DATOS, DATOS, DATOS: EL DATO PERSONAL, EL DATO NO PERSONAL, EL DATO PERSONAL COMPUESTO, LA ANONIMIZACIÓN, LA PERTENENCIA DEL DATO Y OTRAS CUESTIONES SOBRE DATOS

Data, data, data: Personal data, non-personal data, composite personal data, anonymization, data ownership and other data issues

Andoni Polo Roca
Abogado

http://dx.doi.org/10.18543/ed-69(1)-2021pp211-240

Recibido: 11.01.2021
Aceptado: 18.06.2021

Resumen

La protección de datos resulta un ámbito en constante crecimiento, debido a las nuevas tecnologías y los peligros que éstas suponen para nuestra privacidad. Como núcleo de la protección de datos, tenemos precisamente eso: el «dato personal». Pero, ¿qué es un dato personal? La respuesta la encontramos en el RGPD, pero es posible que la definición jurídica no cubra todos los datos que sí debería. A ello se le añaden la doctrina del TJUE o la doctrina del TEDH en relación a los «datos relativos a la vida privada y familiar». Junto a ello nos aparecerá, asimismo, el «dato no personal» que también ha sido definido por el Derecho de la UE, y que están fuera de la aplicación del RGPD, pero ¿tienen alguna protección? En ese ámbito irrumpirán los llamados metadatos, que son datos no personales *per se*, pero que pueden suponer una amenaza a la privacidad. Por ello, el TJUE hizo unos pronunciamientos de gran relevancia respecto a esos «datos no personales» (técnicamente), que han derivado en lo que se puede denominar como la teoría del «dato personal compuesto» o «teoría del perfil», un dato que es al mismo tiempo personal y no personal (híbrido); ello

unido a la combinación de datos y a la agregación de datos. En todo ello, también, deberemos tener presente la seudonimización y la anonimización, pero especialmente la posibilidad de reidentificar a una persona. Y, por último, es necesario abordar el análisis relativo a la pertenencia del dato personal y su comercialización, respondiendo para ello a dos preguntas: ¿de quién es el dato?, y ¿son nuestros datos objetos de comercio?

Palabras clave

dato, dato personal, TJUE, anonimiziación, reidentificación

Abstract

Data protection is an area in constant growth, due to new technologies and the dangers they pose to our privacy. At the core of data protection, we have just that: «personal data». But what is a personal data? The answer is found in the GDPR, but the legal definition may not reach all the data that it should. To this is added the doctrine of the CJEU, or the doctrine of the ECHR in relation to «data relating to private and family life». Along with this, we will also see the «non-personal data» that has also been defined by EU law, and that is outside the application of the GDPR, but do they have any protection? In this area, so-called metadata takes relevance, which is non-personal data per se, but which can pose a threat to privacy. For this reason, the CJEU made some highly relevant pronouncements regarding these «non-personal data» (technically), which have resulted in what can be called the theory of «composite personal data» or «profile theory», a data which is both personal and non-personal (hybrid); this coupled with the combination of data and the aggregation of data. In all this, we must also bear in mind the pseudonymization and anonymization, but especially the possibility of re-identifying a person. And finally, it is necessary to address the analysis regarding the ownership of personal data (data ownership) and its commercialization, answering two questions: whose data is it? And are our data objects of commerce?

Keywords

data, personal data, ECJ, anonymization, re-identification

I. INTRODUCCION

Vivimos rodeados de datos, y más en la actualidad. En la denominada Sociedad de la Información, los datos (la información) se han convertido en el epicentro de nuestro día a día, en el petróleo del siglo XXI. Así, hay datos y datos, algunos personales y otros no, pero serán los personales los que sean objeto de especial protección, ya que unidos a ellos tendremos a una persona física, su intimidad y su vida privada.

La protección de datos tiene por objeto el dato personal, pero puede que la concepción jurídica actual que el Reglamento General de Protección de Datos[1] (RGPD) ha dado no alcance a todos los datos que debería. Ahí tendremos la doctrina del Tribunal de Justicia de la Unión Europea (TJUE) y del Tribunal Europeo de Derechos Humanos (TEDH).

En el lado opuesto, en cambio, encontramos el dato no personal, cuya definición también ha sido fijada por el Derecho de la Unión, pero no les es aplicable el RGPD ni su protección, por lo que puede ser debatible si tienen algún tipo de protección o no. Resulta un debate de gran relevancia, por ejemplo, a la hora de saber si en un movimiento internacional de datos resulta aplicable el RGPD (dato personal) o el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un

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

marco para la libre circulación de datos no personales en la Unión Europea (dato no personal).

En esa dicotomía dato personal-no personal, tomarán relevancia los llamados metadatos, que son, en sí mismos, datos no personales; no obstante, si bien son datos no personales, puede que constituyan una gran amenaza para la privacidad de la ciudadanía.

Es ahí donde cobrarán relevancia los pronunciamientos que el TJUE hizo tanto en el año 2014 como en posteriores, que supondrán un dique de contención en un terreno tan farragoso como el de los metadatos y los datos no personales que pueden llegar a ser personales: la que podemos llamar teoría del «dato personal compuesto» o «teoría del perfil». En ello aparecerán cuestiones como la combinación de datos y a la agregación de datos.

Por otro lado, cuestiones como la seudonimización y la anonimización también serán objeto de estudio, especialmente por la posibilidad de reidentificar a una persona, lo cual atacaría directamente su privacidad.

En todo ello, por último, se analizarán también dos cuestiones de gran relevancia en torno a los datos como son la pertenencia del dato personal y su comercialización, respondiendo para ello a dos preguntas: ¿de quién es el dato?, y ¿son nuestros datos objetos de comercio?

Todo ello teniendo como núcleo el dato, que es objeto de lo que se denomina la protección de datos.

II. LA PROTECCIÓN DE DATOS

El derecho fundamental a la protección de datos lo encontramos reconocido, garantizado y protegido tanto en el ámbito nacional, como en el comunitario e internacional, pero son especialmente tres los preceptos más relevantes que lo recogen: el artículo 18.4 de la Constitución (CE), el artículo 8 de la Carta de Derechos Fundamentales de la UE (CDFUE) y el artículo 16 del Tratado de Funcionamiento de la UE (TFUE); un derecho que se ha europeizado según la doctrina[2].

Como notas características de este derecho fundamental, según el Tribunal Constitucional (TC), una de las principales sería que atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos[3], configurándolo, así, como un derecho de prestación.

Se trata, así, de un derecho que comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para

[2] Rallo Lombarte, 2017: 658 y ss.

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

fines distintos de aquel legítimo que justificó su obtención[4], siendo la finalidad de este derecho fundamental «garantizar a la persona un poder de disposición sobre el uso y destino de sus datos con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, garantizando a los individuos un poder de disposición sobre esos datos»[5].

El alto tribunal lo ha definido, por tanto, como el derecho fundamental «dirigido a controlar el flujo de informaciones que concierne a cada persona»[6].

Consiste, en suma, en que la ciudadanía tenga un control total y absoluto sobre sus datos personales.

III. EL «DATO PERSONAL» (TJUE), EL «DATO RELATIVO A LA VIDA PRIVADA Y FAMILIAR» (TEDH), Y EL «DATO NO PERSONAL»

1. *La regulación del «dato personal»: evolución*

El Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal —primera norma vinculante a nivel de Europa en el ámbito de la protección de datos—, actualmente sucedido por el *Convenio n.º 108+* de 2018[7], estableció que por «datos de carácter personal» debía entenderse, a efectos del Convenio, «cualquier información relativa a una persona física identificada o identificable», que la norma denominó «persona concernida» (art. 2).

Por su parte, la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) definió los «datos de carácter personal» como «cualquier información concerniente a personas físicas identificadas o identificables» (art. 3).

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

[4] STC 96/2012, de 7 de mayo, FJ 6º.

[5] STC 17/2013, de 31 de enero, FJ 4º, y STC 292/2000, de 30 de noviembre, FJ 6º, *in fine*.

[6] STC 76/2019, de 22 de mayo, FJ 5.

[7] Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, modificado por el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 108), adoptado por el Comité de Ministros en su Sesión n.º 128ª el 18 de mayo de 2018. Accesible en: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

—primera norma comunitaria en la materia— estableció que por «datos personales», a efectos de la Directiva, se entendía «toda información sobre una persona física identificada o identificable», a la cual denominaba el «interesado» (art. 2).

Del mismo modo lo recogió la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que traspuso la Directiva 95/46/CE; según la LOPD los «datos de carácter personal» eran «cualquier información concerniente a personas físicas identificadas o identificables» (art. 3).

