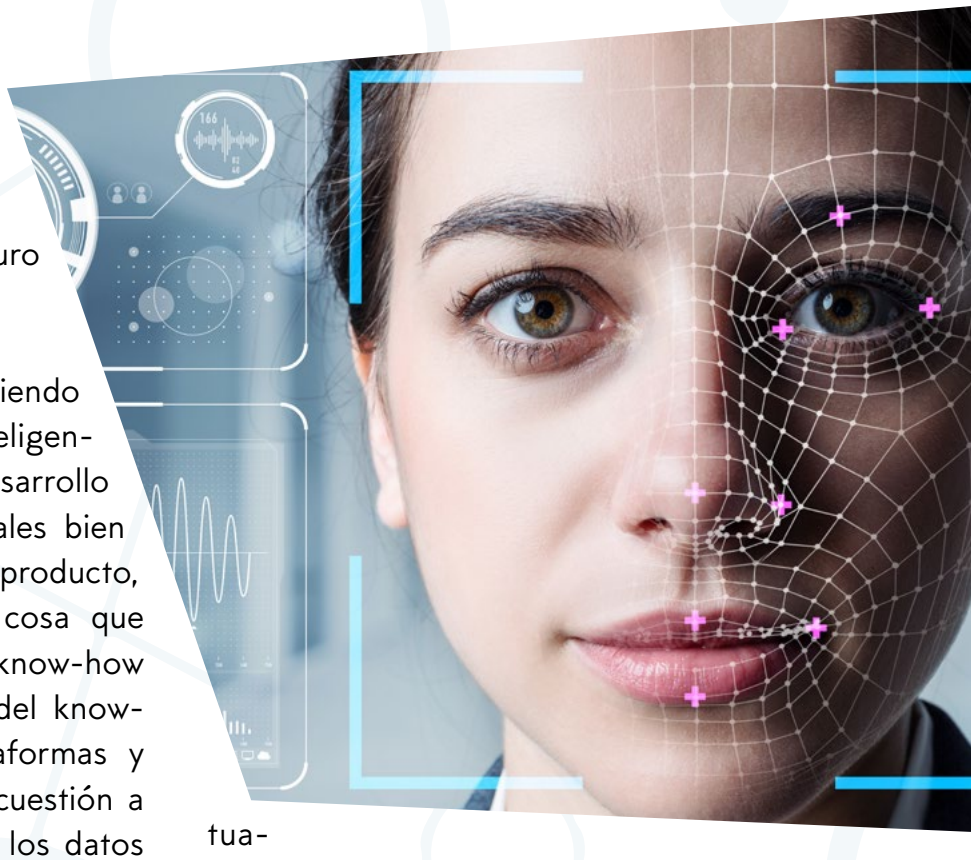
Por todo lo anterior podemos observar la verdadera importancia de las nuevas tecnologías y las nuevas técnicas de explotación y análisis de datos y su posible inferencia la gestión y uso de las plataformas digitales. Las nuevas tecnologías son herramientas que nos permiten generar nuevos productos o servicios tecnológicos basados en sistemas telemáticos y procedimientos internos de tratamiento y gestión de datos totalmente informatizados y automatizados. El uso de las plataformas digitales en el actual contexto de sociedad en red genera una serie de metadatos que pueden permitir a quien sepa leerlos e interpretarlos averiguar secretos de la vida privada de cada usuario sin necesidad de transgredir ninguna legislación. La posibilidad de crear contenidos a la carta no es jurídicamente incorrecto, siempre y cuando se encuentre todo dentro de un contrato entre las partes y dependiendo del tipo de plataforma, si es de pago, gratuita o pago bajo demanda.

2. Definiendo el futuro jurídico de la Inteligencia Artificial

La legislación en materia de Inteligencia Artificial no puede ser única y solo basarse un en único precepto.

El futuro jurídico de la Inteligencia Artificial pasa por un proceso de codificación que unifique el máximo de puntos de vista jurídicos sobre un sólo lugar.

Pero el eje principal de todos ellos deber ser al referente a la materia de protección de datos. La protección de datos juntos con los derechos civiles se tiene que convertir en los ejes principales que establezcan los pilares básicos jurídicos sobre los que fundamentar el resto de legislaciones satélite espe-



cializadas que compongan ese futuro códice.

Por un lado en primer lugar partiendo de la base que el futuro de la inteligenciar artificial se encuentra en el desarrollo privado de soluciones empresariales bien como bienes y servicios o como producto, se debe recoger jurídicamente, cosa que ahora no sucede, el concepto de know-how y know-howtech. La protección del know-how respecto aplicaciones, plataformas y servicios digitales debe ser una cuestión a tener en cuenta. Pues si siempre los datos han sido un bien preciado, en el futuro lo va a ser aún más, no sólo por cuestiones relativas a protección de datos tradicional sino también por conceptos vinculados a la de protección de conocimientos empresariales respecto a la inversión realizada en materia de recaptación de datos en base al desarrollo de nuevas tecnologías protegidas bajo el paraguas conceptual derivado del know-how denominado know-howtech. La capacidad de extracción de datos de una empresa aumenta exponencialmente según avanza la tecnología. La diferencia entre un producto o servicio con éxito radica en sus particularidades y su tratamiento comercial respecto al know-howtech de una empresa. Ahora por otro lado se avecina una nueva era donde el know-howtech como nuevo concepto jurídico va a emerger.

El know-howtech va a ser el gran secreto de todas las empresas, pues los productos virtuales, productos físicos y servicios virtuales y físicos, van a estar hibridados sirviéndose simultáneamente a los consumidores tanto por parte de las empresas como de las administraciones. La supervivencia empresarial en un mundo tecnificado se vale del conocimiento exhaustivo de sus usuarios.

Por ello y teniendo en cuenta las precisiones realizadas, podemos pasar a definir conceptualmente **el know-howtech como el conjunto de datos almacenados o en uso, de base tecnológica, bajo forma de paquetes de datos o datos independientes** que usados en su conjunto o examinados en conjunto forman los conocimientos necesarios que posteriormente bajo el uso de técnicas y aptitudes necesarias se convierten en el know-how industrial o empresarial cumpliéndose el objetivo con el correcto uso o aplicación del mismo para fines comerciales o de ejecución de servicios tanto físicos

como de base tecnológica, convirtiéndose el know-howtech en la base primigenia de conocimientos de los productos o servicios ofertados independientemente de que sean físicos o virtuales.

Por otro lado una vez definido el know-howtech, debemos entender que **este concepto no es independiente, sino interdependiente de otros**. Al respecto podemos hablar de Big Data, como concepto clave principal sobre el que pivotarán diferentes conceptos dentro del marco que hemos estado analizando a lo largo de todos los capítulos. Por ello el Big Data desde un punto de vista jurídico, se compone de una serie de conceptos núcleo que entre todos ellos forman el denominado Big Data. Los conceptos jurídicos núcleo del Big Data son cuatro; tecnología, métodos, información e impacto.

- La tecnología como primer concepto jurídico núcleo del Big Data se puede definir jurídicamente como el uso de una concreta y precisa tecnología que permite de forma adecuada y en base a unos servicios propuestos alcanzar un fin ulterior primerio en base a una serie de competencias analíticas con el objetivo de usar dicha base tecnológica organizar y vertebrar datos con fines de explotación.

- Los métodos son el segundo concepto jurídico núcleo se definiría como el conjunto de reglas metodológicas que se usan para extraer y ejecutar diferentes análisis de información que permiten conocer de forma más depurada los datos recaptados con el fin de alcanzar un objetivo primario establecido por un tercero responsable de un servicio a través del análisis de datos con el fin de conseguir un impacto asociado a una rentabilidad directa o indirecta.

- La información es el tercer concepto jurídico núcleo del Big Data y se basa en la organización de la información obtenida en el segundo concepto núcleo bajo parámetros más complejos con el fin de extraer y transformar los datos obtenidos convirtiéndolos en información delimitada bajo unos parámetros concretos de búsqueda y reconstrucción de información en base a los datos obtenidos y con el fin de alcanzar el objetivo primario de Big Data.

- El impacto es el cuarto concepto jurídico núcleo, mediante al cual podemos asociar el concepto valor a la información obtenida gracias a la aplicación de los tres primeros conceptos núcleo con el fin de extraer rentabilidad bajo cualquier prisma respecto a la información final.

Partiendo por lo tanto de los diferentes conceptos jurídicos núcleo que forman el concepto Big Data, si definimos el concepto Big Data desde un punto de vista jurídico; lo podríamos definir al Big Data como aquel conjunto de información en constante actualización debido a que su estructura conceptual se basa en el análisis de grandes

cantidades de datos que cambian en tiempo real bajo una tipología diversa que requieren de una tecnología de explotación específica en base a una serie de métodos de explotación analíticos concretos y con el fin de obtener mediante la transformación de esos datos una serie de conclusiones con un valor específico en base a procesos analíticos con relevancia para el tratador de dichos datos mediante Big Data.

Por otro lado tenemos otro déficit normativo dentro de la actual legislación, que es el metadato como tipo de dato con suficiente relevancia como para tener autonomía jurídica. El metadato es una palabra compuesta de dos palabras "meta" y "dato" el cual se enmarca jurídicamente como una de las subcategorías dentro del concepto de "Datos No Normalizados". Los datos no normalizados son aquellos conjuntos de datos que se componen de una serie de elementos técnicos o tipos de datos denominados "Meta" existentes en todo archivo digital y que se encuentran dentro de los "Datos Normalizados", de ahí la palabra "metadato", un dato dentro del dato.

Para ello estos elementos Meta dentro de los datos no normalizados, o metadatos; no pueden ser visibles y deben contener una serie de datos clasificados en diferentes categorías que muestren una serie de información única y exclusiva, adicional o complementaria a la contenida en el archivo, dato o conjunto de datos transmitidos principalmente. La finalidad del metadato no es otra que obtener más información en relación al contenido del archivo transmitido, ampliando la información principal, para además poder vincularla con otros datos no relacionados.

El concepto de metadato ha evolucionado junto con la tecnología a la que iba asociado y se ha ido ampliando con nuevas categorías y subcategorías de elementos meta. **La creación de nuevos metadatos cada vez más complejos ha añadido complejidad al propio metadato en sí, alcanzando casi una nueva categoría propia dentro del metadato que podríamos denominar ultradato**. No obstante y partiendo del concepto más técnico desde un punto de vista de ingeniería se deben incluir nuevas características al concepto metadato (Senso & Rosa Piñero, 2003).

Por todo ello y partiendo desde un punto de vista jurídico, una vez definido los "Datos No Normalizados" podríamos establecer una definición jurídicamente estandarizada sobre el concepto metadato. Conceptualmente el metadato sería el conjunto de datos no normalizados, no visibles y ubicado dentro de los datos normalizados de un archivo o independiente a éste, con la finalidad de obtener información adicional o exclusiva sobre el contenido del mismo bajo la condición de que sea totalmente interoperable y explotable respecto al operador pero inmutable para el usuario operante.

Para finalizar indicaremos que **existen tres tipos básicos de metadatos, los descriptivos, los estructurales y los administrativos** (Lamarca Lapuente, 2006).

Asimismo otro problema del legislador lo encontramos a la hora de definir que es el Data Mining. El Data Mining se encuentra enmarcado dentro de un campo multidisciplinar cuyo objetivo no es otro que el establecimiento de una metodología que permita discriminar que datos generados pueden parecer a priori relevantes e irrelevantes teniendo en cuenta el objetivo de un análisis de datos concreto. La idea de mining proviene precisamente de la dedicación que se necesita, siendo un paralelismo con el trabajo que se realiza en una mina para localizar un determinado material.

El data mining es una subcategoría del concepto matriz Knowledge Mining from Data, el cual realmente estructura 7 procesos diferentes con los cuales se pretende alcanzar el objetivo de extraer datos relevantes para diferentes usos. El proceso más importante que conforma este Knowledge Mining from Data es el data mining (Kamber, Pei, 2011)

Por último nos encontramos con un concepto imprescindible dentro del ordenamiento jurídico de cualquier país, el algoritmo. Los algoritmos por otro lado son el último de los conceptos a definir y uno de los principales aglutinantes de todo lo anterior. El algoritmo es la herramienta que gracias a la metodología del Data Mining consiguen explotar el contenido de los metadatos existentes en los diferentes archivos digitales derivados de un know-howtech se enmarca dentro de un proyecto de explotación de datos de Big Data para la consecución de una serie de objetivos por parte de un prestador de servicios. Por ello un algoritmo se puede entender desde un punto de vista técnico como una secuencia concretamente definida de reglas (operaciones) que indican la forma de cómo producir un resultado concreto (output) mediante la entrada de una serie de datos o inputs usando una serie de pasos concretos que pretender alcanzar el output indicado.

Por ello un algoritmo al cual se le aplica una metodología de data mining para la explotación de una serie de datos **podemos verlo como una red neuronal de explotación automatizada**. Las redes neuronales se basan en los principios de procesamiento distribuido en paralelo o PDP mediante mecanismos computacionales basados en percepciones para la clasificación de información (González-Ruiz, Gómez-Gallego, Pastrana-Brincones & Hernández-Mendo, 2015) .

El algoritmo desde un punto de vista jurídico podríamos definirlo como una serie de instrucciones síncronas y asíncronas a través de las cuales se ejecutan una serie de procesos automatizados que pretenden dar respuesta a un objetivo preestablecido mediante

una serie ordenada y concreta de pasos automatizados que pretenden resolver un problema para tomar una decisión que ayude a alcanzar un objetivo preestablecido.