Dicha definición fue ampliada por el Reglamento de la LOPD de 2007[8] (RLOPD), que dio la siguiente definición de «datos de carácter personal»: «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables»[9] (art. 5.1).

2. *La regulación actual del dato personal en el RGPD*

El actual Convenio n.º 108+ de 2018, actualizando la anterior versión de 1981, define los «datos personales» como «cualquier información con respecto a un individuo identificado o identificable», al que denomina «titular de datos» o «interesado» (art. 2)

En lo que respecta al RGPD, éste ha seguido la línea marcada por las normas anteriormente citadas (especialmente por su predecesora, la Directiva 95/46/CE), y ha establecido que «datos personales» son «toda información sobre una persona física identificada o identificable» —el «interesado»— (art. 4, apartado 1, del RGPD).

Tenemos, por tanto, dos tipos de «datos personales»: «toda información sobre una persona física identificada» y «toda información sobre una persona física identificable».

En dicha dicotomía «identificada» e «identificable», el RGPD ha recogido lo siguiente: «considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica,

[8] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[9] En cuanto a la «información acústica» como dato personal, véase: Arzoz Santiesteban, 2010: 149 y ss.

económica, cultural o social de dicha persona» (art. 4, apartado 1, del RGPD)[10].

Por tanto, al hablar de un dato relativo a persona física «identificada», hacemos referencia a un dato que indica directamente a esa persona sin necesidad de acudir a un conjunto de medios para poder averiguar su identidad (entre ellas: el DNI o el pasaporte).

En cambio, al hacer referencia a un dato relativo a persona física «identificable», hablamos de un dato que no indica la identidad de esa persona, ni aporta suficiente información acerca de la misma, pero sí aporta información suficiente para poder averiguar su identidad (la información no es suficiente acerca de la persona y su identidad, pero sí es suficiente para poder averiguar su identidad); así, mediante la utilización de los medios adecuados dicho dato permite la identificación exacta del individuo o persona física («interesado»).

El Grupo de Trabajo sobre Protección de Datos del artículo 29 (en lo sucesivo, GT 29) —en la actualidad, Comité Europeo de Protección de Datos (CEPD)[11]— ha declarado que, en lo que respecta a un dato relativo a una persona física «identificable», aquélla será «identificable» cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo «ble»); así, a juicio del GT 29, esta segunda alternativa es, en la práctica, la condición suficiente para considerar que la información entra en el ámbito de aplicación del tercer componente[12].

De este modo, como hemos mencionado, el RGPD recoge que el dato personal será relativo a una persona física, cuando su identidad puede determinarse, «directa o indirectamente»: por un «identificador» (nombre, número de identificación, datos de localización o un identificador en línea) o por «elementos propios de la identidad» (física, fisiológica, genética, psíquica, económica, cultural o social).

Así, también se ha de subrayar la distinción entre «directa» o «indirectamente»: según el GT 29, una persona «puede ser identificada directamente

[10] Ello es parecido a lo que en su día recogió la Directiva 95/46/CE en su artículo 2, apartado a): «se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

[11] El Grupo de Trabajo sobre Protección de Datos del artículo 29 (GT 29) fue creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, en su artículo 29 (de ahí el nombre). Sin embargo, el RGPD (art. 68-76) ha creado el Comité Europeo de Protección de Datos (CEPD), un organismo europeo independiente que ha venido a sustituir al GT 29 y en el que también se ha incluido el Supervisor Europeo de Protección de Datos (SEPD).

[12] Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 20 de junio, p. 13.

por su nombre y apellidos o indirectamente por un número de teléfono, la matrícula de un coche, un número de seguridad social, un número de pasaporte o por una combinación de criterios significativos (edad, empleo, domicilio, etc.)»[13].

A ello, el RGPD le añade que «para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos» (Considerando n.º 26). Relacionado con ello, el RLOPD de 2007 estableció que una persona física no se considerará identificable «si dicha identificación requiere plazos o actividades desproporcionados» (art. 5.1); no obstante, no se ha pronunciado sobre ese punto el nuevo RGPD.

Sin embargo, será la categoría de «identificada» la más limitada o estricta, y la «identificable» la más extensa u holgada. Así, el DNI únicamente será un dato relativo a persona física «identificada», cuando podemos ver el DNI entero o una foto; no obstante, cuando únicamente podamos ver el número de DNI será un dato relativo a persona física «identificable», ya que habrá que asociar el número de identificación a una persona física —indudablemente, eso sí, será un dato personal, ya sea por una vía o por la otra—.

Por otro lado, los nombres y apellidos también serán datos personales, pero, al igual que con el DNI, pueden serlo por la vía de «identificada» o «identificable»: un nombre y apellidos muy comunes no identifican a una única persona física, sino a todas las personas físicas que lleven dicho nombre (dato de una persona física «identificable», en la que haría falta combinar el nombre y apellidos de la persona con otros datos, como la fecha de nacimiento, dirección postal, fotografía de su rostro, etc.); en cambio, un nombre compuesto con unos apellidos poco comunes serían un dato de una persona física «identificada».

Por ello, el GT 29 se refiere al contexto: así, que el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate[14].

[13] Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 20 de junio, p. 14.

[14] Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 20 de junio, p. 14. El GT 29 pone como ejemplos los siguientes: «un apellido muy común no bastará para identificar a una persona – es decir, para aislarla – dentro del conjunto de la población de un país, mientras que es probable que permita la identificación de un alumno dentro de una clase. Incluso una información auxiliar, como, por ejemplo, «el hombre que lleva un traje negro», puede identificar a alguno de los transeúntes que esperan en un semáforo. Así pues, el que se identifique

Por la vía de dato de una persona física «identificable» tenemos: el ADN, la huella dactilar, el iris del ojo, número de teléfono, el IBAN bancario, dato de localización, etc. Todos ellos son dato personal, ya que permiten determinar la identidad del interesado: la persona física que está detrás de dicho dato.

3. *El «dato personal» en la jurisprudencia y doctrina*

El Tribunal de Justicia de la Unión Europea (TJUE) ha venido declarando que el concepto de dato personal es muy amplio.

Así, según el TJUE, para que un dato pueda ser calificado de «dato personal» no es necesario que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona, ya que el conjunto de los medios que puedan ser razonablemente utilizados para identificar a una persona física pueden ser usados no solo por el responsable del tratamiento, sino, también, por cualquier otra persona[15].

A juicio del TJUE constituyen datos personales las respuestas escritas de un aspirante en un examen profesional y las eventuales anotaciones al respecto del examinador[16], y también, la escritura a mano en algún documento (información sobre su escritura)[17].

Tal como ha declarado el Tribunal de Luxemburgo, además, son datos personales: el nombre de una persona, su número de teléfono y otra información relativa a sus condiciones de trabajo o a sus aficiones[18]; datos sobre movimientos bancarios (ingresos, transferencias, etc.)[19]; datos que obran en

o no a la persona a la que se refiere una información depende de las circunstancias concretas del caso».

[15] STJUE (Sala Segunda), de 20 de diciembre de 2017, asunto C-434/16, Peter Nowak y Data Protection Commissioner, ap. 31 y STJUE (Sala Segunda), de 19 de octubre de 2016, asunto C-582/14, Patrick Breyer y Bundesrepublik Deutschland, ap. 43.

[16] STJUE (Sala Segunda), de 20 de diciembre de 2017, asunto C-434/16, Peter Nowak y Data Protection Commissioner, ap. 36. Así, tal como declara el TJUE, «el contenido de tales respuestas revela el nivel de conocimientos y el grado de competencia del aspirante en un área determinada, así como, en su caso, el proceso de reflexión, el discernimiento y la capacidad de análisis del propio aspirante» (ap. 37), y «mediante la obtención de las respuestas se pretende valorar la capacidad profesional del aspirante y su aptitud para ejercer el oficio de que se trate» (ap. 38).

[17] *ibíd*. En este caso, el TJUE dictamina que «si el examen está escrito a mano, las respuestas contienen, además, información sobre su escritura» (ap. 37); de ello se deduce que la información sobre la escritura es un dato personal.

[18] STJ (Gran Sala), de 6 de noviembre de 2003, asunto C-101/01, caso Göta hovrät (Suecia) c. Lindqvist, ap. 24.

[19] STJ (Gran Sala), de 20 de mayo de 2003, asuntos acumulados C-465/00, C-138/01 y C-139/01, caso Österreichischer. Rundfunk y otros, ap. 64.

poder del municipio, como el nombre o domicilio[20]; información relativa a los perfiles creados en la red social por los clientes de ésta (los perfiles de usuario de las redes sociales)[21]; datos conseguidos por un detective privado[22]; los datos que figuran en un registro del tiempo de trabajo que se refieren a los períodos de trabajo diario y a los períodos de descanso de cada trabajador[23]; la imagen de una persona grabada por una cámara[24]; los datos fiscales[25]; datos que figuran en una minuta (nombre, fecha de nacimiento, nacionalidad, sexo, etnia, religión e idioma, etc.)[26]; etc.

También debemos tomar por datos personales: la dirección de correo electrónico (siempre que en la misma dirección de correo electrónico aparezca el nombre de la persona física en cuestión), datos de localización (como la función de los datos de localización de un teléfono móvil), el identificador de una cookie, o el identificador de la publicidad del teléfono.

Por otro lado, el Tribunal Europeo de Derechos Humanos (TEDH) ha considerado que son «datos relativos a la vida privada y familiar»: las comunicaciones escritas o habladas e imágenes[27], las filmaciones[28] o sonidos[29] de circuito cerrado de televisión, etc.

Resulta necesario mencionar que, a diferencia de en España y en la UE, en el TEDH (y en el CEDH) no existe el «derecho de protección de datos» como derecho autónomo; el TEDH únicamente analiza si ha habido vulneración o no del derecho al respeto a la vida privada y familiar (art. 8 del

[20] STJ (Sala Tercera), de 7 de mayo de 2009, asunto C-553/07, caso Rijkeboer, ap. 42.

[21] STJUE (Sala Tercera), de 16 de febrero de 2012, asunto C-360/10, caso SABAM c. Netlog NV, ap. 49.

[22] STJUE (Sala Tercera), de 7 de noviembre de 2013, asunto C-473/12, caso IPI, ap. 26.

[23] STJUE (Sala Tercera), de 30 de mayo de 2013, asunto C-342/12, caso Worten y ACT, ap. 19.

[24] STJUE (Sala Cuarta), de 11 de diciembre de 2014, asunto C-212/13, caso František Ryneš y Úřad pro ochranu osobních údajů, ap. 22.

[25] STJUE (Sala Segunda), de 27 de septiembre de 2017, asunto C-73/16, caso Peter Puškár y otros, ap. 41 y STJUE (Sala Tercera), de 1 de octubre de 2015, asunto C-201/14, caso Bara y otros, ap. 29.

[26] STJUE (Sala Tercera), de 17 de julio de 2014, asuntos acumulados C-141/12 y C-372/12, caso YS c. Minister voor Immigratie, Integratie en Asiel S (C-141/12) y caso Minister voor Immigratie, Integratie en Asiel c. M y S (C-372/12), ap. 38.

[27] STEDH (Sección Tercera), de 24 de junio de 2004, asunto Von Hannover c. Alemania; STEDH (Sección Cuarta), de 11 de enero de 2005, asunto Sciacca c. Italia.

[28] STEDH (Sección Cuarta), de 28 de enero de 2003, asunto Peck c. el Reino Unido; STEDH (Sección Quinta), de 5 de octubre de 2010, asunto Köpke c. Alemania.

[29] STEDH (Sección Tercera), de 25 de septiembre de 2001, asunto P.G. y J.H. c. el Reino Unido, ap. 59 y 60; STEDH (Sección Segunda), de 20 de diciembre de 2005, asunto Wisse c. Francia.

CEDH), por lo que no hay «datos personales» *per se*, sino «datos relativos a la vida privada y familiar».

Por último, también la dirección de protocolo de internet (IP) de un ordenador, según el Tribunal Supremo (TS), son datos personales, ya que contienen información concerniente a personas físicas identificadas o identificables[30], siguiendo el mismo criterio que el TJUE, que ya lo venía declarando[31] y ya confirmó dejando clara su posición al respecto[32].

De igual modo se pronunció el TEDH, considerando las direcciones IP como «datos relativos a la vida privada y familiar»[33].

Los datos personales objeto de tutela, por lo tanto, serán toda aquella información sobre una persona física identificada o identificable (art. 4, apartado 1, del RGPD), es decir, todos aquellos que identifican o permitan identificar a cualquier persona[34]. La información del dato personal debe, así, poder vincularse a una persona[35].

4. *El «dato no personal»: ¿sin protección?*

Dicho todo ello, interpretando el artículo 4, apartado 1, del RGPD *a contrario sensu*, el «dato no personal» será el que no identifique a una persona física o no proporcione elementos suficientes para averiguar la identidad de la persona física, o, también, no exista una probabilidad razonable de que se utilicen medios para identificar a una persona física.

[30] STS 3896/2014, de 3 de octubre, FJ 4º (rec. n.º 6153/2011) «estimamos que las direcciones IP son datos personales, en el sentido del artículo 3.a) LOPD y, como tales, se encuentran protegidos por las garantías establecidas por dicho texto legal para su tratamiento».

[31] STJUE (Sala Tercera), de 24 de noviembre de 2011, asuntos acumulados C-468/10 y C-469/10, caso ASNEF y FECEMD y Administración del Estado y otros, y TJUE, Conclusiones del Abogado General, asuntos acumulados C-468/10 y C-469/10, caso ASNEF y FECEMD y Administración del Estado y otros, ap. 61.

[32] STJUE (Sala Segunda), de 19 de octubre de 2016, asunto C-582/14, Patrick Breyer y Bundesrepublik Deutschland, ap. 47 a 49. En este caso el TJUE no es tan claro como el TS, pero concluye que todos los proveedores de servicios de medios *on line* pueden llegar a identificar a las personas físicas a través de las direcciones IP por el mero hecho de que existan mecanismos a través de los cuales los proveedores de acceso a Internet puedan llegar a proporcionar su identidad.

[33] STEDH (Sección Cuarta), de 24 de abril de 2018, asunto Benedik c. Eslovenia, n.º 62357/14, par. 130 a 134. En este caso, según el TJUE la información del abonado asociada a la dirección IP está bajo la protección de artículo 8 de la CEDH.

[34] STEDH, de 16 de febrero de 2000, Amann c. Suiza, n.º 27798/1995, par. 65; y STC 292/2000, de 30 de noviembre, FJ 6º. También SAN de 24 de enero de 2003, nº rec. 400/2001, FJ 5º.

[35] *Cfr*. Arias Pou, 2016: 118 y Piñar Mañas, 2010: 193 y 194.

Así, en esos casos estaremos ante un «dato no personal», fuera de la aplicación del RGPD. En este caso, por ejemplo, si se hiciera algún movimiento de estos datos, sería de aplicación el citado Reglamento (UE) 2018/1807, y no el RGPD, pero si fueran «personales», se aplicaría el RGPD.

El Reglamento (UE) 2018/1807, además, no ha definido precisamente el «dato no personal», sino que ha definido el «dato» desde una nota negativa: «datos» son «los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679» (art. 3).

No obstante, aunque se trate de un «dato no personal», no significa que no esté protegido, ya que, si bien su consideración como tal lo excluye del ámbito de protección del RGPD y del derecho a la protección de datos, no lo excluye del ámbito de protección de otros como el derecho a la intimidad, por lo que quedaría amparado por el derecho al respeto a la vida privada y familiar (art. 8 del CEDH), dentro de los «datos relativo a la vida privada y familiar».

IV. EL «DATO PERSONAL COMPUESTO»: LA TEORÍA DEL «DATO COMPUESTO» O «TEORÍA DEL PERFIL»

1. *El caso Digital Rights Ireland y Seitlinger y otros (2014)*

Debemos traer a este trabajo el caso *Digital Rights Ireland y Seitlinger y otros*[36] del año 2014. Esta resolución invalidó la Directiva de Conservación de Datos del año 2006[37] en su totalidad. No obstante, lo relevante a efectos de este análisis es la fundamentación jurídica del TJUE.

La sentencia que anulaba la mencionada Directiva, se basaba fundamentalmente en la vulneración de dos derechos fundamentales: el respeto de la vida privada y familiar (art. 7 de la CDFUE) y la protección de datos de carácter personal (art. 8).

En dicho pronunciamiento el TJUE estableció una doctrina de gran importancia que ha venido repitiendo: «Estos datos [datos de comunicaciones electrónicas], considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las

[36] STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y Seitlinger y otros.

[37] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 , sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan»[38].

Ahí tenemos una idea de vital importancia respecto a la protección de datos: «considerados en su conjunto».

Esta sentencia de 2014 versaba sobre los datos relativos a las comunicaciones (o «metadatos»); es decir, todos aquellos que nos encontraremos cada vez que se produzca una comunicación electrónica[39] (una llamada telefónica, por ejemplo): fecha y hora de la comunicación, duración, destinatario, número marcado, lugar de la llamada, etc. Todos los que nos encontraremos en las comunicaciones encaminadas a través de una red de telecomunicaciones.