Un ordenamiento jurídico debe tener como objetivo vertebrar el orden social y proteger a todos los integrantes de la sociedad a la que pertenece. El ordenamiento jurídico y las leyes que lo componen no tienen otra finalidad que organizar la sociedad. El orden no se impone sino que se protege, ese es el fin del derecho poder ofrecer soluciones ante conflictos y generar sistemas de cumplimiento positivo o negativo. **Las nuevas tecnologías que integran sistemas de inteligencia artificial, necesitan no de una modificación de las actuales leyes para integrar todos los conceptos, sino de una nueva generación legislativa**. La historia en un futuro nos enmarcará dentro de un contexto de revolución industrial, por ello los juristas y legisladores deben estar a la altura de ese reto, para quedar como los que vertebraron el proceso protegiendo a la sociedad en la transición hacia un nuevo orden social integrado por la robótica y la inteligencia artificial.

BIBLIOGRAFÍA

Fuster Guillen, D. (2019). Investigación cualitativa: Método fenomenológico hermenéutico. Consultado el 7 Noviembre 2020.

Han, J., Kamber, M., & Pei, J. (2011). Data mining concepts and techniques third edition. Morgan Kaufmann.

González-Ruiz, S.L., Gómez-Gallego, I., Pastrana-Brincones, J.L., & Hernández-Mendo, A.. (2015). Algoritmos de clasificación y redes neuronales en la observación automatizada de registros. Cuadernos de Psicología del Deporte, 15(1), 31-40. https://dx.doi.org/10.4321/S1578-84232015000100003

Klimovsky, G. (1971). El método hipotético deductivo y la lógica. Cuadernos Del Instituto De Lógica Y Filosofía De Las Ciencias. Serie-celeste, 1. Consultado el 7 Noviembre 2020.

Lamarca Lapuente, M. (2006). Hipertexto: El nuevo concepto de documento en la cultura de la imagen. (Doctorado). Universidad Complutense de Madrid.

Miguez Passada, M. (2014). Metodologías de investigación desde la razón dialéctica. Revista Latinoamericana De Metodología De La Investigación Social., 7(7), 7-18. Consultado el 7 Noviembre 2020.

Senso, J., & Rosa Piñero, A. (2003). El concepto de metadato: algo más que descripción de recursos electrónicos. Ciência Da Informação, 32(2), 95-106. doi: 10.1590/s0100-19652003000200011

World Internet Users Statistics and 2019 World Population Stats. (2019). Consultado el 18 February 2020, de https://bit.ly/3k7sHbj

LOS DELEGADOS SINDICALES NO TIENEN DERECHO A QUE LA ADMINISTRACIÓN LES CEDA DATOS PERSONALES DE LOS TRABAJADORES DEL HOSPITAL SIN JUSTIFICACIÓN

Vicente Lomas Hernández

El Alto Tribunal (STS nº 160/2021, rec. 1229/2020) se pronuncia sobre el recurso de casación en el que se plantea la siguiente cuestión:

<< (...) si es contrario al derecho fundamental de la libertad sindical (art. 28.1 CE) denegar por razón de la normativa sobre ***protección de datos*** *, información sobre nombramientos estatutarios de personal facultativo, especificando el tipo y fecha de inicio de prestación del servicio e incluyendo tanto los nombramientos por "acumulo de tareas" como las "sustituciones" y otras plazas "no estructurales" >>.*

Los hechos:

Solicitudes de los delegados sindicales de la Organización Sindical O'Mega-Médicos de Galicia Independientes, y del Sindicato de Médicos de Galicia (SIMEGA/CESM GALICIA) de información y documentación en las que se exponía que "*en base al derecho a la información que nos asiste como representantes sindicales de esta área sanitaria la relación de los contratos de todos los facultativos de cada servicio, especificando nombre, tipo de contrato actual y fecha de inicio del mismo, incluyendo en este registro además de los contratos estructurales, todos aquellos no estructurales: "acúmulo de tareas", "obra y servicios", "sustituciones", etc... que pueda haber suscrito la EOXI con los facultativos del área*".

Posteriormente solicitaron también que se facilitaran, respecto de la cirugía y consulta "autoconcertada" de la EOXI de Santiago de Compostela, la tarifa del proceso quirúrgico y por facultativo, la tarifa global por proceso quirúrgico y la tarifa por consulta y servicios. Así como la reiteración de la solicitud sobre la documentación que acredite la fecha de inicio de la prestación del servicio de los nombramientos estatutarios de todos los facultativos por servicio, incluyendo los nombramientos por "acúmulo de tareas", las sustituciones y las plazas "no estructurales".

El criterio del TS:

No genera dudas que- como muy bien precisa la Sentencia- estamos ante datos de carácter personal, pues "*los datos relativos al nombre y apellidos, tipo de puesto de trabajo, o el inicio de la prestación no disociados de aquél, son datos, que aunque no sean íntimos, están protegidos por la citada Ley Orgánica de Protección de datos de carácter personal de 1999*" (vigente en la fecha de los hechos).

En este contexto (libertad sindical vs protección de datos personales), el TS desestima el recurso de casación interpuesto por las mencionadas organizaciones sindicales. El argumento central es que tanto el Estatuto Básico del Empleado Público, como la Ley Orgánica de Libertad Sindical, y el Estatuto de los Trabajadores, no prevén la cesión automática de la información solicitada, ya es preciso que conste debidamente justificada la necesidad de disponer de tales datos para el correcto cumplimiento de sus funciones sindicales, o en su defecto, se haya recabado el consentimiento de los afectados:

"Sin embargo a juicio del TS esta fudamentación legal resulta insuficiente para conceder el acceso a los datos solicitados, pues " no describen un supuesto legalmente previsto que excepcione el consentimiento de los interesados a los efectos del artículo 11.2.a) de la Ley de 1999, en un caso como el examinado en el que se solicita una cuantiosa e indiscriminada cesión de datos , sin proporcionar una mínima explicación, al tiempo de su solicitud, de la necesidad o relevancia de esos datos para el ejercicio de sus labores sindicales.

Resulta relevante, por tanto, que medie la debida relación entre los datos personales del personal estatutario que se solicitan, con la importante función sindical que se desarrolla. De modo que únicamente cuando estos datos personales son necesarios para el ejercicio de las labores sindicales, podrían considerarse excepcionados del consentimiento, pero no cuando se encuentran desvinculados o se desconozca su relación, al no haberse puesto de manifiesto su conexión con dichas funciones sindicales.

En consecuencia, la mera invocación, ayuna de justificación, de la representación sindical no puede servir de excusa para acceder a todo tipo de documentación, si no se quiere por esta vía vaciar el contenido del derecho fundamental a la protección de datos, cuando el titular de los mismos ignore el uso que se hace de sus datos , perdiendo su poder de disposición, en supuestos en los que no se justifica la concurrencia de alguna de las excepciones legalmente establecidas".

Cuestión distinta hubiera sido si la petición hubiese versado sobre la entrega de este tipo de datos personales, siendo el destinatario las comisiones encargadas de controlar y comprobar la correcta gestión de las bolsas de trabajo. En este sentido se pronunció el Informe de la AEPD nº 084069/2012, de 24 de abril de 2012, para quién la fundamentación jurídica de la respuesta afirmativa a la consulta realizada descansaba en el propio Pacto de selección de personal temporal de Instituciones Sanitarias del Sescam, al establecer que para la aprobación definitiva de los méritos los representantes sindicales presentes en dicha comisión podían acceder a todos aquellos datos de carácter personal de los trabajadores estatutarios temporales que resultasen necesarios para determinar si la autobaremación efectuada por los aspirantes era o no correcta.

A su vez la STSJ Castilla y León (Burgos) de 19-6-2009, nº 407/2009, rec. 43/2009 permitió ceder datos de contratación de trabajadores de un hospital público a un sindicato, sin necesidad de obtener el previo consentimiento de aquéllos. La fundamentación jurídica recogida en dicha resolución judicial se reproduce a su vez en la posterior STSJ Castilla y León (Burgos) Sala de lo Contencioso-Administrativo, sec. 2ª, S 28-4-2015 que también versa sobre entrega de datos de bolsa de trabajo de hospital público, y en la que se discutía si resultaba procedente que la Gerencia facilitase los datos de los trabajadores incluidos en bolsa de trabajo al delegado sindical del sindicato recurrente.

En este caso la información solicitada, a saber, la relación de trabajadores con nombramientos de carácter temporal de todas las categorías de personal estatutario con relación laboral con el citado complejo Asistencial, se enviaba mensualmente por la Gerencia a la Junta de Personal, de la que a su vez formaba parte el recurrente, alegando la Administración en apoyo de su negativa que

a) No estaba obligada a duplicar dicha información.

b) No había norma jurídica que amparase la cesión de los datos solicitados, por lo que, sin el consentimiento del interesado no es posible cederlos.

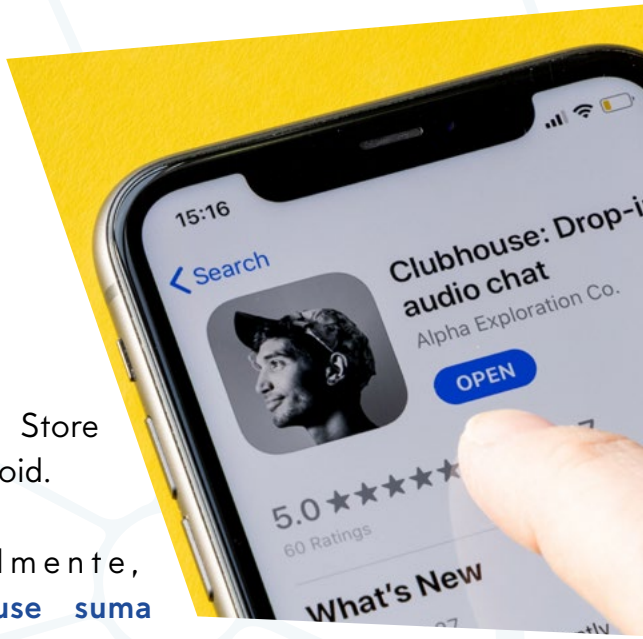
La Sala desestimó el recurso de la Administración sanitaria, pues la obligación de

ésta de garantizar el derecho a la protección de datos personales de sus empleados estaría mediatizada por las funciones atribuidas a la Junta Personal/Delegados de Personal recogidas en el entonces vigente artículo 40 de la Ley 7/07 del Estatuto Básico del Empleado Público- que se corresponden con las descritas en el actual art. 40 del actual Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público-. Según el referido precepto legal las Juntas de Personal y los Delegados de Personal, en su caso, tendrán las siguientes funciones, entre otras "a) Recibir información, sobre la política de personal, así como sobre los datos referentes a la evolución de las retribuciones, evolución probable del empleo en el ámbito correspondiente y programas de mejora del rendimiento" (...) y "Vigilar el cumplimiento de las normas vigentes en materia de condiciones de trabajo, prevención de riesgos laborales, Seguridad Social y empleo y ejercer, en su caso, las acciones legales oportunas ante los organismos competentes".

A lo anterior añade la Sentencia que conforme al art. 10.2 del EBEP- aplicable igualmente al personal estatutario- "*la selección de funcionarios interinos habrá de realizarse mediante procedimientos ágiles* ***que respetarán en todo caso los principios de igualdad, mérito, capacidad y publicidad. Está claro que la solicitud de datos formulada por el recurrente apelante en representación de la junta de personal para controlar, en el ejercicio de sus funciones, que se han respetado en las contrataciones las normas previstas, orden de la bolsa de trabajo , llamamientos etc., se refiere a datos que han de estar en el dominio público por disposición legal, para garantizar la publicidad de las condiciones de acceso a los empleos públicos a fin de poder garantizar que se cumplen los principios de igualdad***".

EL TRATAMIENTO DE DATOS EN LA NUEVA RED SOCIAL CLUBHOUSE

Jesús Ramírez Samaniego



Introducción

Desde la aparición de la Covid-19, algunas aplicaciones han cobrado especial relevancia en la vida digital de las personas, especialmente en la de los jóvenes.

Ejemplo de ello es la plataforma **ClubHouse**, la red social de chat de audios lanzada en abril de 2020. El funcionamiento de esta red social se basa en ofrecer una variedad de salas virtuales donde se puede conversar sobre diversos temas de actualidad. Por lo que fusiona algunos aspectos atractivos de productos que ya existían, como los podcasts y Twitter.

No hay presencia de cámara y únicamente pueden enviar audios y activar el micrófono aquellas personas que los moderadores decidan y previamente hayan podido registrarse gracias a una invitación privada. Estas conferencias tienen un aforo máximo de 5000 personas y sólo se podía participar desde el sistema operativo IOS de Apple, pero desde hace unos días la aplicación se encuentra en el Play Store de Android.

Actualmente, **Clubhouse suma más de 10 millones de usuarios** y ha creado un fenómeno que Twitter y Facebook no han podido obviar, pues desde el mes de marzo de 2021, Instagram (propiedad del grupo Facebook), ofrece la posibilidad de retransmitir en directo a través de la creación de una sala de hasta máximo 4 personas.

Al igual que Twitter que ha introducido en su plataforma este mismo concepto con el término "Spaces". En dicha herramienta podrás crear salas de chat públicas (sin límite de oyentes) basadas en audio.

Agora como proveedor que aloja los datos

La polémica que ha surgido en torno ClubHouse proviene de la aparición de un estudio realizado por Investigadores del

Observatorio de Internet de la Universidad de Stanford del estado de California en EEUU.

En un comunicado emitido[1], demuestran que el Gobierno chino podría acceder a los datos de los usuarios que utilizan esta red social, debido a que la compañía basa su aplicación de audio en Agora, un proveedor chino de software de voz y vídeo en tiempo real.