Como hemos mencionado en el anterior apartado, un «dato no personal» es el que no identifica ni permite identificar a una persona física y que no está bajo la protección del RGPD ni del artículo 8 del CDFUE. En este caso preciso la duración de una llamada telefónica («metadatos») es un «dato no personal», ya que él solo, por sí mismo, ni identifica ni permite identificar a una persona física.

Sin embargo —aquí es donde adquiere relevancia el pronunciamiento del TJUE—, todos los datos de tráfico «considerados en su conjunto» constituyen un «dato personal», ya que permiten identificar a una persona física.

De este modo, podemos estar ante un dato personal «simple» o «compuesto»: una dirección IP o número de teléfono (dato simple) que tiene un titular y sólo sería necesario comprobar quién es el titular —buscando el número de teléfono, por ejemplo, en los listines telefónicos[40] o en buscadores—, con lo que estaríamos hablando de una persona física identificable; o bien, otros datos de tráfico que «considerados en su conjunto» (fecha y hora de la comunicación, duración, etc.), permiten identificar a una persona física (el dato personal es el derivado del conjunto de estos datos de tráfico, como un «perfil»[41]).

---

[38] STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger y otros, ap. 27. También: STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB y Secretary of State for the Home Department y otros, ap. 99.

[39] Son «datos de tráfico»: «cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma», art. 2 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), modificada en 2009.

[40] Listines telefónicos con números de teléfono particulares (conocidas popularmente como «Páginas Blancas») o con anuncios y teléfonos corporativos (conocidas popularmente como «Páginas Amarillas»).

[41] Aunque lo denominemos «perfil», estamos en un caso distinto del concepto «elaboración de perfiles» del artículo 4, apartado 4, del RGPD; no debemos confundirlos. A efectos

Así, un sólo dato (duración de la llamada) no sería un dato personal («dato no personal») porque no permite identificar a una persona física, pero, «considerados en su conjunto» (la fecha, más la hora, más la duración, más el lugar, etc.), estaríamos ante una información sobre una persona física identificable.

2. *El «dato personal compuesto»*

Con el «dato personal compuesto», paradójicamente, tendremos varios «datos no personales» que conforman un «dato personal». Pasa, así, de estar fuera de la protección de datos, a estar bajo el ámbito de protección del RGPD y del artículo 8 de la CDFUE.

Por tanto, el «dato personal compuesto», será aquel que está compuesto por varios «datos no personales» (ya que no identifican ni permiten identificar a una persona física), pero que al considerarlos en su conjunto conforman un dato personal.

Esto tiene una relevancia máxima en el ámbito de los datos personales, ya que pueden darse fraudes de ley al RGPD, ya que, en este aspecto, encontramos un vacío legal o laguna legal en el reglamento.

Así, cogiendo como ejemplo un movimiento de estos datos, al tratarse de «datos no personales» sería de aplicación el Reglamento (UE) 2018/1807, excluyendo el RGPD y su régimen mucho más exigente y garantista.

Sin embargo, el «dato personal compuesto» es un dato personal, pero formado por «datos no personales»; ello puede dar lugar a hacer movimientos de «datos no personales» bajo la aplicación del Reglamento (UE) 2018/1807 («norma de cobertura»), cuando, en realidad, lo que se está produciendo es un movimiento ilícito, ya que el régimen aplicable es el del RGPD («norma eludible o soslayable»), al ser un dato personal.

De este modo, se daría la «fragmentación» del dato compuesto y su conversión a varios «datos no personales», eludiendo el RGPD, pero, en realidad, se estaría haciendo uso de datos personales.

Pero no es solamente aquella situación la única que puede darse, sino que también las empresas o los poderes públicos pueden hacer uso de estos datos a

---

del RGPD, por «elaboración de perfiles» debe enterderse «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física» (art. 4, apartado 4, del RGPD). De este modo, se parte de «datos personales» para elaborar el perfil que evalúa distintos aspectos personales de una persona física. En cambio, en este caso, es diferente a ello, porque partimos de distintos «datos no personales» y conjuntamente conforman un «datos personal» que permite identificar a una persona física, y, además, conocer detalles muy precisos sobre la vida privada de la persona física en cuestión.

© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 69/1, enero-junio 2021, págs. 165-194
http://dx.doi.org/10.18543/ed-69(1)-2021pp211-240 • http://www.revista-estudios.deusto.es/

voluntad, porque jurídicamente, *de iure*, no son datos personales («datos no personales»), mas, *de facto*, sí lo son (no por sí mismos, sino su combinación).

En cambio, esta doctrina del TJUE abre la puerta a controlar dichas situaciones, para no dejar sin protección a la ciudadanía; en especial, para garantizarle a la persona el poder de controlar el flujo de informaciones (datos) que le concierne y de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado[42].

V. LOS «METADATOS», LA «AGREGACIÓN DE DATOS» Y SU CLAVE: «CONSIDERADOS EN SU CONJUNTO»

Esta cuestión en torno a los datos relativos a las comunicaciones (o «metadatos») ha sido puesto de relieve también por el Consejo de Derechos Humanos (CDH) de las Naciones Unidas: «la agregación de la información comúnmente conocida como «metadatos» puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada»[43].

Así, estarán en juego los «metadatos»: la información que «rodea» una llamada (en este caso); no obstante, va mucho más allá de las llamadas.

El consultor tecnológico estadounidense Edward Snowden definió «metadatos» como «registros de actividad»[44]; es decir, todos aquellos datos que «rodean» una actividad (en el caso de una llamada, éstos serían: la fecha y hora, la duración el destinatario, etc.).

Los «metadatos», sin embargo, no está presentes únicamente en las comunicaciones electrónicas, sino en cualquier actividad: al sacar una fotografía (hora y fecha de la fotografía, lugar, tamaño de imagen, resolución y dimensiones, etc.), al publicar un tweet en Twitter (hora y fecha del tweet, lugar, cantidad de caracteres, etc.), al enviar un correo electrónico (hora y fecha, destinatario, etc.), al enviar un mensaje en WhatsApp, etc. Todos esos metadatos quedan registrados.

También la navegación (búsquedas) en Internet: el buscador utilizado, URL visitada, hora y fecha de la búsqueda, etc.

---

[42] STC 17/2013, de 31 de enero, FJ 4º, y STC 292/2000, de 30 de noviembre, FJ 6º, *in fine*.

[43] Véase: Consejo de Derechos Humanos (CDH) de las Naciones Unidas. Informe de la Oficina del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital, de 30 de junio de 2014, A/HRC/27/37, nº 19.

[44] *Cfr*. El tweet en la red social Twitter de Edward Snowden (@Snowden): «Are your readers having trouble understanding the term «metadata»? Replace it with «activity records.» That's what they are. #clarity» 11:15 p. m. • 2 nov. 2015. Accesible en: https://twitter.com/Snowden/status/661305566967562240

Como declaró el CDH, el problema aparecerá al hacer uso de la «agregación de datos», que se basa en recopilar esa información para preparar conjuntos de datos.

Así, las grandes cantidades de datos (de metadatos en este caso), y su transferencia al servidor del agregador, pueden conformar un perfil completo de una persona física e identificarla[45].

No obstante, los todo ello no identifica solamente a una persona física, sino que, también ofrece detalles muy íntimos sobre la vida privada de la persona física que se haya identificado: el destinatario de una llamada, o el lugar de una llamada, además de identificar a una persona, pueden decirnos qué aficiones tiene, dónde trabaja, quiénes son sus amigos o pareja, etc. Todo ello partiendo de los datos de las bases de datos de los registros de una comunicación electrónica (u otra: navegación *web*, etc.).

De este modo, un estudio realizado por Jonathan Mayer, Patrick Mutchler, y John C. Mitchell[46] demostró que únicamente con los metadatos de una llamada (sin el contenido), además de identificar a una persona, se podía saber que la persona en cuestión padecía esclerosis, tenía armas de fuego, o que había abortado[47].

Si bien todo, los metadatos son «datos no personales» y, por ello, están fuera de la aplicación del RGPD. Sin embargo, el TJUE abrió la puerta a aplicar el RGPD, ya que «considerados en su conjunto» constituyen un dato personal.

En términos generales, ya sea un metadato o cualquier otro dato, que éste no sea «personal» no significa que carezca de valor: dicha información

[45] Véase: Vartanian y Ledig, 2000.

[46] El estudio se encuentra en el siguiente trabajo: Mayer, Jonathan, Mutchler, Patrick y Mitchell, John C. 2016. «Evaluating the privacy properties of telephone metadata». *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, 113, n.º 20. https://doi.org/10.1073/pnas.1508081113

[47] En este caso, los resultados del estudio fueron los siguientes (*vid*. Mayer, Mutchler y Mitchell, 2016):

«i) El *participante A* mantuvo conversaciones con una farmacia especializada en atención crónica, un servicio para pacientes que coordina el manejo de afecciones graves, varias prácticas de neurología local y una línea directa farmacéutica para un medicamento recetado que se utiliza únicamente para controlar los síntomas y la progresión de múltiples remisiones y recaídas. esclerosis. [...];

iii) El *participante C* realizó llamadas frecuentes a un distribuidor local de armas de fuego que anuncia de manera destacada una especialidad en la plataforma de rifle semiautomático AR. También realizó largas llamadas a la línea directa de atención al cliente de un importante fabricante de armas de fuego; el fabricante produce una popular línea de rifles AR. [...];

v) La *participante E* hizo una larga llamada telefónica a su hermana una mañana temprano. Luego, 2 días después, llamó varias veces a una clínica de planificación familiar y de aborto (*Planned Parenthood clinic*) cercana. Dos semanas más tarde, realizó breves llamadas adicionales a la clínica de planificación familiar y de aborto, y realizó otra llamada breve un mes después».

seguirá teniendo un inmenso valor, aunque en ámbito jurídico no pueda ser calificado de «personal».

VI. EL CRUCE DE DATOS Y LA COMBINACIÓN DE DATOS

Como ya hemos mencionado, un único metadato no es un dato personal, pero al cruzarlo o combinarlo con otros metadatos de una actividad concreta permite identificar a una persona física y, además, conocer muchos detalles sobre su vida privada, conformando un dato personal.

En este aspecto, cobran relevancia el cruce de datos o la combinación de datos, al igual que la agregación de datos respecto a los metadatos.

El análisis de datos da lugar a muchas situaciones que amenazan nuestra privacidad, por ejemplo: hacer uso de algoritmos para construir una «ficha» personal de un sujeto en base a «datos no personales» (a efectos del RGPD) que éste deja al navegar por Internet, por ejemplo.

Así, haciendo uso de «datos no personales», se pueden combinar de modo que lleguen a identificar a una persona, y , también, saber dónde vive, dónde trabaja, con quién tiene relaciones de amistad o románticas, etc.

Únicamente es necesario para ello seguir el rastro de «datos no personales», combinarlos y ello construye, no solo «datos personales», sino conocer los detalles más íntimos de una persona.

El RGPD no ha regulado estos aspectos tan técnicos, pero sí les ha hecho mención. En su Considerando n.º 30 ha recogido que «las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet [dirección IP], identificadores de sesión en forma de *cookies* [cookie de identificación] u otros identificadores, como etiquetas de identificación por radiofrecuencia [RFID]». Como ya hemos mencionado, las citadas en dicho considerando son *per se* «datos personales».

No obstante, sigue el Considerando n.º 30, y establece que todo ello «puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas».

Hablamos, por tanto, paradójicamente, de identificar a personas físicas a través de «datos no personales», lo cual escapa al RGPD. Es por ello que la puerta que abrió el TJUE en el año 2014 es de una relevancia máxima.

VII. LA ANONIMIZACIÓN DE DATOS: ¿FUNCIONA?

1. *La «anonimización» y la «seudonimización»*

En primer lugar, en lo que a la «anonimización» respecta, debemos distinguirla de la «seudonimización».

La «seudonimización» puede ser definida por un «medio camino» entre la «anonimización» y el «dato personal»; se trata de una técnica para ocultar identidades, y su finalidad es poder recopilar más datos sobre una misma persona sin necesidad de conocer su identidad[48].

Así, por «seudonimización», a efectos del RGPD, debemos entender: «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable» (art. 4, apartado 5, del RGPD).

De este modo, en la «seudonimización» no hay una disociación absoluta e irreversible, ya que también se almacenará información adicional a dichos datos (por separado y sujeta a estrictas medidas de seguridad), por lo con ésta última siempre se puede identificar al interesado. Por ello, el RGPD también recoge que se deberá mantener «por separado la información adicional para la atribución de los datos personales a una persona concreta» (Considerando n.º 29).

Así, todas las técnicas de seudonimización tendrán una información adicional aparte o método (*v. g*. una clave) adicional que permitirá identificar a la persona física que está detrás del dato seudonimizado[49].

De este modo, el RGPD establece una diferencia muy relevante la técnica de seudonimización y la de anonimización: la seudonimización, a diferencia de la anonimización, sí es considerada un «dato personal», ya que, mediante la información adicional, se puede llegar identificar a una persona física, por lo que el dato es relativo a una persona física identificable (art. 4, apartado 1, del RGPD)[50].

Mediante esta técnica el reglamento quiere otorgar mayor protección a los interesados, porque, si bien se consideran datos personales, el acceso está restringido a determinadas personas autorizadas, lo cual reduce el riesgo en el tratamiento (*vid*. Considerando n.º 28). Además, el RGPD pretende incentivar el uso de esta técnica, mediante obligaciones menos estrictas en ciertos tratamientos[51].

---

[48] Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 20 de junio, p. 19.

[49] Las técnicas de seudonimización más utilizadas son las siguientes: el cifrado con clave secreta, la función hash, la función hash «con sal», la función con clave almacenada, el cifrado determinista o función hash con clave con borrado de clave, y la descomposición en tokens. *vid*. Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 10 de abril de 2014, pp. 22 y 23.

[50] Así, debemos tener en cuenta también el Considerando n.º 26 del RGPD: «los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable».

[51] Por ejemplo, en lo que respecta al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, el RGPD permite hacer

2. *La «anonimización»*

Un dato «anonimizado» es aquel que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona[52]. Con la «anonimización» sí se da la disociación absoluta e irreversible; de este modo, esos datos no pueden asociarse con el interesado, es decir, con la persona física (ni identificarla).

La Agencia Española de Protección de Datos (AEPD) ha definido el «proceso de anonimización» como «la ruptura de la cadena de identificación de las personas»[53]; así, el objetivo es evitar la reidentificación de las personas, disociándose el dato de la persona física en cuestión.

El GT 29 ha declarado que el objetivo de la anonimización es impedir de forma irreversible la identificación del interesado; es decir, obtener una desidentificación irreversible[54].

Así, ha puesto el acento, específicamente sobre tres criterios o tres riesgos clave de la anonimización, que son los que pueden asegurar si se ha logrado la disociación y la desidentificación irreversible y absoluta: la «singularización», la «vinculabilidad» y la «inferencia» («riesgo de singularización», «riesgo de vinculabilidad» y «riesgo de inferencia»)[55].

No obstante, el GT 29 también se ha pronunciado sobre el riesgo implícito del proceso de anonimización, expresando que se ha de tener en cuenta la identificabilidad, el contexto y las circunstancias particulares de cada caso,

---

uso de los datos seudonimizados con finalidades distintas a la recogida (ello siempre con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos), lo cual es inconcebible en el tratamiento ordinario. Cfr. art. 89.1 del RGPD.

[52] Dictamen 4/2007 sobre el concepto de datos personales, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 20 de junio, p. 23.

[53] AEPD. 2019. «Orientaciones y garantías en los procedimientos de anonimización de datos personales», p. 2. https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf

[54] Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 10 de abril de 2014, p. 7.

[55] Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 10 de abril de 2014, p. 12: «Singularización: la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros) que identifican a una persona.

Vinculabilidad: la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas. Si el atacante puede determinar (p. ej., mediante un análisis de correlación) que dos registros están asignados al mismo grupo de personas pero no puede singularizar a las personas en este grupo, entonces la técnica es resistente a la singularización, pero no a la vinculabilidad.

Inferencia: la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos»

no basta con eliminar los elementos que pueden servir para identificar directamente a una persona, sino que harán falta medidas adicionales para evitar dicha identificación[56].

Por su parte, la AEPD ha declarado que será suficiente que exista la mera posibilidad, incluso remota, de que, mediante la utilización, con carácter previo, coetáneo o posterior de cualquier medio (proceso informático, programa, herramienta del sistema, etc.), la información concerniente a los titulares de los datos pueda revelar la identidad de estos, para que quede plenamente sometida a la normativa en materia de protección de datos[57].

Por otro lado, la anonimización «absoluta» o la desidentificación irreversible «absoluta» tiene una restricción: el TJUE en el caso *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*[58] de 2009 declaró que se deben conservar los datos en un formato identificable a fin de que puedan ejercerse, por ejemplo, los derechos de acceso por parte de los interesados[59]. Y así lo ha remarcado el GT 29 expresando que la anonimización ha de ajustarse a las restricciones legales marcadas por el TJUE[60].