Agora tiene su sede en Shanghái y Silicon Valley, esto implica que su actuación esté sujeta a la ley de ciberseguridad de la República Popular China. A esta cuestión el Observatorio de Internet de Stanford recuerda que si el gobierno chino sospecha de una posible conducta criminal dentro de esta red social, que pueda poner en peligro la seguridad nacional, la empresa china estaría obligada legalmente a almacenar y localizar estos audios para ayudar a la prevención del delito.

Sin embargo, el proveedor se ha desmarcado de esta posible actuación afirmando que las autoridades no tienen acceso, no comparten ni almacenan datos personales identificables de los usuarios finales, excepto para facturar a sus clientes, (en este caso ClubHouse) y mejorar la calidad de su red.

También añaden que el tráfico de voz o vídeo de los usuarios no basados en China, incluidos los estadounidenses, nunca se enruta a través de China.

A este respecto la propia red social ha informado de la implementación de nuevos cambios en la seguridad de la aplicación para añadir encriptación y bloqueos adicionales, que eviten la transmisión de direcciones IP con datos del usuario, de la plataforma a los servidores chinos.

Elementos críticos que esconde ClubHouse

Uno de los grandes retos para la expansión de una nueva red social es definir una política de privacidad clara, segura y que cumpla con todo lo recogido en la legislación de los países en los que va a operar. En mi opinión, este es un factor determinante que puede poner en riesgo el crecimiento de una nueva plataforma, que sin duda contará con la competencia de otras redes sociales que harán lo posible por ofrecer un servicio igual o mejor lo antes posible.

Tras un análisis superficial del funcionamiento de esta aplicación y teniendo en cuenta lo que dice la legislación europea al respecto, es importante resaltar algunas cuestiones críticas que la empresa deberá paliar desde un punto de vista legal:

- El acceso a la libreta de contactos de los usuarios. Para invitar a un tercero es necesario dar estos permisos a la app y de este modo podremos realizar invitaciones, ya que

1. El comunicado emitido por la Universidad de Stanford en el que se evidencia la brecha de seguridad que puede existir debido a la relación Clubhouse-Agora: https://cyber.fsi.stanford.edu/io/news/clubhouse-china

es el único requisito excepcional de entrada para poder hacer uso de la plataforma. Este punto puede causar controversias legales a ClubHouse como sucedió con Facebook en 2016[2] al permitir crear "perfiles de sombra".[3]

- Desinformación total relativa al tratamiento de los datos que proporciona el usuario para poder utilizar la aplicación.[4]

- Falta de claridad acerca del tiempo por el cual la aplicación tratará los datos de los usuarios, en especial los audios. Por lo que no se respetan los principios de licitud, transparencia y lealtad, limitación de la finalidad o minimización de datos.

- A día de hoy, la compañía no ha nombrado todavía un representante legal en la Unión Europea.[5]

- La transferencia de datos a estados no europeos que se ha mencionado anteriormente, como era el caso de China. Inclusive a Estados Unidos, tema en el que todavía no se ha previsto ningún procedimiento para recabar el consentimiento de esta actividad específica. Ni siquiera puede utilizar **la doctrina del "Privacy Shield"**, ya que ha sido invalidado por **la sentencia "Schrems II"**.[6]

- El procesamiento de datos biométricos no tiene ninguna regulación establecida. Ejemplo de ello sería el motor de la red social, la voz de los usuarios o la huella dactilar para el login. Entrando en conflicto con el **artículo 9 del RGPD**.

- Las actividades de la propia aplicación que conlleva a la elaboración de perfiles. Estas operaciones deben respetar reglas precisas que garantiza el **artículo 22 del RGPD**.

- Por último, el aspecto que suscita más preocupación es la relación que ClubHouse mantiene con Agora y el control indirecto que puede mantener el Gobierno Chino con los datos tratados por la aplicación.

De este breve análisis podemos observar la importancia del tratamiento de los datos en la actualidad y el peligro que puede desencadenar una mala política de gestión de privacidad para el desarrollo de una idea novedosa, en este caso una nueva red social.

A esto, se suma que este tipo de aplicaciones crecen exponencialmente en cuestión de días, desarrollando un impacto internacional a corto plazo. Hecho que a su vez, supone un enorme desafío jurídico desde el punto de vista de

2. Alemania declara ilegal la herramienta de "Buscar amigos" en Facebook: https://www.audea.com/alemania-declara-ilegal-la-herramienta-de-buscar-amigos-en-facebook/
3. Los perfiles sombra se crean para almacenar información sobre los posibles usuarios interesados y notificar a estas personas para incentivar el uso de la aplicación.
4. Incumple lo dispuesto en el artículo 13 del RGPD, en el que se establece una serie de puntos a informar al usuario en el caso de haber obtenido datos personales.
5. Tal y como establece el RGPD, en su considerando 80 y el artículo 37.
6. El 16 de julio de 2020 el Tribunal de Justicia de la Unión Europea (TJUE) ha hecho pública una sentencia en la que anula la Decisión 2016/1250 de la Comisión que declaraba el nivel adecuado de protección del esquema del Escudo de Privacidad (Privacy Shield) para las transferencias internacionales de datos a EEUU. Esta Decisión sustituía a su vez a Puerto Seguro, que también fue declarado inválido por el TJUE en octubre de 2015.

regular o controlar todo lo que sucede dentro de la actividad de la propia aplicación.

En este caso nos encontramos con un medio que ejemplifica las circunstancias actuales de los fenómenos tecnológicos crecientes. **Clubhouse se desarrolla inicialmente y su sede está en Estados Unidos, depende directamente de una empresa China y, a su vez, los usuarios son ciudadanos de todo el mundo.**

Nos encontramos, por tanto, ante una nueva realidad de la que se deberá tomar consideración desde los organismos pertinentes en materia de regulación de derechos y obligaciones, ya que, hasta hace unos años, este panorama parecía inimaginable.

LA TRANSCENDENCIA TRIBUTARIA. UN LÍMITE LEGAL AL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS PERSONALES

María Prendes Valle

Introducción

Hace más de 100 años, cuando se promulgó en Estados Unidos, el primer impuesto federal que gravaba la renta del país para financiar la Guerra Civil, el Congreso estipuló que todas las declaraciones deberían estar «abiertas a examen». Al interpretar por escrito esta instrucción, el Departamento del Tesoro admitió que «todas y cada una de las personas» podían inspeccionar las listas de impuestos. Inicialmente, este ejercicio de transparencia fue aplaudido incluso por el mismo New York Times, no obstante, unos años más tarde este periódico acabaría denunciando la divulgación de estas declaraciones al entender que eran ofensivas y objetables. Era el año 1869.

Este tributo menos longevo que su coetáneo americano nace en España en 1977 como consecuencia de la formalización de los Pacto de Moncloa, en un empeño por tratar de modernizar lo que hasta el momento era un sistema fiscal anacrónico e ineficiente. Hoy en día, el Impuesto de la Renta de las Personas Físicas, es, sin duda, una de las claves de bóveda del sistema fiscal dada su importante recaudación, aunque no es el único. Lo que merece destacar es que inicialmente y durante dos años, el impuesto se configuró de tal modo que cualquier ciudadano podía tener acceso a la información fiscal mediante una simple consulta en las sedes de Hacienda. No obstante, esta práctica se suprimiría cuando el empresario Luis Suñer, el español con más ingresos según la primera lista confeccionada por Hacienda, fue secuestrado por ETA. Era el año 1981.

Hasta aquí, solo se pretende reseñar una simple anécdota de la tensión que ha generado y genera el conflicto de diversos principios antagónicos en el ámbito tributo, cuales son el derecho a la intimidad o la protección de datos, la publicidad o divulgación de los mismos y la obligación de contribuir a los gastos públicos mediante un sistema tributario justo.

En nuestro caso, se trata de la colisión entre preceptos arraigados en el texto constitucional. Por el contrario, en otros países, como en Estados Unidos, ni la privaci-

dad, ni el derecho a la divulgación están explícitamente protegidos por la Constitución, aunque ello no ha impedido reconocer sus connotaciones constitucionales. De modo que en uno u otro caso, las raíces constitucionales del enfrentamiento no se pueden desdeñar.

Dicho lo anterior, merece destacar que el debate sobre esta confrontación constitucional ha generado una importante normativa y cosecha jurisprudencial que ha permitido concretar los criterios, gracias a los cuales se puede ponderar la prioridad de uno u otro derecho, atendiendo a las circunstancias del caso. Estas líneas se limitan únicamente a precisar los parámetros de actuación más esenciales que se han venido dictando en esta materia.

Derecho a la intimidad y derecho a la protección de datos

Ciertamente, cuando se presenta una declaración de impuestos, ya sea el Impuesto sobre la Renta de las Personas Físicas, el Impuesto sobre el Valor Añadido, el Impuesto sobre Sucesiones y Donaciones o cualquier otro, se facilita una auténtica amalgama de datos propios y de terceros. Pensemos por ejemplo, en una deducción por arrendamiento a menores de 30 años reconocida en el impuesto de la renta, una clínica de estética que efectúa distintas tipos de operaciones quirúrgicas, cuando algunas de ellas pueden ser operaciones exentas en el IVA o un requerimiento de información a una entidad de seguros para que facilite el nombre de suscriptores y beneficiarios de determinadas pólizas.

La vulneración del derecho que aquí se estudia tiene su base normativa en el art.18.1 de la Constitución (CE) -**EDL 1978/3879**-. El derecho a la intimidad como derecho fundamental se encuentra estrictamente vinculado a la propia personalidad y deriva directamente de la dignidad de la persona que reconoce el art.10 CE. Se trata de admitir y reconocer la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, pues sólo así y dadas las pautas sociales, se puede garantizar una calidad mínima de vida humana[1].

1. STC 231/1988, de 2 de diciembre -EDJ 1988/547- ECLI:ES:TC:1988:231. En esta Sentencia se abordó la titularidad y alcance de los derecho a la imagen y a la intimidad personal y familiar reconocidos en el art.18 CE -EDL 1978/3879-, a propósito de ciertas imágenes relacionadas con la muerte del torero don Francisco Rivera, a consecuencia de las heridas causadas por un toro en la plaza de Pozoblanco.

Pero junto a este derecho fundamental, debemos incluir en su misma dimensión pero con distinto alcance, el derecho a la protección de datos sobre la base del art.18.4 CE -**EDL 1978/3879**-. El Tribunal Constitucional en la STC 292/2000 de 30 de noviembre -**EDJ 2000/40918**-, ECLI:ES:TC:2000:292 se encargó de perfilar las diferencias sustanciales con el derecho a la intimidad, de modo que si el derecho a la intimidad garantiza un ámbito de la vida personal y familiar reservado al individuo, el derecho a la protección de datos reconoce a la persona, un poder de control sobre la información personal, esto es, sus datos personales, uso y destino.

En concreto, el contenido de este segundo derecho consiste «en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.»

La exposición de motivos de la derogada LO 5/1992, de 29 octubre, de regulación del tratamiento automatizado de los datos de carácter personal -**EDL 1992/16927**- se refería a la privacidad, a propósito de las técnicas de recolección y almacenamientos de datos, entendiendo que protegía una esfera más amplia y global que la intimidad, pues abarcaba un conjunto de facetas de su personalidad que permitían construir el retrato del individuo.

En este sentido, el derecho a la intimidad y a la protección de la esfera de privacidad o según el término americano «the right to be let alone[2]» ha obtenido un amplio reconocimiento en la esfera constitucional de nuestro ordenamiento jurídico, tanto en su faceta individual como social, pues no se puede obviar que el libre desarrollo de la personalidad incentiva la participación del individuo y con ello, se fortalece la sociedad democrática. Es decir, ambos derechos como exponentes de la dignidad de la persona participan no sólo de una dimensión individual sino también co-

2. La expresión «the right to be let alone» fue reformulada en el estudio titulado «The Right to Privacy», en la Harvard Law

lectiva en la medida en la que fomentan la paz y el orden social al que se alude en el art.10 CE -**EDL 1978/3879**-.

No obstante, el reconocimiento del derecho a la intimidad y más en concreto de la protección de datos depende de su conciliación con otro bien constitucionalmente protegido, cual es, en el presente caso, la distribución equitativa del sostenimiento de los gastos públicos (art.31 CE -**EDL 1978/3879**-). El deber de contribuir que se impone a todos los ciudadanos avala tanto la situación de sujeción a la Administración tributaria, como la legitimación de su actividad inspectora y comprobadora, ya que de otro modo se produciría una distribución injusta de la carga fiscal, o tal como mencionaba el propio Tribunal Constitucional, «lo que unos no paguen, debiendo pagar, lo tendrán que pagar otros con más espíritu cívico o con menos posibilidad de defraudar»[3].

Por otra parte, es jurisprudencia del Tribunal de Justicia, la que reconoce que los datos fiscales constituyen «datos personales» puesto que se trata de información sobre una «persona física identificada o identificable»[4].

La plasmación de este conflicto se refleja también en la normativa. En clave nacional, se debe destacar la actual LO 3/2018, de 5 diciembre, de Protección de Datos Personales (LOPD) -**EDL 2018/128249**-, que pretende la adaptación de la regulación existente hasta el momento al reciente acervo comunitario.

En clave internacional, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental reconocido en el art.8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea -**EDL 2000/94313**- y en el art.16, apartado 1, del Tratado de Funcionamiento de la Unión Europea -**EDL 1957/52**-. Asimismo, el desarrollo de este reconocimiento, lo podemos encontrar en la actualidad en el Reglamento 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas -**EDL 2016/48900**- en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RPTD) y que vino a derogar la anterior Dir 95/46 -**EDL 1995/16021**-. Por otro lado, la protección del respeto a la vida privada y familiar tiene su base en el artículo 7 de la Carta -**EDL 2000/94313**-.