Por tanto, mantener la posibilidad de identificar a la persona conlleva que ese dato sea un dato personal, y, por ello, resulta aplicable el régimen del RGPD, y ello no casa del todo con la disociación «absoluta» y extrema que exige la anonimización.

Con todo, sí la anonimización consiste en la disociación irreversible del dato de la persona física en cuestión con la correspondiente desintentificación absoluta, pero el TJUE y el GT 29 han subrayado que se debe mantener una posibilidad de identificación para que el interesado pueda ejercer sus

[56] Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 10 de abril de 2014, pp. 9 y ss.

[57] AEPD. Informe 0283/2008 de la Agencia Española de Protección de Datos. Accesible en: https://www.aepd.es/es/documento/2008-0283.pdf

[58] STJUE (Sala Tercera), de 7 de mayo de 2009, asunto C-553/07, College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer.

[59] STJUE (Sala Tercera), de 7 de mayo de 2009, asunto C-553/07, College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer, ap. 70: «El artículo 12, letra a), de la Directiva obliga a los Estados miembros a garantizar un derecho de acceso a la información sobre los destinatarios o categorías de destinatarios a quienes se comunican los datos y al contenido de la información comunicada, no sólo para el presente, sino también para el pasado. Corresponde a los Estados miembros fijar un plazo de conservación de dicha información, así como el acceso correlativo a ésta, guardando un justo equilibrio entre, por un lado, el interés del afectado en proteger su intimidad, concretamente a través de las distintas vías de intervención y de recurso previstas por la Directiva y, por otro, la carga que la obligación de dicha información puede representar para el responsable del tratamiento».

[60] Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 10 de abril de 2014, p. 8.

derechos, no estaríamos ante una anonimización *per se*, sino ante una seudonimización.

Por otro lado, cierto es que si mediante la técnica de anonimización se consigue la disociación absoluta, sin ningún, absolutamente ningún resquicio para la reidentificación, ello supondría que no fuera un dato personal, al no poder identificarse a la persona física que hay detrás de aquél, y, por consiguiente, no sería de aplicación el RGPD, ni los derechos del interesado, ni la exigencia del TJUE; no obstante, como ya se ha mencionado, será suficiente que exista la mera posibilidad, incluso remota, de que los datos puedan revelar la identidad de la persona física, para que sea aplicable el RGPD, y los derechos del interesado, en cuyo caso se debería acudir a la seudonimización.

3. *La «reidentificación»*

Como hemos analizado, la anonimización tiene por objeto, y como razón de ser misma, la imposibilidad absoluta de «reidentificación» (al ser la base de aquélla la disociación del dato de la persona y la desidentificación irreversible).

Sin embargo, una anonimización diseñada defectuosamente da lugar a la posibilidad de reidentificar a las personas[61], con lo que es aplicable el RGPD.

En el año 2000, un estudio de la Profesora de la Universidad de Harvard Latanya Sweeney analizó los datos del censo de EEUU de 1990, y descubrió que el 87,1 por ciento de la ciudadanía estadounidense se podía identificar de manera única combinando tres datos[62]: su código postal de EEUU[63] (cinco dígitos), fecha de nacimiento (incluido el año), y sexo.

Pero, además, incluso con datos menos específicos se podía identificar a una persona: el 58,4 por ciento de la ciudadanía seguía siendo identificable con una combinación de ciudad[64], fecha de nacimiento y sexo; y el 18,1 por cierto con una combinación de condado, fecha de nacimiento y sexo

[61] Como ejemplo de una anonimización diseñada defectuosamente véase: Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 10 de abril de 2014, p. 19.

[62] *Cfr*. Sweeney, 2000.

[63] Es importante matizar este dato, ya que dicho código postal de EEUU (*five-digit ZIP code*, en inglés) es mucho más específico que el CP en España: así, el ZIP estadounidense identifica también un segmento geográfico dentro de un área, como puede ser una manzana (*residential block* o, simplemente, *block*, en inglés), un grupo de apartamentos, un apartado postal, etc.

[64] En este caso la ciudad es menos específica que el ZIP estadounidense (*Cfr*. nota anterior).

—incluso un 0,04 porciento con la combinación de condado, sexo, y mes y año de nacimiento—[65].

A ello se le añade un estudio del año 2006 de Philippe Golle que confirmaron los resultados del estudio de la Profesora Latanya Sweeney[66], si bien, en este caso, se analizó los datos del censo de EEUU del año 2000, por lo que hay una pequeña variación en el porcentaje[67].

La Profesora Latanya Sweeney trató de demostrar que la anonimización no aseguraba la imposibilidad absoluta de reindetificación. Y, en 1996, lo demostró de la siguiente manera[68]:

> «En Massachusetts, una agencia gubernamental aseguradora llamada *Group Insurance Commission* (*GIC*) contrató un seguro médico para los empleados estatales. A mitades de 1990, la agencia GIC publicó datos anónimos que mostraban las visitas al hospital de empleados estatales (registros de visitas al hospital), para que estuvieran disponibles a efectos de investigación.
>
> Al eliminar los campos que contienen nombre, dirección, número de seguro social y otros «identificadores explícitos», dicha agencia asumió

[65] Sweeney, 2000: 30 y 31. Así, la autora concluyó lo siguiente: «*Experiment B reported that 87.1% (216 million of 248 million) of the population in the United States had characteristics that were likely made them unique based only on {*5-digit ZIP, gender, date of birth*}. [...] Experiment F reported that 58.4% of the population in the United States had characteristics that were likely made them unique based only on {*Place, gender, date of birth*}. [...] Experiment J reported that 18.1% of the population in the United States had characteristics that were likely made them unique based only on {*County, gender, date of birth*}. Experiment K reported that 0.04% of the population in the United States had characteristics that were likely made them unique based only on {*County, gender, Month and year of birth*}. Experiment L reported that 0.00004% of the population in the United States had characteristics that were likely made them unique based only on {*County, gender, Year of birth*}. Experiment M reported that 0.00000% of the population in the United States had characteristics that were likely made them unique based only on {*County, gender, 2year age range*}, but despite it being a very small number, it is not 0.*».

[66] Golle, 2006.

[67] Golle, 2006: 80. El autor explica que la variación se basa en los distintos censos (1990 y 2000) utilizados en ambos estudios: «*We show that in 2000, only 63% of the US population is uniquely identifiable by {gender, ZIP code, full date of birth}, whereas [10] found 87% uniquely identifiable by the same characteristics in 1990. Unfortunately, we lack detailed information about the methodology and data collection of [10], so we can offer no definite explanation for this discrepancy. We speculate however that the discrepancy might come in part from the fact that the 1990 census does not directly tabulate data by ZIP codes: Summary Tape File 1, which contains 100% of the 1990 census data, can not be queried by ZIP code. A smaller set of sample data from the 1990 census data, in Summary Tape File 3, can be queried by ZIP code, but gives only a coarser representation of the age distribution of individuals (ages are aggregated in 5 year intervals)*».

[68] Ohm, 2010: 1719 y 1720.

> que había protegido la privacidad del paciente, a pesar de que todavía se incluían «casi cien atributos por» paciente y visita al hospital, incluido el trío crítico de código postal, fecha de nacimiento y sexo.
>
> En el momento en que GIC dio a conocer los datos, William Weld, entonces gobernador de Massachusetts, aseguró al público que GIC había protegido la privacidad del paciente mediante la eliminación de identificadores. En respuesta, entonces, la Profesora Latanya Sweeney (estudiante de posgrado, por aquel entonces) comenzó a buscar los registros médicos del gobernador en los datos de GIC.
>
> Sabía que el gobernador residía en Cambridge (Massachusetts) una ciudad de cincuenta y cuatro mil residentes y siete códigos postales. Por veinte dólares, compró las listas de votantes completas de la ciudad de Cambridge, una base de datos que contiene, entre otras cosas, el nombre, la dirección, el código postal, la fecha de nacimiento y el sexo de cada votante. Al combinar estos datos con los registros de GIC, Sweeney encontró al gobernador William Weld con facilidad. Solo seis personas en Cambridge compartieron su fecha de nacimiento; solo tres eran hombres, y de los tres, solo él vivía en su código postal. Sweeney envió los registros de salud del gobernador (incluidos diagnósticos y recetas) a su oficina».

De esta manera, la profesora Sweeney demostró al gobernador que estaba equivocado, al encontrar sus registros médicos en el conjunto de datos y enviárselos a su oficina. Después, en el citado estudio del año 2000, demostró que la reidentificación de datos supuestamente anonimizados era posible (como ya se ha visto).