Review en 1890 por los abogados Samuel D. Warren y Louis D. Brandeis. La importancia de este ensayo radica en que originó en el sistema jurídico norteamericano, una preocupación colectiva en torno a la privacidad como fundamento de un Estado democrático.
3. STC 110/1984, de 26 de noviembre -EDJ 1984/110-. ECLI:ES:TC:1984:110.
4. STJUE 1-10-15, Bara y otros, C-201/14 -EDJ 2015/168879-, EU:C:2015:638, apartado 29.

Ahora bien, cualquiera que sea el ámbito de la regulación, se ha venido admitiendo que el derecho a la protección de datos personales, al igual que ocurre con el derecho a la intimidad no es un derecho absoluto, sino que se debe procurar su equilibrio con otros derechos fundamentales, de conformidad con el principio de proporcionalidad. De este modo, es interesante recalcar que expresamente el RPTD autoriza la utilización de datos personales, cuando se trata de autoridades públicas como las fiscales, aduaneras u organismos de supervisión de los mercados financieros y estos actúan en el ejercicio de su actividad gracias al suministro de determinados datos.

A raíz de lo expuesto, nos podemos preguntar qué datos puede manejar la Administración tributaria. La derogada LO 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal (LOPD) -**EDL 2018/128249-**, disponía en su artículo 7.3 una previsión concreta de aquellos datos de especial protección, cuando mencionaba lo siguiente:

> ***Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.***

La literalidad del precepto consignaba expresamente dos supuestos que avalaban la posibilidad de recabar aquellos datos especialmente sensibles: una disposición legal o el consentimiento expreso. Por el contrario, la nueva ley no incluye ningún artículo semejante, aunque el Reglamento comunitario, que es directamente aplicable, alude al tratamiento de categorías especiales de datos personales en su artículo 9, cuando señala que:

Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

De nuevo establece como excepciones entre otras el consentimiento explícito o razones de interés público esencial entre las que se incluyen expresamente las obligaciones existentes en el ámbito fiscal.

Por otro lado, el art.93 de la Ley General Tributaria (LGT) -**EDL 2003/149899**- consagra la obligación de proporcionar a la Administración tributaria toda clase de datos, informes, antecedentes y justificantes siempre que tenga transcendencia tributaria y se encuentren relacionados con el cumplimiento de las obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras. Este mandato imperativo se impone en particular a retenedores, obligados a realizar ingresos a cuentas, en-

tidades bancarias en relación con las cuentas bancarias, valores...

La pregunta que debemos realizar es sencilla ¿puede entonces el profesional impugnar su acuerdo de liquidación sobre la base de la vulneración de la protección de datos de sus clientes?

En definitiva, las circunstancias del caso obligan en cada supuesto a contraponer con rigor el derecho a la protección de datos, con la necesaria actividad realizada en el ámbito de la Administración tributaria, máxime teniendo en cuenta las excepciones consistentes en el consentimiento expreso y la existencia de una disposición legal que ampara la actuación de una investigación fiscal.

Consentimiento expreso

En primer lugar, en torno al consentimiento expreso, ha de significarse que según el art.93.4 LGT -**EDL 2003/149899**- (antiguo artículo 111. 5 de la Ley 230/1963 -**EDL 1963/94**-) el deber de los profesionales de facilitar información (médicos, abogados, agentes de la propiedad...) se limita a aquella con trascendencia tributaria, por lo que no alcanza a los datos privados no patrimoniales que conozcan por razón de su actividad y cuya revelación atente al honor, la intimidad personal y familiar de las personas o la protección de datos.

A propósito de la relación médico-paciente, el precepto originario fue interpretado ya por nuestro Tribunal Supremo en sentencias tales como la STS de 2 de julio de 1991, en el sentido de que se pueden facilitar los datos personales de los clientes y de facturación, pero no la historia clínica, el tipo de exploraciones, el diagnóstico, el tratamiento y las intervenciones que puedan orientar sobre la naturaleza del padecimiento o desarreglo que haya motivado la actuación profesional.

Ahora bien, debe insistirse que dicho precepto disciplina las complejas relaciones entre el deber de colaboración con la Administración tributaria por un lado, y el derecho-deber de guardar secreto de un profesional, como por ejemplo un médico, a quien le resulta exigible no revelar información que atente a la intimidad o al honor de sus pacientes.

Más si el mencionado paciente quien ha sido requerido para aportar información que sólo a él le atañe y que sirve de base para el cálculo de las ganancias del profesional, no formaliza ninguna objeción al requerimiento, no puede pretender después el profesional excluir los datos proporcionados voluntariamente por su propio paciente, pues, en primer lugar, debe recordarse que los derechos fundamentales tienen un contenido personalísimo, cuya defensa e invocación compete exclusivamente a su titular.

A modo de ejemplo, si un paciente responde al requerimiento, manifestando la cantidad que abono a un profesional en el ejercicio de su actividad, ya se trate de una persona física o jurídica o facilita información sobre los tratamientos y operaciones en los que participo, permitiendo averiguar qué operaciones médicas se encuentran exentas o cualquier otra información ... debe constatarse la existencia de un consentimiento implícito, pues dicho consentimiento se materializa precisamente en el suministro voluntario de la información a la inspección.

Llegados a este punto, se debe destacar que no existe ninguna norma que exija que el consentimiento deba adoptar una fórmula escrita concreta, pues ni el artículo 7 del Reglamento -**EDL 2016/48900**-, ni el artículo 6 de ley, así lo exigen, únicamente se alude a una manifestación libre, específica, informada e inequívoca, ya sea mediante una declaración o una clara acción afirmativa.

La investigación tributaria

Pero a mayor abundamiento, es necesario resaltar que no es necesario ni siquiera el consentimiento de los clientes o profesionales, cuando la información suministrada se califica como de «transcendencia tributaria», pues existe tanto un precepto legal que así lo habilita (art.93.1 y 3 LGT -**EDL 2003/149899**-), como un interés público que lo reconoce (art.23 RPDT -**EDL 2016/48900**-).

La STJUE 27-9-17, C-73/16, Peter Puškár contra Finančné riaditeľstvo Slovenskej Republiky y Kriminálny úrad finančnej správy -**EDJ 2017/188341**-, ECLI:EU:C:2017:725[5], reconoció que la recaudación y la lucha contra el fraude fiscal son misiones de interés público, que avalan la injerencia en los datos. Únicamente exige que se vele adecuadamente por el respeto del principio de proporcionalidad, puesto que la protección del derecho fundamental a la intimidad a nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario. Con idéntico contenido, destaca la sentencia de 21-12-16, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartado 96 -**EDJ 2016/227785**-.

A grandes rasgos, lo que conviene retener es que esta sentencia legitima que las autoridades tributarias puedan tratar datos personales a efectos de recaudación y lucha contra el fraude fiscal, sin que medie el consentimiento de los interesados, siempre que la normativa nacional les confiera misiones de interés público y las medidas adoptadas sean efectivamente idóneas.

5. Este asunto resuelve una decisión prejudicial planteada por el Tribunal Supremo de la República Eslovaca en el marco de un litigio en el que se dirimía la inclusión del Sr. Puskár en una lista de personas consideradas como testaferros por la Dirección General de Tributos. Dicha lista fue elaborada en el ámbito recaudatorio de la Administración y debe ser actualizada por la propia Dirección, las delegaciones de Hacienda subordinadas y la Unidad de delitos de la administración tributaria.

En nuestro marco legal y en aras a proceder a un mejor examen de esta habilitación legal, conviene recordar, en primer lugar, el contenido y ubicación sistemática del art.93 LGT -**EDL 2003/149899**- que se sitúa en el Título III, relativo a la aplicación de los tributos, capítulo primero, que lleva por rúbrica «Principios Generales» en su sección tercera, dedicada a la «colaboración social en la aplicación de los tributos». Dice así el art.93 LGT:

> ***1.*** *Las personas físicas o jurídicas, públicas o privadas, así como las entidades mencionadas en el apartado 4 del artículo 35 de esta Ley, estarán obligadas a proporcionar a la Administración tributaria toda clase de datos, informes, antecedentes y justificantes con trascendencia tributaria relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas. [...]*
>
> ***2.*** *Las obligaciones a las que se refiere el apartado anterior deberán cumplirse con carácter general en la forma y plazos que reglamentariamente se determinen, o mediante requerimiento individualizado de la Administración tributaria que podrá efectuarse en cualquier momento posterior a la realización de las operaciones relacionadas con los datos o antecedentes requeridos.*

En conexión con dicho artículo, la Ley incluye entre las obligaciones tributarias formales, en su art.29, apartado 2 letra f) -**EDL 2003/149899**-, la siguiente:

> *[...] f) La obligación de aportar a la Administración tributaria libros, registros, documentos o información que el obligado tributario deba conservar en relación con el cumplimiento de las obligaciones tributarias propias o de terceros, así como cualquier dato, informe, antecedente y justificante con trascendencia tributaria, a requerimiento de la Administración o en declaraciones periódicas. Cuando la información exigida se conserve en soporte informático deberá suministrarse en dicho soporte cuando así fuese requerido.*

En cuanto a la facultad de requerir información tributaria por parte de la inspección de los tributos, es de reseñar que el art.141 LGT -**EDL 2003/149899**- reconoce entre sus facultades la posibilidad de requerir información tributaria en el marco de la investigación de supuestos de hecho que son ignorados por la Administración, la comprobación de la veracidad y exactitud de las declaraciones presentadas por los obligados tributarios o la realización de actuaciones de obtención de información relacionadas con la aplicación de los tributos.

Por otro lado, la obligación de aportar a la Administración, información con trascendencia tributaria que recoge el antedicho artículo 93 de la Ley, ha sido desarrollada en el capítulo V «Obligaciones de información» del Título II «Las obligaciones tributarias formales» del RD 1065/2007, de 27 julio -**EDL 2007/115078**-, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos (RGGI), en su artículo 30.

Ahora bien, una vez que hemos hecho referencia al deber de colaboración, se debe delimitar qué es lo que se entiende como información con transcendencia tributaria, pues en el presente supuesto la obtención de información se exige en mérito de la relación profesional.

En este sentido, es numerosa la jurisprudencia que ha abordado el tema. Así, entre las más recientes se puede destacar la STS 479/2019 de 8 abril, Sección 2ª, Rec. 4632/2017 -**EDJ 2019/563406**-, ECLI: ES:TS:2019:1311, que remitiéndose a pronunciamientos anteriores define la transcendencia tributaria como: la cualidad de aquellos hechos o actos que puedan ser útiles a la Administración para averiguar si ciertas personas cumplen o no con la obligación establecida en el art.31.1 de la Constitución -**EDL 1978/3879**- de contribuir al sostenimiento de los gastos públicos de acuerdo con su capacidad económica, y poder, en caso contrario, actuar en consecuencia, de acuerdo con la Ley. Y esa utilidad puede ser "directa" (cuando la información solicitada se refiere a hechos imponibles, o sea, a actividades, titularidades, actos o hechos a los que la Ley anuda el gravamen) o "indirecta" (cuando la información solicitada se refiere sólo a datos colaterales, que puedan servir de indicio a la Administración para buscar después hechos imponibles presuntamente no declarados o, sencillamente, para guiar después la labor inspectora -que no se olvide, no puede alcanzar a absolutamente todos los sujetos pasivos, por ser ello materialmente imposible- hacia ciertas y determinadas personas)».

En relación con la trascendencia tributaria de la información requerida, continúa la sentencia diciendo que el significado y alcance de este concepto jurídico indeterminado precisa que: la información puede solicitarse en cuanto sirva o tenga eficacia en la aplicación de los tributos, obviamente tomando la frase en términos generales, pues la norma no se refiere a la comprobación e investigación de una determinada relación tributaria, sino que busca habilitar para recabar información, tanto de particulares como de organismos, para cuanto conduzca a la aplicación de los tributos.

A continuación, podemos preguntarnos hasta cuando persiste la calificación de una información como de transcendencia tributaria y si esta apreciación se puede mantener en el tiempo, a pesar de la prescripción del tributo en el que se ha tenido en cuenta esta información. A este respecto, la Sala Tercera del Tribunal Supremo en su Sentencia de fecha 22-6-15, Rec. 2339/2014 -**EDJ 2015/130470**-, ECLI: ES:TS:2015:3359 ha concluido que la cuestión sobre si los datos conservados siguen siendo o no relevantes tributariamente debe resolverse en el procedimiento en el que se utilicen. No obstante, ha matizado que una cosa es que la Administración no pueda liquidar un tributo, como consecuencia del transcurso del plazo de cuatro años y otra distinta que se deban cancelar o eliminar aquellos datos con transcendencia tributaria correspondiente a ejercicios anteriores. Ni la Ley General Tributaria, ni ninguna norma en materia protección de datos imponen ninguna limitación temporal. Ahora bien, no parece que se puedan conservar datos ad perpetuam, cuando los mismos carezcan de cualquier utilidad a los efectos tributarios.

Asimismo, en aras a efectuar una correcta identificación de los datos con transcendencia tributaria es importante identificar cuál es la información que debe constar a efectos de facturación, ya que sería un contrasentido admitir el carácter reservado de la misma.

El RD 1496/2003, de 28 noviembre -**EDL 2003/136134**-, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido regula las obligaciones de facturación que incumben a los empresarios y profesionales. En cuanto al contenido de las facturas, se exige que sean «completas», de modo que toda factura debe estar numerada, incluir en ella el nombre y apellidos o denominación social del expedidor del documento y del destinatario, la descripción de la operación y su contraprestación total, así como el lugar y fecha de emisión entre otros (artículo 6).