Dicho supuesto mencionado es el denominado «anonimato k»[69], que es, en sí, una técnica de anonimización; una técnica de anonimización que puede dar lugar a la reidentificación, por lo que no cumpliría la exigencia básica de la anonimización: disociación irreversible e imposibilidad absoluta de reidentificación[70].

De este modo, en general, se ha afirmado que los datos que tradicionalmente no se consideran datos personales, aún se pueden usar para identificar a las personas combinando datos supuestamente anónimos con información externa[71].

[69] Dictamen 05/2014 sobre técnicas de anonimización, del Grupo de Trabajo sobre Protección de Datos del artículo 29, de 10 de abril de 2014, p. 37 y ss.

[70] Sobre el modelo de protección de «anonimato k», en relación a los ataques y formas de evitar estos ataques, véase: Sweeney, 2002.

[71] Ohm, 2010: 1723 y 1724. Así, el autor concluye que puede que todo sean datos personales para aquellos que tengan acceso a la información externa correcta («*These results suggest that maybe everything is personal identifying information (PII) to one who has access to the right outside information*»).

Ello responde a combinar o cruzar datos, con otros conseguidos de manera externa, lo cual hoy es más probable y fácil que nunca, especialmente por la información que ofrecen los motores de búsqueda, por ejemplo; ello supone un alto grado de lo que el GT 29 denomina «riesgo de la vinculabilidad».

Este es el caso del Instituto Nacional de Estadística (INE), el cual para miles de estudios estadísticos hace uso de datos anonimizados, pero existe un gran problema: el INE tiene miles de bases de datos de la ciudadanía que fácilmente puede cruzar o combinar con los datos supuestamente anonimizados (la denominada información externa).

Por tanto, la anonimización no es un espejismo, ni un mito. No obstante, que los datos recopilados se hayan anonimizado no significa que la privacidad de las personas en cuestión esté a salvo o que no haya ninguna posibilidad de reidentificar a las personas.

VIII. LA PERTENENCIA DEL DATO PERSONAL: ¿DE QUIÉN ES EL DATO?

En lo que respecta a la pertenencia del dato, ésta resulta una cuestión bastante debatida, desde el punto de vista jurídico como el filosófico.

En primer lugar, aunque le «demos» «nuestros» datos personales a un responsable del tratamiento para que los trate, los datos siguen siendo «nuestros», sólo los facilitamos para un fin predeterminado[72]. El hecho de que esos datos personales estén en posesión del correspondiente responsable del tratamiento, no lo convierte en «dueño» de esos datos ni de esa información; siguen siendo «nuestros».

En segundo lugar, tal como afirman algunos autores, cabe decir que cada uno es «dueño» de sus datos, en tanto en cuanto cada uno tiene el control y disposición absoluto de sus datos personales (por ello ha de dar su consentimiento para que se traten, o para que se exploten, etc.), pero eso no quiere decir que los datos personales sean, realmente, una «propiedad»[73].

Un dato personal, como puede ser un nombre y apellidos, puede ser de más de una persona, por lo que no es posible decir que hay un «derecho dominical» exclusivo sobre aquél.

Así, según se ha afirmado, una cosa es que esos datos identifiquen a una persona (y por eso se protegen), y otra cosa es que sean «nuestros» o «de nuestra propiedad»; así, no se protegen los datos en sí, sino que se protege la identidad, el honor y la intimidad de la persona que está detrás del dato[74]. Por

[72] Del Peso Navarro, 1998.

[73] Adsuara Varela, 2018.

[74] Adsuara Varela, 2018. En este caso, el autor lo explica de manera brillante de la siguiente manera: «Si alguien le preguntara a Angela Merkel cuál es su país, ella diría que

tanto, se debe entender que «los datos no son de nadie», y que «la pregunta clave no es «¿de quién son los datos?», sino «¿a quién afectan los datos?»»[75].

Otros sostienen, además, que considerar los datos como «privados», nos configura como «dueños» o «propietarios» de dichos datos, y ello puede derivar en un mercado, al tomarlos por objetos de comercio[76]. Se ha considerado que «los datos también son una propiedad moral hasta que son extraídos, momento en el que tendrían que convertirse en un bien común»; así, «ser susceptibles de suministrar datos no nos convierte en sus dueños, sino en sus responsables»[77].

En todo ello, por otro lado, debemos tener en cuenta que un dato personal no es solo «nuestro»: el ADN contiene información genética de una persona y de sus familiares, un dato de geolocalización también es el dato de las personas que estén con la persona en cuestión, la dirección de residencia habitual es también el dato de los convivientes con dicha persona física, etc. Por ello, no somos «dueños» ni «propietarios» de «nuestros» datos personales; no nos «pertenecen», sino que nos «afectan».

Así, tenemos el control y disposición absoluta sobre un dato personal, en tanto en cuanto éste nos afecta al hacer posible nuestra identificación o la averiguación de detalles íntimos sobre nuestra vida privada. En cambio, no tenemos el control o disposición sobre ese mismo dato personal cuando éste afecte a otra persona y no a la persona que está decidiendo sobre aquél —si no, estaríamos decidiendo sobre la vida de otra persona—; es por ello, que no es posible hablar de «pertenencia» del dato, ya que, si no, daríamos una especie de «carta blanca» para destruir la esfera íntima o vida privada de otra persona, porque al tener un «dominio» sobre el dato, podríamos decidir sobre un dato que afecta a la vida privada de otra persona.

Todo ello sin tener en cuenta, asimismo, que la aceptación de una especie de «derecho dominical» sobre un dato personal nos llevaría directos al comercio de datos, al igual que al comercio de órganos humanos.

Por tanto, no se debe centrar el debate en la «pertenencia» del dato, sino en la «afectación» del dato; el objeto protegido no es (paradójicamente) el dato, sino la persona que hay detrás de éste —sujeto protegido—.

Alemania. ¿Pero eso quiere decir que Alemania es suya, en el sentido de propiedad? No, simplemente indica un vínculo entre un sujeto y un dato, pero el dato (Alemania) no es de nadie y está vinculado también a todos los que tienen esa nacionalidad. Cuando rellena un formulario y en la casilla del sexo pone mujer, ¿quiere decir que el dato mujer es suyo, de su propiedad o compartido con todas las mujeres? Y lo mismo podríamos decir de cualquier característica física: la altura, el peso, el color del pelo o de los ojos; datos que no son propiedad de nadie en exclusiva».

[75] *ibíd*.

[76] Lafuente, 2020.

[77] *ibíd*.

IX. ¿SON NUESTROS DATOS OBJETOS DE COMERCIO?

Teniendo en cuenta que, desde el punto de vista económico, estos datos tienen un enorme valor económico (ya que es de donde más beneficios pueden sacar las empresas), una cuestión interesante en relación a los datos personales es si pueden ser considerados objetos de comercio o no, desde el punto de vista jurídico.

Según se ha afirmado, puede que una empresa prestadora de un servicio obtenga beneficio económico de la cesión (para su tratamiento) de los datos personales que hagan sus clientes (vía publicidad de terceros, por ejemplo, que se ofrecerá sobre dichos datos personales), lo que supondría que hubiese dos prestaciones por parte de ambas partes contractuales (cliente-empresa / interesado-responsable del tratamiento): la del servicio y la cesión de los datos que lo permite[78].

El RGPD ha recogido el «consentimiento del interesado» como una mera «manifestación de voluntad» (art. 4, apartado 11, del RGPD), pero no ha previsto el consentimiento en los casos que los datos personales puedan ser considerados objeto contractual.

Esta naturaleza jurídica resulta, cuanto menos, discutible. Si consideramos que tiene una naturaleza estrictamente contractual, desde una perspectiva *iusprivatista*, convertiríamos los datos personales en objetos puramente de consumo y mercantiles y, al estar éstos bajo la protección de los poderes públicos según el mandato del artículo 18.4 de la CE, el 8 de la CDFUE y el 16 del TFUE, no podemos considerarlos como objetos exclusivamente privados, ya que, si así fuera, los poderes públicos no tendrían obligación de control sobre ellos y el mercado predominaría en una materia tan sensible como nuestros datos de carácter personal.

Hablamos, en casos como el de la «prestación de servicios a cambio de privacidad» (cuando ya se esté pagando dicho servicio por el cliente).

En relación con este aspecto, el CEPD ha declarado que para que el consentimiento se manifieste libremente, en términos del RGPD, el acceso a los servicios y funcionalidades no puede supeditarse a que el usuario preste su consentimiento al almacenamiento de información, o al acceso a la información ya almacenada, en el equipo terminal del usuario (las denominadas «barreras de cookies»)[79]. Por ello, tal como declaró el GT 29 también, la no aceptación de las cookies no puede llevar la denegación total del servicio, ya que, si no, el consentimiento no se daría de forma libre[80].