Así las cosas, cuando la información facilitada que se traduce en la mínima expresión para relacionar la factura, con su correspondiente cliente, identifica el servicio profesional recibido o el importe satisfecho, podemos fácilmente concluir que se trata de una información indispensable para poder efectuar una correcta liquidación del impuesto. Por ejemplo, si una factura identifica la operación a la que está sometido un paciente como una operación estética, dicha información no es ni mucho menos superflua, pues puede servir para discriminar los ingresos obtenidos en operaciones exentas, respecto de otras que no lo son. Es decir, lo que resulta determinante en último lugar es que nos encontramos con información con una traducción económica y por ende, puede tener una relevancia fiscal inequívoca.

Lo que no tendría en ningún caso justificación es la incorporación de fichas de clientes, historias clínicas o similares, pues lo único que interesan son los datos propios de facturación.

Efectivamente, las facturas contienen datos personales de los clientes, pero no todo dato personal es íntimo, ni la protección que la información personal fundamenta el art.18.4 CE -**EDL 1978/3879**- puede erigirse en obstáculo para el cumplimiento del deber que la propia Constitución impone a todos de contribuir al sostenimiento de los gastos públicos de acuerdo con la capacidad económica de cada uno.

Conclusiones

La proliferación actual de herramientas informáticas ha obligado a actualizar la regulación existente en materia del derecho a la intimidad o el acceso a la información y protección de datos para evitar que la misma pudiera quedar pronto obsoleta, atendiendo a la velocidad de las innovaciones existentes en esta área.

Hoy en día, no se puede cuestionar que la protección de la privacidad participa de una doble dimensión individual y social. Si una vida privada, libre de injerencias de terceros en la protección de datos permite el libre desarrollo de personalidad y con ello, la consolidación de la autonomía personal no hay duda que la protección de los datos se inserta en el marco de la dignidad de la persona y ésta a su vez, sirve para consolidar el carácter democrático de la sociedad. Así, lo entendía el juez Douglas en Osborn v. United States, cuando afirmaba que «el derecho a ser dejado sólo es el principio de toda libertad».

Ahora bien, el reconocimiento del derecho a la intimidad o a la protección de datos no significa la existencia de un derecho absoluto y ajeno a la existencia de otros bienes jurídicos protegidos, como ocurre con el deber de contribuir en un sistema tributario justo. En este sentido, deben ponderarse adecuadamente el ejercicio de los derechos bajo el prisma del principio de proporcionalidad.

De este modo, no se puede pretender limitar la actividad investigadora de la Administración tributaria, cuando el tratamiento de los datos se limita a la existencia de una información con transcendencia tributaria o se ha obtenido mediante el consentimiento libre del titular del derecho. Lo que tampoco significa que se legitime ningún totalitarismo en materia de información como si se tratase de la sociedad descrita por George Orwell en su obra 1984.

La apreciación de qué información es o no transcendente a efectos de tributos dependerá ya de la correcta identificación de los intereses en conflicto y eso sólo se podrá alcanzar mediante un análisis de las distintas circunstancias del caso en concreto.

LA CESIÓN DE DATOS PERSONALES DENTRO DE UN SUPUESTO CONTEMPLADO POR LEY

Arán Feijoo Covelo

Es mes de abril la **Agencia Española de Protección de Datos ha archivado una reclamación presentada por Navarra Suma contra la Hacienda foral** por haber compartido con la Dirección General de Vivienda del Gobierno de Navarra datos sobre el suministro de agua de viviendas. El objetivo de la Dirección General de Vivienda al acceder a estos datos era determinar la posible inclusión de inmuebles en el censo de viviendas vacías.

La reclamación del grupo parlamentario de Navarra Suma, se inicia cuando propietarios de Viviendas de la comunidad Foral comienzan a recibir cartas de la Dirección general de Vivienda. La reclamación del Grupo Parlamentario de Navarra Suma exponía que la Mancomunidad de la Comarca de Pamplona facilita a la Hacienda Tributaría de Navarra los datos relativos al suministro del agua de todas las viviendas para prevenir el fraude por viviendas que podrían estar alquiladas, al amparo de lo establecido en la ley foral General Tributaria. Sin embargo, Navarra Suma señalaba que, al haber trasladado Hacienda estos datos a la Dirección General de Vivienda, fueron cedidos para un fin diferente, el control de viviendas deshabitadas. También alegaba Navarra Suma que la información de todas las viviendas que Hacienda entrega al Departamento de Vivienda era excesiva.

Según establece el procedimiento, la AEPD antes de admitir a trámite la reclamación, traslado a la Hacienda Foral navarra el escrito de Navarra Suma para que diera respuesta. La argumentación de la Hacienda Foral Navarra, la contestación consistió en indicar que el suministro de información aportada a la Dirección general de vivienda está amparado de forma específica en la ley foral general tributaria y en el "***deber de colaboración interadministrativa***" previsto en la ley de Régimen Jurídico del Sector Público.

Descartando el segundo argumento el cual choca de frente con el principio de cesión de datos y autorización expresa del tratamiento ya que los datos cedidos a una administración pública no pueden ser utilizados más que para el tratamiento objeto de la cesión de los mismos. Sin embargo la primera argumentación si es correcta ya que según contestación de la Hacienda Foral "*la cesión se realizó al Departamento competente en materia de vivienda para la gestión y mantenimiento de un registro de vivienda sobre el que posee plena competencia, lo que, en definitiva, no puede sino llevar a concluir que la cesión de información se encuentra plenamente subsumida en el supuesto de cesión" del artículo 105.1 ñ) de la ley foral General Tributaria*".

Este artículo de la ley foral establece que los datos obtenidos por la Administración tributaria tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto, entre otros aspectos, "la colaboración con el Departamento del Gobierno de Navarra competente en materia de vivienda en el ejercicio de sus funciones de fomento del acceso a la vivienda, de gestión de las ayudas públicas y de mantenimiento de los registros de viviendas que se encuentren a su cargo".

Es por tanto que se considera que la cesión está legalmente autorizada y es conforme a Derecho la cesión de datos que se hizo a la Dirección General de Vivienda.

Una vez recibida esta respuesta, la Agencia de Protección de Datos concluye, en una resolución que, "analizadas las razones expuestas por la Hacienda foral de Navarra, se ha constatado la **falta de indicios racionales de la existencia de una infracción** en el ámbito competencial de la Agencia Española de Protección de Datos, no procediendo, en consecuencia, la apertura de un procedimiento sancionador". Se realiza especial hincapié en que la aplicación del principio de inocencia impide imputar una infracción administrativa cuando no se presenten evidencias o indicios de los que se deriva la existencia de infracción, cuestión donde el escrito de Navarra Suma no aporta evidencia alguna de infracción y por tanto es archivada.

Esta reclamación contra la Hacienda Foral Navarra, da pie a recordar, los requisitos específicos para la cesión de datos, entendiendo como cesión de datos cualquier mecanismo que permita a un tercero acceder a los ficheros que no estén bajo su responsabilidad.

Para poder realizar una cesión de datos hay que cumplir dos requisitos. El primero que la cesión de datos sea para el cumplimiento de fines relacionados con las funciones del cedente y el cesionario siendo el segundo requisito, el previo consentimiento del interesado.

Siguiendo estos requisitos, la hacienda foral Navarra, responsable del tratamiento de los datos de los administrados para la gestión fiscal y contributiva, habría incurrido en una posible infracción al ceder estos mismos datos a la dirección General de Vivienda, el cual los empleo los datos para fines diferentes a los que el cesionario tenía previsto.

Sin embargo el RGPD establece una serie de supuestos donde no será necesario informar sobre la cesión de datos, siendo seis supuestos:

1. Cesión autorizada expresamente por ley
2. Se trate de datos recogidos de fuentes de acceso público siempre y cuando los datos sean para la satisfacción de interés propio y se respeten los intereses de los interesados.
3. El tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo cumplimiento y control implique una necesaria conexión del tratamiento de ficheros a terceros (Cuando exista un contrato para prestar un servicio)
4. El destinatario sea el Defensor del Pueblo, el ministerio fiscal, Tribunal de cuentas o Tribunales
5. La cesión sea entre las administraciones públicas con el fin de tratarlos posteriormente con finalidades históricas, estadísticas o científicas.
6. La cesión de datos relativos a la salud sea necesaria para solucionar una urgencia (medica) que requiera acceder a un fichero.

En el primer supuesto, cesión de datos autorizada por la ley habría que determinar cuáles son los requisitos necesarios para conocer si la afirmación de la Hacienda foral "*la cesión de información se encuentra plenamente subsumida en el supuesto de cesión" del artículo 105.1 ñ) de la ley foral General Tributaria*" es correcta.

El articulo 105 dice de forma expresa que "Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto"

La colaboración con el Departamento del Gobierno de Navarra competente en materia de vivienda en el ejercicio de sus funciones de fomento del acceso a la vivienda, de gestión de las ayudas públicas y de mantenimiento de los registros de viviendas que se encuentren a su cargo.

Siendo por tanto un supuesto expresamente contemplado por una ley y entrando dentro de las competencias de la Hacienda Foral navarra. Es una Cesión perfectamente ajustada a norma en materia de protección e datos.

TEORÍA DEL MOSAICO Y DATA MINING: ANÁLISIS JURÍDICO DEL ESTADO ACTUAL EN COMPARATIVA CON LA THEORY MODULAR

Javier Antonio Nisa Ávila

Introducción

En los inicios de la civilización moderna el salario se utilizaba como medio de pago a cambio de la obtención de un rendimiento para un empresario, era el coste a pagar a cambio de una mercancía. La palabra salario etimológicamente tiene origen en la palabra salarium que deriva directamente de la palabra sal. (Martínez, 1989) En la antigua Grecia y Roma, era costumbre que los pagos que se realizaban de forma generalizada, fueran en sal, de hecho los esclavos eran intercambiados por sal y de ahí nació la expresión "no vale su sal". Por ello la sal se convirtió en la antigüedad en un producto que adquirió mucha importancia. En la antigua Roma la sal fue el motivo de la construcción de las primeras vías comerciales, abriendo una vía de las salitreras de Ostia hacia Roma alrededor de 500 años A. C. La llamada "Vía Salaria" era custodiada por soldados para que no asaltaran los cargamentos de sal y recibían el pago por su servicios en sal y le llamaron a ese pago "salarium argentum" (Rodríguez Menjibar, 2004). A lo largo de los siglos la sal quedó a un lado y el pago por realizar servicios o trabajos se comenzó a realizar en monedas de diversos materiales.

Actualmente estamos cerca de un cisma que está provocando paulatinamente otro nuevo cambio en el patrón social y empresarial respecto al pago de salarios al emerger un tipo de "moneda" adicional a la actual. Nos referimos a los datos, como nuevo patrón moneda aflorando en la sociedad. Los datos son un tipo de mercancía que se puede transformar en un beneficio económico directamente o indirectamente y aplicable tanto a empresas como a particulares.

La principal fuente de datos donde obtener beneficios son las redes sociales; la comunicación por red. La existencia de empresas especializadas en la compra de datos personales o profesionales obtenidos directa o indirectamente de usuarios que los venden es un hecho real. La cuestión respecto todo ello es que a la velocidad que está evolucionando comienza a ser jurídicamente problemático.

La comunicación es un hecho natural que nace como un mecanismo de entendimiento en nuestra especie enfocado a la construcción de acuerdos pretendiendo persuadir, inducir o intentar hacer creer un razonamiento sobre un determinado problema o concepto con el principal objetivo de un entendimiento que justifique esa comunicación. La comunicación es un juego de persuasión y entendimiento (Cisneros, 2002). La sociedad de la información, el mundo de la "red" entendido como un mundo virtual donde nos podemos comunicar de diferentes formas; directamente con nuestra identidad, con una identidad falsa, anónimamente, corporativamente, en grupo, etc, nos permite construir una nueva forma de comunicarnos.

La comunicación en red o comunicación en red social es el nuevo standard de comunicación emergente donde todos los usuarios de las diferentes redes se vinculan entre sí por cuestiones de afinidad. La comunicación en red tiene como uno de sus principales características la perdida del emisor/receptor, provocando un cambio de papeles donde todos los usuarios se siente ambas cosas al mismo tiempo y en simultaneidad (Herreros, 2008).

Por ello y partiendo del concepto de comunicación en red como el pilar básico de donde surge esa nueva moneda de cambio que son los datos que se extraen de la comunicación que realizan las personas, no debe confundirse la interacción respecto a la interactividad en el ámbito comunicativo. La interacción conceptualmente se está refiriendo a una serie de acciones recíprocas que realizan entre sí diversos individuos. Sin embargo la interactividad se refiere a la forma en que los servidores o el software gestiona esas redes de comunicación de masas; es decir la interacción y la interactividad no son conceptos totalmente diferentes, sino que están interconectados. La interacción es una relación entre los participantes de una red que de forma interactiva se vinculan entre sí mediante diferentes sistemas de software y servidores que gestionan y tratan todos los datos que se mueven por esa red para conseguir una comunicación entre diferentes personas que sin ayuda de los medios técnicos, la interactividad, sería imposible conseguirs la citada interacción (Köster, 2005).

Por ello y antes de pasar analizar los peligros de este nuevo sistema de comunicación en red, que elementos la componen y como la legislación puede ayudarnos a protegernos ante el avance de la inteligencia artificial, cabe recordar lo que Laswell decía sobre la comunicación "es necesario que

no nos olvidemos quien dice qué, en qué canal, a quién y con qué efectos" (Laswell, 1986).

No obstante la comunicación en red tiene también sus peligros; sobre todo ante el uso de la inteligencia artificial y el Data Mining como principales elementos de interactividad.

Por todo lo anterior los actuales sistemas de comunicación en red se basan en tres grupos de elementos:

1) Software
2) Transversalidad comunicativa
3) Legislación

En el grupo del software nos podemos encontrar con la Inteligencia Artificial y el Machine Learning como herramientas ejecutadas bajo metodologías de Data Mining.

En el segundo de transversalidad comunicativa nos encontramos a dos elementos transversales entre si. El primero sería el Data Mining como un elemento transversal que conecta a las redes sociales con la inteligencia artificial y el machine learning. El segundo elemento serían las redes sociales y su propia transversalidad conceptual como material que alimenta al software y permite la existencia del Data Mining en si mismo. Las redes sociales y el Data Mining se retroalimentan entre ellos.

Por último un tercer grupo de elementos sería la legislación y el Data Privacy o datos privados, donde nos encontramos de que forma repercute los dos primeros grupos en posibles agresiones a la vida privada de las personas; usuarias de las redes de comunicación.

Estos cinco elementos son claves para entender los problemas actuales que genera el Data Mining respecto a la comunicación en red y el Data Privacy de los usuarios. Asimismo nos permite saber de que forma puede llegar a influirnos en un futuro próximo los diferentes datos e informaciones que volcamos de forma indiscriminada o voluntariamente en red. Los usuarios estamos facilitando todos los elementos necesarios no sólo para perder nuestra intimidad sino para condicionar diversas parcelas de nuestra vida, como por ejemplo el trabajo o la salud, sin olvidar evidentemente la violación de nuestra intimidad en todos sus aspectos sociales y personales.

El florecimiento de diferentes problemas vinculados directamente con la inteligencia artificial, el machine learning y el Data Mining que se realiza sobre las redes, genera una pérdida de intimidad por la publicidad o venta de nuestros datos a entes privados o públicos. Todo ello tiene como objetivo por ejemplo el estudio para procesos de selección en recursos humanos o seguros de salud entre otros; esto no está legislado y genera un problema. El derecho tiene como reto protegernos frente a esta corriente tecnológica que inunda nuestras vidas ofreciendo los mecanismos legales necesarios.

Por ello para poder realizar esta investigación hemos utilizado una metodología cualitativa siguiendo un análisis de método analítico y transversal de análisis de datos, mediante el cual se ha procedido a analizar el volumen de tráfico actual de datos en comunicaciones en redes sociales y a través de internet por parte de usuarios de forma voluntaria e involuntaria junto con la actual legislación y sus posibles fallas para vertebrar las posibles soluciones en base a las teorías jurídicas actuales sobre protección de datos.

Definiendo conceptos

En primer lugar antes que nada cabe definir una serie de conceptos como el Data Mining, la Inteligencia Artificial, el Machine Learning, la transversalidad de las redes y el Data Privacy, para así poder contextualizar mejor el análisis de datos que vamos a realizar. Todos estos conceptos están entrelazados entres sí con un equilibrio entre ellos que permite optimizar al máximo la explotación de datos de los usuarios.

Data Mining

El primero de los conceptos es el Data Mining el cual se enmarca dentro de un campo multidisciplinar que da soporte a los especialistas dedicados a la extracción de información de relevancia en entornos de comunicación. El objetivo es discriminar que datos generados pueden parecer a priori irrelevantes. La idea de mining proviene precisamente de la dedicación que se necesita, siendo un paralelismo con el trabajo que se realiza en una mina para localizar un determinado material (Han, Kamber, 2002).

Como se ha indicado el data mining pertenece a un campo multidisciplinar en el cual realmente el concepto data mining se encuentra dentro del gran concepto Knowledge Mining from Data, el cual realmente estructura 7 procesos diferentes con los cuales se pretende alcanzar el objetivo de extraer datos relevantes para diferentes usos. Los procesos que conforman este Knowledge Mining from Data donde el data mining es el más relevante y de ahí su uso como nomenclatura generalizada (Kamber, Pei, 2011) son:

1. **Data cleaning;** donde se separan datos que se consideran ruido informativo o desechable de los que no lo son.

2. Data integration; se dedica a combinar los datos extraídos de los diferentes data cleaning que se le ha realizado a un mismo usuario, preparando dichos datos para un posterior tratamiento.

3. Data selection; es un proceso donde se realizan tareas de análisis para detectar posibles datos relevantes eliminando aquellos que por su combinación con otros datos se consideran desechables.

4. Data transformation; en este apartado se transforman los datos relevantes en datos consolidados y se le agregan a modo de índice que datos se han desechado y las razones de porqué se ha tomado dicha decisión, los orígenes de los datos y diferentes datos adicionales pueden ayudar a perfilar dichos datos en el data minning.

5. Data mining; éste es el proceso más importante de todos; los cuatro anteriores se han utilizado exclusivamente para preparar los datos para éste quinto paso. Aquí mediante diferentes algoritmos basados en inteligencia artificial no autónoma de segundo nivel dentro de la escala de tipos de inteligencia artificial legal, se extraen combinando todos los datos de un usuario, nuevos datos más complejos que generan nueva información con suficiente relevancia y reflejo de la realidad del usuario extraído que sirva para diferentes usos comerciales, gubernamentales, etc (Nisa Avila, 2016).

6. Pattern evaluation; se dedica a identificar en base a unos patrones de interés preestablecidos si la información obtenida por data mining es la buscada.

7. Knowledge presentation; es la capa final de presentación de los datos.

Inteligencia Artificial

La inteligencia artificial se puede definir como aquellos mecanismos basados en hardware y software que tienen una serie de capacidades de toma de decisiones bien de forma asistida o no asistida para el desarrollo de unas tareas y funciones básicas programadas por un operador humano bien porque su finalidad es el desarrollo de diferentes tareas preprogramadas o que bajo condiciones de funcionamiento autónomo y con libre albedrío sean capaces de seguir unos objetivos tomando las decisiones de forma independiente al ser humano; siempre en todo caso para fines socialmente correctos, no violentos, y que no sean nocivos; ni para humanos ni para los propios robots (Nisa Avila, 2016).

Machine Learning

El machine learning es una rama dentro de la inteligencia artificial que tiene como objetivo mediante algoritmos de aprendizaje mejorar los procesos que realiza una inteligencia artificial sin necesidad de intervención humana, automejorando de forma constante tomando sus propias decisiones sobre como obtener en el caso que nos compete mejores datos, y pensando en base a dichos algoritmos como mejorar sus sistemas de forma autónoma y sin intervención humana (Mena, 1999).

Transversalidad de la red

La transversalidad en red es la forma de comunicación que tiene todo individuo a través de las redes sociales mediante formas de comunicación tradicional o directa donde el individuo es el emisor de la información y existe un receptor activo que es otro individuo. Todo ello directa o indirectamente mediante el uso de los metadatos que se emiten por parte del individuo emisor de información a un receptor ciego que es la plataforma de la red social que está utilizando. La transversalidad en red viene dada cuando un individuo usa más de una red de comunicación, entendiendo por red de comunicación, email, whatssapp, telegram, instagram, facebook, twitter, tiktok, dropbox, google drive, búsquedas en buscadores, foros, etc.

Ésta transversalidad provoca como más adelante veremos una composición de datos que se ejecuta gracias a diferentes teorías jurídicas sobre protección de datos.

Data Privacy

El Data Privacy es el conjunto de datos que pertenecen a la esfera privada de un individuo y que pueden ser sensibles por su contenido o relevancia de forma que su uso o conocimiento puede suponer violar su derecho a la intimidad en cualquier clase de circunstancia.

Todo este conjunto de herramientas y conceptos están unidos entre sí gracias a los datos tanto voluntarios como involuntarios que las personas vuelcan de forma constante en la red. Las diferentes formas de comunicarse que usan como vehículo comunicativo a una red social como facebook o twitter, mensajería como whatssapp o un foro de algún tipo, son la fuente de donde se nutren las diferentes herramientas mencionadas para configurar gracias a diferentes teorías jurídicas que luego veremos, la composición de la vida de una persona.

Un claro ejemplo de uso de datos recogidos en redes sociales lo tenemos en el caso de Cambridge Analytica, con fines políticos tras analizar con herramientas de inteligencia artificial y data mining los datos de millones de usuarios para influir en las elecciones de EEUU (Muñoz, 2018).

IOT y Data Privacy

El Internet Of Things (IOT) y la gestión de los datos personales que se mueven entorno a dicho concepto es realmente un gran problema en auge. El IOT junto al IORT (Internet Of Robotic Things) es una de las principales revoluciones del siglo XXI. La posibilidad de tener al alcance todo tipo de herramientas de software en cualquier tipo de dispositivo que nos ayuda a nuestra vida diaria y que nos ofrece grandes cantidades de información a los usuarios sobre nuestros hábitos de vida, nuestros niveles físicos asociados a actividades deportivas, datos sanitarios con pulseras biométricas, datos domóticos, etc; se están convirtiendo en una gran fuente de información para diferentes organismos y entidades corporativas.

El IOT gestiona constantemente datos durante las 24 horas del día, como ejemplo muy interiorizado ya en nuestra sociedad tenemos a las pulseras cuantificadoras que nos monitorean las pulsaciones, el oxígeno en sangre, el nivel de ejercicio y la calidad del sueño entre otras cosas, remitiendo datos de forma constante. Otro ejemplo está en el smartphone, como constante sistema de geolocalización. Aunque tengamos el GPS desactivado la capacidad de localización de nuestra posición que tiene la empresa de telefonía o cualquier aplicación que se instale en nuestro smartphone con el GPS desactivado es de tan sólo 3 metros de error sobre nuestra posición. Esto ya nos da la medida de que capacidad de análisis de datos estamos ofreciendo como usuarios simplemente el tener nuestro teléfono encendido y sin GPS (Del Risco Montero, 2012).

La constante subida de datos de forma constante durante las 24 horas de cada día, bien sean subidos de forma voluntaria o involuntaria, sumado a la capacidad actual de computación con el data mining y la inteligencia artificial genera una cantidad de posibilidades infinitas a muchas entidades acerca de nuestra intimidad.

En la actualidad existe un gran déficit educativo en nuestra sociedad acerca de la importancia de tener los conocimientos suficientes como para saber como deberíamos comunicarnos. La comunicación por redes en general bien sea a través de redes sociales, aplicaciones de diversa índole o programas de mensajería, se ha subestimado y está provocando que nos

comuniquemos de forma indiscriminada sin atender que decimos, a quien se lo decimos, con que finalidad y con que consecuencias. La educación en comunicación en red debe ser un reto a tener en cuenta en la sociedad del siglo XXI.

La principal problemática de este reto viene dato por la constante subida incesante de datos sin descanso a la red por parte de todos las personas que se conectan a la red.

La gran piedra angular bajo el prisma jurídico viene dada principalmente por el concepto de datos voluntarios y datos involuntarios.

Los datos voluntarios son aquellos de los cuales somos conscientes a la hora de volcarlos a internet, como la subida de una foto a una red social, la opinión sobre una cuestión determinada que se hace pública, el compartir contenido en redes, la participación en foros tematizados bien por hobby o por cuestiones profesionales, o un mensaje de whatssapp. Los datos voluntarios los podríamos definir como el conjunto de datos que se suben a una plataforma conectada a internet de forma voluntaria con una finalidad de la cual somos participes y mediante la cual somos conscientes que nuestros datos serán visibles de forma sencilla y con pocos sistemas de seguridad. Por ejemplo; Facebook, Twitter, Instagram, o diversos foros.

Los datos involuntarios son aquellos datos considerados fantasma que sin tener conocimiento de su existencia o conociéndola el individuo dueño de los mismos, se generan y envían de forma automática a un tercero el cual los recopila y trata según considera conveniente al pasar a convertirse dicho tercero como propietario de dichos datos. Por ejemplo; cualquier aplicación que recopile datos desde metadatos de una fotografía al subirla a una plataforma como facebook o datos automáticos que aparatos de domótica o pulseras deportivas mandan a sus respectivas aplicaciones.

Por ello resulta más que necesario una conciencia ciudadana sobre la comunicación digital, y como debemos de comunicarnos digitalmente; al igual que se nos educa a como debemos comunicarnos como seres vivos entre nosotros de forma natural (lenguaje natural) se debería al mismo tiempo educar en un lenguaje digital.

Para eso tenemos como ejemplo a Facebook y su política de datos cuando un usuario se da de alta en su red social. Las políticas de datos que por ley están en todas las páginas y que tienen como finalidad informar de la legislación que se aplica en dicha aplicación o web y que compromisos y clausulas contractuales acuerda el usuario con dicha empresa que gestiona esa página o aplicación normalmente nunca los usuarios tienden a leerlas. La política de datos cuando un usuario se da de alta en redes sociales o aplicaciones de mensajería, se limita en la mayoría de ocasiones simplemente a rellenar lo ne-

cesario para estar de alta y obvia la lectura de paginas y páginas de advertencias legales y cláusulas contractuales con las que adquieren un compromiso al darse de alta en una plataforma.

Extracto del pliego de condiciones de usuario al darse de alta en la plataforma Facebook®

> *"Usamos la información que tenemos (incluida la actividad que llevas a cabo fuera de nuestros Productos, como los sitios web que visitas y los anuncios que ves) con objeto de ayudar a los anunciantes y otros socios a medir la eficacia y la distribución de sus anuncios y servicios, así como para ayudarles a conocer qué tipos de personas usan sus servicios y cómo interactúan con sus sitios web, aplicaciones y servicios" (Data Policy, 2020)*

Por todo lo anterior podemos observar como nuestros datos pueden ser usados para fines comerciales u otros cualesquiera decida.

Para el caso de Facebook, sin necesidad de que nos deban de informar más allá de una simple cláusula. Simplemente dándonos de alta en sus servicios aceptamos las condiciones que firmamos y por ende que nuestros datos de cualquier tipo en esa plataforma sean cedidos para lo que consideren conveniente e incluso monitoreen nuestra navegación. Pero ello no es exclusivo de Facebook, sucede también en Twitter, Whatssapp, Instagram, Dropbox, todos los productos de Google, etc.

Todos esos datos que se ceden a terceros por nuestra actividad son principalmente datos "tradicionales", los archivos o publicaciones conscientes que realizamos así como metadatos o "datos fantasma" que se suben automáticamente con esas publicaciones o mediando procesos secundarios. En todos ellos subyacen los fines comerciales o gubernamentales y por ello una educación en comunicación en red es necesaria para conocer por un lado a lo que nos comprometemos como usuarios, y por extensión de esa forma ser conscientes del alcance y escasa privacidad de lo que publicamos.

Si a todo ello le unimos los datos conseguidos gracias a la tecnología de Inteligencia Artificial, Data Mining y Machine Learning y que se advierte en la Teoría jurídica del mosaico, nos encontramos con una gran visión de nuestras vidas en manos ajenas.

Alcance del Data Mining: privacidad cuestionada

El Data Mining como hemos podido observar se convierte en una herramienta capaz de obtener datos que a priori pueden pasar desapercibidos pero que para, como hemos visto, los dueños de esos datos que son las diferentes redes son una fuente de ingresos, y por ende los buscan para monetizarlos.

Como casos relevantes de lo que podría

considerarse como una violación de nuestra privacidad y que resultó no serlo legalmente nos podemos encontrar con el caso de Rehtaeh Parsons o Winston Smith.

El caso de Rehtaeh Parsons es un claro caso de cesión de datos en Facebook, esta chica tras más de cuatro años muerta, Facebook usó su imagen para una campaña publicitaria de una web de citas, sin pedir consentimiento a los padres de la fallecida, pues era menor en el momento del fallecimiento. El caso se saldó con una disculpa por parte de Facebook al ser Facebook el propietario de la fotografía (BBC News, 2013).

Por otro lado **el caso Winston Smith contra Facebook y la American Cancer Society** con sentencia del 06 de Diciembre de 2018 evidencia el grado de vinculación legal que tiene un usuario respecto a los pliegos que acepta cuando se da de alta en una plataforma y la gestión de datos y metadatos o datos fantasma. El caso Winston Smith denuncia que Facebook recolectaba sus datos médicos y sanitarios. Para ello el demandante aportó documentación donde se observa que mientras se estaba realizando un tratamiento contra el cáncer, la plataforma Facebook recopiló datos de geoposicionamiento, lugares donde se estaba tratando, tratamientos que se estaba dando por productos que compraba y un seguimiento de la navegación de todas las páginas donde accedía sobre la enfermedad que padecía. Ésto provocó que se le comenzaran a ofrecer anuncios personalizados directamente sobre tratamientos del cáncer, y de otra índole así como emails y "SPAM" aludiendo de forma indirecta a su dolencia.

La sentencia No. 5:16-cv-01282-EJD del estado de California concretamente la Court for the Northern District of California falló que no existía violación alguna del derecho a su intimidad por dos razones (Winston Smith vs Facebook and American Cancer Society, 2018) que son:

1.- Tenía un contrato válidamente firmado con Facebook cuando se dio de alta en el cual aceptaba sus condiciones de cesión de datos. (véase el extracto anteriormente citado del pliego de condiciones de Facebook).

2.- La información publicitaria que le ofrecían no citaban datos expresos de el directos, sino indirectos y nunca publicaron su historial médico de forma expresa. Por lo que la tenencia de datos sensibles sin publicación, no lo considera violación del derecho a la intimidad.

Ésta sentencia es muy relevante porque es la primera de Estados Unidos en enjuiciar la privacidad de datos en una red social de forma tan relevante y expresa; una privacidad que va mucho más allá de unas simples "cookies".

Por ello podemos evidenciar que estos casos, pero sobre todo el último es un ejemplo de lo que el data mining, y la inteli-

gencia artificial pueden conseguir en materia de privacidad. Pero el como lo consiguen es otro aspecto a tener en cuenta; lo consiguen aplicando los conceptos básicos de privacidad de datos de la Teoría del Mosaico de Madrid Conesa entre otras teorías.

Teoría del Mosaico e Inteligencia Artificial: hacia una nueva teoría

No somos conscientes del alcance del data mining que junto con al machine learning y la inteligencia artificial dan alas a la utilización de la teoría del mosaico a las grandes corporaciones. La Teoría del Mosaico de Fulgencio Madrid Conesa (1984) es una teoría jurídica que estudia la protección de datos y que sustituyó a nivel mundial a la Teoría jurídica Alemana de las Esferas en el ámbito del Derecho a la Privacidad, estableciéndose como la nueva teoría jurídica sobre protección de datos a nivel mundial.

En la teoría alemana de las esferas, los datos se organizaban en círculos concéntricos. El aspecto más personal en la que se encontraban los datos más íntimos de un individuo correspondían a un círculo que estaría en la zona más cercana al individuo, lo privado en un círculo más amplio y así sucesivamente. Madrid Conesa sin embargo teoriza que ese sistema de protección de datos en base a círculos con las nuevas tecnologías es ineficaz y formula un nuevo concepto llamado teoría del mosaico. La teoría del mosaico considera que la información de un individuo en cuanto a lo privado y lo público son datos abiertos y no pertenecientes al 100% a un apartado determinado. Por ello se puede entender que existe una delgada linea entre los datos que se pueden considerar privados y cuales públicos, puestos que esa clasificación según Madrid Conesa va a depender de quien sea el sujeto receptor de la información y quien el emisor de la misma. Por otro lado lo que en un principio puede parecer un dato irrelevante, como el sexo de una persona, el nombre, la fecha de nacimiento, sus inclinaciones políticas, sus datos de renta, etc si se presentan aislados; si los mismos en lugar de verlos de forma aislada los unimos, todo cambia. Los datos que a priori pueden parecer no importantes y que no afectan al derecho a la intimidad si los conectamos con otros que quizás tampoco parezcan irrelevantes, pero que pertenezcan al mismo individuo, podemos llegar a conseguir una composición exacta de dicho individuo sin que éste tenga conocimiento de ello. Por tanto sucede “al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado” (Miguel, 1994).

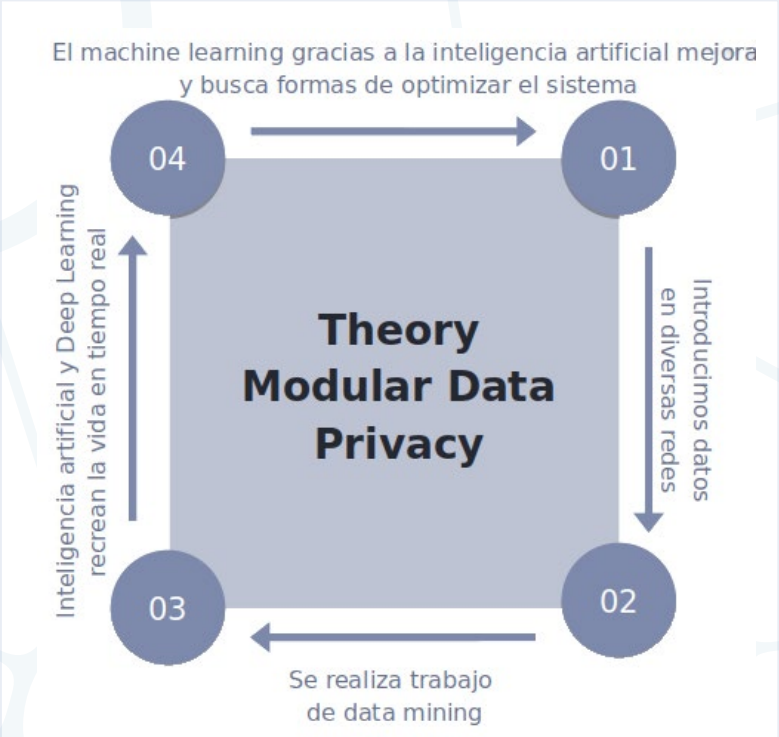
El conjunto de pleno significado que se teorizaba en su momento por parte de Madrid Conesa en 1984 es actualmente al igual que sucedió con la teoría alemana de las esferas; desfasado. Actualmente resulta necesario que sea actualizado al igual que sucedió con la teoría alemana de las esferas. La teoría del mosaico tras todos los datos que es-

tamos analizando debería evolucionar hacia una nueva teoría que podríamos denominar "Teoría modular de la privacidad de datos" o "Theory modular data privacy".

La "Theory modular data privacy" es en el campo jurídico teórico del ámbito de protección de datos el reflejo del actual sistema de explotación de datos que usan las grandes corporaciones y gobiernos para elaborar esa composición de cada individuo donde uniendo diferentes piezas de datos consiguen averiguar diferentes situaciones reales de una persona. La "Teoría modular de la privacidad de datos" a diferencia de la "Teoría del mosaico" donde directamente los datos sin tratamiento alguno se unen entre si para identificar un aspecto concreto de un usuario; en la "Teoría modular de la privacidad de datos", se refleja la actual realidad.

La gestión de datos en la actualidad usa sistemas para ejecutar recreaciones de datos. Por ello se vendría a definir que los "datos" se usan primero como combustible para una "máquina" que se dedica a fabricar un producto que arroja datos más complejos y monetizables. La "Teoría modular de la privacidad de datos" parte de la base que los datos actualmente no sólo se usan en bruto sino que se depuran y sobre todo se transforman. Ésta "máquina jurídica" que propone la "Teoría modular de la privacidad de datos" está compuesta por diferentes módulos que encajan entre sí para funcionar; si falta una pieza se rompe la "máquina", deja de funcionar y no se obtiene el producto final, que no es otra cosa que datos con capacidad de monetización para quien los busca y reconstruye o construye.

En el siguiente esquema de elaboración propia podemos ver la "Teoría de modular de la privacidad de datos" la cual se compone por cuatro pasos repetitivos donde al acabar de analizar datos todo vuelve a comenzar por el paso 1.



El paso primero se encontraría protagonizado por el individuo que introduce datos tanto voluntarios como involuntarios en diferentes redes. Posteriormente nos encontraríamos con el paso 2 donde gracias a un proceso de data mining se recrea la vida de un usuario en tiempo real como si fuera un video pixel a pixel y cuyos datos permite obtener un rendimiento económico. En la tercera fase gracias a un sistema de inteligencia artificial se relacionan todos los datos en base a una serie de parámetros que previamente se han configurado creando un producto final que sería una "recreación" en tiempo real de una parcela privada concreta de una persona. Posteriormente en una cuarta fase gracias al machine learning, se depuran los posibles fallos del producto final y sino es adecuado, útil o es optimizable se introducen medidas correctoras en los pasos 1, 2 y 3 que permita mejorar el producto final.

En el ámbito del derecho y el campo jurídico de la protección de datos lo que describe la "Theory modular data privacy" es lo que está sucediendo en el ámbito de la comunicación actual en redes y se convierten en los cuatro puntos cardinales que se deberían de proteger jurídicamente en materia de protección de datos.

Es necesario resaltar que **un dato aislado no es un problema, el problema radica en el conjunto de datos que se vuelcan y como se pueden ir engarzando estos entre sí como si de un collar de perlas se tratase**. Todo este panorama jurídico se completa con la cesión de datos entre empresas lo que permite conseguir una mayor fidelidad de datos y la justificación en relación a ala evolución jurídica de un postulado teórico del mosaico a otro donde la evolución tecnológica recrea la vida de las personas con datos con una precisión extraordinaria

Pero hasta que punto pueden llegar a alcanzar en cuanto a número de datos absolutos todo lo que se vuelca en la red. Pues pueden llegar a ser reveladores los datos, en la actualidad en 2020 hay 4536 millones de usuarios en internet, que equivalen al 58,8% de la población mundial y generan un total de 6.826.667 documentos por segundo, los cuales contienen cada uno de ellos muchos datos explotables en base al perfil descrito anteriormente (World Internet Users Statistics and 2019 World Population Stats, 2019).

Conclusiones

Puede parecer que estamos totalmente desprotegidos frente a este nuevo reto jurídico, pero actualmente existen multitud de herramientas jurídicas y organismos que protegen al consumidor digital como la European Network and Information Security Agency o ENISA. Asimismo tenemos directivas europeas y tratados internacionales que nos protegen como el Reglamento (UE) 2016/679, de 27 de abril o las "Binding corporate rules" que el legislador de la UE está comenzando legislar. La Unión Europea es el legislador

más avanzado en materia de protección de datos y mayor número de sanciones en todo el mundo. Todo ello gracias a la posibilidad de una legislación única para 27 países y un tribunal propio como el TJUE que si a eso le sumamos las diferentes agencias nacionales de protección de datos de cada país, formamos un tejido protector que pretende frenar estas prácticas.

Pero aunque exista una multitud de legislación como acabamos de indicar que pretende protegernos, su eficacia no es realmente completa. El problema radica en que dicha legislación sólo se centra en generar obligaciones jurídicas a empresas teniendo solo que elaborar pliegos de condiciones en sus productos que expliquen el uso y cesión de datos. La realidad es que una de las novedades es introducir a los clásicos pliegos de condiciones un apartado donde expliquen si van a ceder o no datos a terceras empresas. El legislador europeo actual tiene la creencia de que mostrando un pliego explicativo es suficiente para darse por protegido al consumidor. Tener la creencia que el consumidor está protegido obligando a dichas empresas en mostrar esos pliegos jurídicos inmensos y que es efectivo para una correcta protección, es una creencia más que una certeza jurídica alejada de la realidad.

Por ello y aunque existan los derechos ARCO de Acceso, Rectificación, Cancelación y Oposición, **realmente no tenemos un derecho como consumidores de redes a conocer la trazabilidad los dichos datos que volcamos en dicha red**. El hecho de poder tener acceso a una trazabilidad de datos que nos permita saber en todo momento qué tipo de tratamiento tienen los mismos es una necesidad que el legislador debe aportar como un derecho nuevo. Asimismo como también **debería existir un derecho al olvido de metadatos al igual que existe el derecho al olvido en los buscadores como Google**.

Los datos y la finalidad de los mismos son una gran laguna jurídica por regular y que ante al apabullante incremento tecnológico y la creciente monetización y rentabilización de nuestros datos resulta más que necesario una actuación que devuelva al derecho en materia de protección de datos su halo protector que siempre ha tenido.

BIBLIOGRAFÍA

Martínez, G. C. (1989). Generalidades acerca del salario. Revista Facultad de Derecho y Ciencias Políticas, (85), 39-49.

Rodríguez Menjívar, M. D., Sagastume Díaz, R. D., & Alfaro Moreno, C. A. (2004). La inembargabilidad del salario.

Cisneros, J. (2002). El concepto de la comunicación: El cristal con el que se mira. Ámbitos. Revista Internacional de Comunicación, 5, 49-82.

Herreros, M. C. (2008). La Web 2.0 como red social de comunicación e información. Estudios sobre el mensaje periodístico, 14, 345-361.

Rausell Köster, C. (2005). A propósito del discurso interactivo. Anàlisi: quaderns de comunicació i cultura, (32), 147-161.

LASSWELL, Harold. (1986) "Estructura y función de la comunicación en la sociedad". En: Moragas, M. (editor) Sociología de la comunicación de masas II. Estructuras, funciones y efectos. Gustavo Gili. Barcelona.

Berzal, F., & Matín, N. (2002). Data mining: concepts and techniques by Jiawei Han and Micheline Kamber. ACM Sigmod Record, 31(2), 66-68.

Han, J., Kamber, M., & Pei, J. (2011). Data mining concepts and techniques third edition. Morgan Kaufmann.

Nisa Ávila, J. A. (2016). Robótica e Inteligencia Artificial¿ legislación social o nuevo ordenamiento jurídico. Revista El Derecho, Francis Lefebvre

Mena, J. (1999). Data Mining your website. Digital Press.

Muñoz, M. M. (2018). Virtualización del espacio público y concepto débil de privacidad. Lecciones del caso Facebook-Cambridge Analytica. Ensayos de Filosofia, 8(2).

del Risco Montero, L. (2012). Localización de móviles en GSM (Doctoral dissertation, Universidad Central "Marta Abreu" de Las Villas).

Data Policy. (2020). Retrieved 17 February 2020, from https://www.facebook.com/privacy/explanation

BBC News. (2013). Facebook sorry for suicide dating ad. [online] Disponible en: https://www.bbc.com/news/technology-24141835 [Accedido 18 Feb. 2020].

Winston Smith vs Facebook and American Cancer Society. (2018). [ebook] San Francisco: Court for the Northern District of California. Disponible en: https://cases.justia.com/federal/appellate-courts/ca9/17-16206/17-16206-2018-12-06.pdf?ts=1544130056 [Accedido 18 Feb. 2020].

Miguel, C. R. (1994). En torno a la protección de los datos personales automatizados. Revista de estudios políticos, (84), 237-264.

World Internet Users Statistics and 2019 World Population Stats. (2019). Retrieved 18 February 2020, from https://www.internetworldstats.com/stats.htm

CÓMO CUMPLIR LA NORMATIVA DE PROTECCIÓN DE DATOS AL CREAR EL CANAL DE DENUNCIA

ElDerecho.com

Un canal de denuncias, **como hemos publicado en artículos anteriores**, es aquella herramienta que la empresa pone a disposición de los trabajadores, proveedores, o clientes, que permite alertar de manera confidencial sobre cualquier ilegalidad que se haya producido en la organización.

Para que un canal de denuncias reúna todas las garantías que aseguren su eficacia, es necesario que todo el proceso cumpla con los requisitos que establece la normativa sobre Protección de Datos. En el artículo 24 de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), se detalla la regulación de este sistema de denuncias interno.

Canal de denuncias en la Ley Orgánica de Protección de Datos (LOPDGDD)

Establece la LOPDGDD que es lícito crear y mantener un sistema de información a través del cual pueda ponerse en conocimiento de una entidad de Derecho privado, **incluso anónimamente**, la comisión en el seno de esta o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa.

En todo caso, los empleados y terceros deben ser informados acerca de la existencia de este canal de denuncias.

El **acceso a los datos** contenidos en estos sistemas quedará limitado exclusivamente a quienes desarrollen las funciones de **control interno y de cumplimiento**, o a los encargados del tratamiento que se designen a tal efecto. También podrán acceder otras personas (por ejemplo, los abogados de la empresa), cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales.

Si hubiera que adoptar medidas disciplinarias contra un trabajador dentro de la propia empresa, se permitirá el acceso al **departamento de recursos humanos** o al personal con funciones de gestión.

Es imprescindible que la empresa adopte las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias **únicamente durante el tiempo imprescindible** para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

Una vez transcurridos tres meses desde la introducción de los datos de la denuncia, deberá procederse a su supresión del sistema. Con la excepción que permite conservarlos para dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. De este modo, la empresa puede eludir una responsabilidad penal que recaería sobre ella. Transcurrido este plazo, los datos podrán seguir siendo tratados por el órgano al que corresponda la investigación de los hechos denunciados, pero no podrán conservarse en el propio sistema de información de denuncias.

Aquellas denuncias a las que no se haya dado curso, solamente podrán constar de forma anonimizada. Si tienes dudas sobre la mejor manera de anonimizar la información recibida, la Agencia Española de Protección de datos (AEPD) ofrece **esta guía** con todo el proceso.

La Agencia Española de Protección de Datos y los canales de denuncia

En el año 2007 la Agencia Española de Protección de Datos (AEPD) emitió un informe (128/2007) relativo a la creación de sistemas de denuncias internas en las empresas presentadas a través de los sistemas de "whistleblowing", en la que aconsejaba evitar *la existencia de* ***denuncias anónimas****, garantizándose así la exactitud e integridad de la información contenida en dichos sistemas.*

Pero, como hemos visto, este informe ha quedado superado por el artículo 24.1 de la LOPDGDD, que sí permite la denuncia anónima. A pesar de ello, es recomendable que el denunciante se identifique para proteger de manera real sus datos personales. De hecho,

son las empresas las que deberían invitar a los denunciantes para que no utilicen el anonimato, y evitar de esta manera el abuso del canal y que la herramienta quede desvirtuada. Así lo aconseja el Supervisor Europeo de Protección de Datos (SEPD) que aboga por evitar el anonimato para obtener una efectiva protección del denunciante, y poder recabar más información sobre los hechos denunciados.

Forma de comunicar la existencia del canal de denuncias

El Grupo de Trabajo Europeo independiente (GT29), que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales, considera, junto al SEPD y la AEPD, que los titulares de los datos personales deben ser informados tanto de la **existencia del canal de denuncias**, como del **tratamiento de sus datos personales** en relación con cualquier denuncia en la que se vean involucrados.

Más concretamente el SEPD establece que la información ha de ser facilitada en dos fases:

- En una **primera fase**, se deberá informar sobre la implementación del canal de denuncias.

- En una **segunda fase**, en el momento en que se reciba una denuncia, se deberá informar de ello a cada uno de los afectados: denunciante, denunciado, testigos, terceros afectados, etc.

¿En qué momento se debe informar a los titulares de los datos?

Como hemos visto inicialmente el art.24.1 no entra en detalles sobre el momento en el que se debe informar a los titulares de los datos, pero si lo hace el art.13.1 del Reglamento General de Protección de Datos (RGPD) que considera que cuando se obtengan de un interesado datos personales relativos a él, en el mismo **momento en que estos se obtengan**, el responsable deberá informarle sobre los fines del tratamiento, y a qué se destinan estos datos personales.

Pero ¿qué sucede cuando los datos los ha facilitado un tercero que ha puesto la denuncia? ¿En qué momento se debe comunicar al afectado?

En el caso de que los datos se hayan obtenido de terceros, el RGPD en su art.14.3 a) establece lo siguiente: *dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos.*

Este plazo podrá alargarse hasta los tres meses, en aquellos casos en los que se deba realizar una investigación prolongada, por lo que este debería ser el **plazo máximo** de comunicación al interesado.

¿Cuándo debo tener creado el canal de denuncia?

Los empresarios españoles están obligados a incorporar la Directiva (UE) 2019/1937 a su legislación nacional con anterioridad a diciembre de 2021.

Por eso, las entidades públicas y privadas deberán comenzar a cumplir estos requisitos antes del **17 de diciembre de 2021**, excepto las entidades del sector privado que tengan de 50 a 249 trabajadores que tienen de plazo hasta el **17 de diciembre de 2023**.

Si tu empresa está obligada a contar con un canal de denuncias, desde Lefebvre te ofrecemos una herramienta eficiente que cumple con toda la normativa en materia de prevención de delitos, y que garantiza la protección de datos en todo caso.

Más información en **Centinela Canal de Denuncias**.

EL ABOGADO GENERAL DEL TJUE, RESUELVE EN CONTRA DE FACEBOOK

Arán Feijoo Covelo

El abogado General del Tribunal de Justicia de la Unión Europea, Michael Bobek - lo que sería aquí en España el fiscal general del estado- ha declarado que las autoridades nacionales de protección de datos pueden tomar acciones legales contra plataformas de redes sociales como FACEBOOK pese a que su sede social radique en otro estado miembro.

Estas declaraciones figuran en las conclusiones del dictamen que el abogado general ha emitido en contestación a la consulta que el tribunal de apelación Belga realizo el pasado año sobre si el reglamento Europeo de protección de datos, impide a las autoridades nacionales a actuar contra posibles infracciones en el tratamiento transfronterizo de datos personales.

Las declaraciones no son vinculantes sin embargo es una regla no escrita que marcaran la línea en la mayoría de las sentencias del Tribunal de la Unión Europea.

Bobek deja escrito en blanco sobre negro en las conclusiones que "si bien reconoce la competencia General de la autoridad de protección de datos del país donde radique la sede social e la empresa, el concepto de ventanilla única, esto incluye la competencia para emprender acciones legales por infracciones del reglamento.

Tras esto aclara de forma expresa que las autoridades nacionales de protección de datos que puedan estar interesadas tienen unas facultades limitadas frente a la principal en lo que se refiere al tratamiento transfronterizo de datos, pero que sin embargo esto nos e puede entender como una incapacidad para emprender acciones legales en su ámbito y que el deber de cooperación entre las autoridades nacionales cuyo deber es la cooperación estrecha crucial en este ámbito.

Estas conclusiones en el dictamen de contestación a la consulta del tribunal Belga, limitan esta capacidad de las autorida-

des nacionales a cuatro supuestos específicos. En concreto los supuestos serian:

- Cuando el caso se situé fuera del ámbito material del Reglamento General de Protección de datos
- Si se investigan tratamientos transfronterizos de datos por autoridades públicas, en interés público, en el ejercicio de poderes públicos o tratamiento de datos por responsables que no tengan establecimiento en la Unión Europea.
- Cuando se adopten medidas Urgentes o cuando la autoridad principal de protección de datos decida de forma expresa a no tratar un caso.

La importancia de esta declaración radica en el hecho de que en principio las empresas tradicionales tienen radicada su actividad en un país miembro y por tanto su supervisión depende de la autoridad nacional de ese país. Sin embargo en las plataformas tecnológicas en este caso las redes sociales su actividad es global al usar la red y por tanto sucede que se puedan cometer infracciones en otros países en la gestión y tratamiento de datos personales sin embargo al no estar su sede social en eses país es necesario que la autoridad nacional se ponga en contacto con la correspondiente para que esta determine o no si inicia procedimiento contra la empresa.

Este concepto de "Ventanilla única" un solo interlocutor para cada empresa viene dando problemas en las actividades globales de empresas como Facebook desde antes del propio reglamento General de protección de datos cuando la "Comisión de protección de la Vida privada en Bélgica" inicia un procedimiento sancionador contra Facebook por recabar información de los internautas belgas mientras navegaban por internet mediante los denominadas cookies, likes y plug-ins que permiten realizar no solo un seguimiento en la red social de los usuarios de Facebook sino también de aquellos con los que se relacionan mientras navegan aunque no sean usuarios de la red social o no hayan dado permiso para la instalación de estos complementos.

En 2018, la justicia Belga, en primera instancia sentenciaba que la compañía norteamericana cuya sede en Europa se encuentra en Irlanda a modificar sus algoritmos y dejar de rastrear a los usuarios belgas hasta cumplir con la legislación nacional, imponiendo una sanción económica de 250000 € diarios hasta un máximo de 100 millones de euros hasta que cumpliese la sentencia.

Esta Sentencia que el entonces secretario de estado para la defensa de la vida privada **Philippe De Backer** de "Hito para la transparencia" quedo paralizada debido al recurso de apelación que el gigante de la red interpuso alegando que no podían ser juzgadas sus opera-

ciones por un tribunal Belga ya que su sede en Europa estaba en Irlanda y por tanto aplicando en principio de ventanilla única, la competencia correspondía a la comisión para la protección de datos (DPC) Irlandesa.

Este empleo torticero del Reglamento general de protección de datos permitió que Facebook, esquivase la sentencia.

Con la consulta realizada por el tribunal Belga de apelación y el dictamen del abogado general del Tribunal de justicia de la unión europea queda claro que el Reglamento Europeo permite que la autoridad de protección de datos de un estado miembro ejercite acciones judiciales ante los tribunales nacionales en una situación de tratamiento de datos transfronterizo, aunque no sea la autoridad principal siempre que proteja derechos de carácter público de sus ciudadanos.


LEFEBVRE