---

[78] Aparicio Vaquero, 2015: 207 y 208. En este caso preciso, el autor se refiere especialmente a los servicios de la Sociedad de la Información en relación a los datos personales.

[79] Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, del Comité Europe de Protección de Datos, de 4 de mayo de 2020, p. 11.

[80] Documento de Trabajo 02/2013 que proporciona orientación sobre cómo obtener el consentimiento para las cookies, del Grupo de Trabajo sobre Protección de Datos del ar-

Así, según la AEPD, no se puede denegar el servicio en caso de no aceptación de las cookies, pero sí se puede ofrecer una alternativa de servicio para el caso de no aceptación de las cookies[81,82].

De este modo, no es posible que un prestador de servicio (que ya se está pagando por el cliente) utilice, además, los datos personales del cliente como contraprestación, ya que en ese caso obtendría un rédito económico de la contraprestación económica por parte del cliente por la prestación del servicio, por un lado, y de el uso de sus datos personales, por otro. Así, un servicio de la Sociedad de la Información, por ejemplo, prestado normalmente a título oneroso[83], deberá basar dicha onerosidad o en la contraprestación económica o en el uso de los datos personales; ambas resultarían muy gravoso para la persona en cuestión[84].

Por otro lado, además, es difícilmente creíble que sea una función legítima de quien suministra un servicio —para lo cual el interesado les ha facilitado sus datos— comerciar con éstos; ello excede con mucho la finalidad[85].

X. CONCLUSIONES

En primer lugar debemos decir que la regulación actual del RGPD en relación a lo que es un dato personal, ha seguido el esquema básico que siguieron sus antecesoras: «toda información sobre una persona física identificada o identificable»; un concepto que es muy amplio según el TJUE. Tal consideración de «datos personal» traerá la aplicación del RGPD y estar en el ámbito de la protección de datos. A ello se le añaden los «datos relativos a la vida privada y familiar» (TEDH).

En segundo lugar, tenemos el «dato no personal», que ha sido definido desde una nota negativa (todos son datos, menos los que son aquéllos que son

tículo 29, de 2 de octubre de 2013, p. 3.

[81] AEPD. 2020. «Guía sobre el uso de las cookies», p. 30. https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf

[82] La AEPD pone el ejemplo de supuestos en los que la denegación de acceso impediría el ejercicio de un derecho legalmente reconocido al usuario, por ser, por ejemplo, el acceso a un sitio web el único medio facilitado al usuario para ejercitar tal derecho.

[83] Esta es la definición que da la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico en su artículo 1 en relación a los servicios de la Sociedad de la Información («todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario»).

[84] Aparicio Vaquero defiende que dicha onerosidad de los SSI, en los casos en los que el servicio sea (aparentemente) «gratuito», se basa en el uso de nuestros datos personales, de ahí que, aunque en principio parezca «gratuito», en servicio en realidad, es a título oneroso. Vid. Aparicio Vaquero, 2015: 207 y 208.

[85] Del Peso Navarro, 1998.

datos personales). No obstante no debemos olvidar que, si bien éstos no quedarán bajo la aplicación del RGPD, ello no significa que quedarán sin protección ninguna, al quedar bajo el ámbito del derecho al respeto a la vida privada y familiar.

En tercer lugar, tenemos los metadatos y la agregación: datos no personales que están presentes en toda actividad y que mediante la agregación pueden identificar a una persona física, y, además, dar detalles concisos sobre su vida privada. Por ello, los pronunciamientos del TJUE adquieren gran relevancia al declarar que dichos datos no personales «considerados en su conjunto» son un dato personal. Ahí es donde aparecerá la teoría del «dato personal compuesto» o «teoría del perfil».

Dicho «dato personal compuesto» será curiosamente un dato personal construido a partir de distintos datos no personales (de su combinación), una especie de «dato personal no personal». Ello puede dar lugar a hacer usos o transferencias ilícitas de dichos datos por parte de empresas o Estados, al no ser datos personales *de iure*, pero sí *de facto*. Por ello, ahí cobrará su mayor relevancia la doctrina del TJUE sobre los datos personales compuestos.

Que un dato no sea «personal» no significa que carezca de valor: dicha información seguirá teniendo un inmenso valor, aunque en ámbito jurídico no pueda ser calificado de «personal» (salvo por la doctrina del TJUE). Es cierto, no obstante, que el TJUE debería profundizar más en dicha doctrina, para abrir la doctrina de los metadatos a todos aquellos datos no personales que puedan constituir un dato personal, y, por su parte, el RGPD debería hacer lo propio.

En cuarto lugar tenemos la anonimización y la seudonimización, o los datos anonimizados y los datos seudonimizados. Éstos son datos personales, ya que uniendo la información adicional al dato seudonimizado se puede llegar a identificar a una persona; aquéllos, en cambio, no son datos personales.

No obstante, la base de la anonimización será la disociación irreversible y la imposibilidad absoluta de reidentificación, y ello, a veces, puede fallar, por lo que no sería ya un dato anonimizado, sino un mero dato personal sujeto al RGPD. Así, que los datos recopilados se hayan anonimizado no significa que la privacidad de las personas en cuestión esté a salvo o que no haya ninguna posibilidad de reidentificar a las personas. Cualquier resquicio de reindentificación, incluso el más mínimo o remoto, nos lleva a la aplicación del reglamento.

En quinto lugar, en lo que respecta a la pertenencia del dato personal, debemos hablar no de «pertenencia» del dato, sino en la «afectación» del dato, ya que lo que se protege es la persona que está detrás, no el mismo dato. No podemos considerar el dato como algo privado sobre el cual tenemos un dominio exclusivo; el dato no nos pertenece, ya que, si no, ello nos daría poder sobre la esfera íntima de otras personas que tienen el mismo dato que el nuestro.

Por último, en cuanto a considerar nuestros datos objeto de comercio, no hay una respuesta clara en el Derecho; sin embargo, sí podemos decir que en los servicios onerosos, la onerosidad deberá recaer o sobre el rédito económico sacado del uso de nuestros datos personales o sobre la contraprestación económica del cliente a cambio del servicio, pero no ambas, y, además, no podemos considerar nuestros datos como objeto de comercio.

En general, cabe mencionar que el «mundo de los datos» (en este caso el su dimensión jurídica) es extenso, y se plantean miles y miles de cuestiones jurídicas, éticas y filosóficas. Cierto es que el RGPD ha sentado un pilar fundamental en aquél, pero sigue habiendo algún vacío, como los que hemos mencionado en el presente trabajo, en los que el dato «puede escapársenos».

Concluimos pues que en el «mundo de los datos» el hoy siempre será el ayer, y que a veces el Derecho no puede prever todos los avances que se dan a diario, pero, al menos, lo debe intentar: está en juego la privacidad de la ciudadanía.

XI. BIBLIOGRAFIA

Adsuara Varela, Borja. 2018. «¿Nuestros datos son realmente nuestros?». *EL PAÍS Retina: transformación digital y tecnología*. Acceso el 28 de noviembre de 2019. https://retina.elpais.com/retina/2018/02/14/tendencias/1518586501_637288.html

Aparicio Vaquero, Juan Pablo. 2015. «Cuestiones de Derecho aplicable y responsabilidad de los prestadores de servicios de red social y de sus usuarios». En *En torno a la privacidad y la protección de datos en la sociedad de la información*, coordinado por Juan Pablo Aparicio Vaquero y Alfredo Batuecas Caletrío, 187-231. Granada: Colmares.

Arias Pou, María. 2016. «Definiciones a efectos del reglamento general de protección de datos». En *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*, dirigido por José Luis Piñar Mañas, y coordinado por María Álvarez Caro y Miguel Recio Gayo, 115-134. Madrid: Reus.

Arzoz Santiesteban, Xabier. 2010. *Videovigilancia, seguridad ciudadana y derechos fundamentales*. Cizur Menor (Navarra): Thomson Reuters Civitas.

Del Peso Navarro, Emilio. 1998. «¿De quién son nuestros datos». *Revista En Línea Informática, Informáticos Europeos Expertos (IEE)*, n.º 19. http://www.iee.es/pages/bases/articulos/hemeroteca/derint004.html

Golle, Philippe. 2006. «Revisiting the Uniqueness of Simple Demographics in the U.S. Population». *Proceedings of the Fifth ACM Workshop on Privacy in Electronic Society (WPES)*, '06, 77–80. https://doi.org/10.1145/1179601.1179615

Lafuente, Antonio. 2020. «Cuerpo común y soberanía tecnológica». *Ctxt*, n.º 261. Acceso el 28 de noviembre de 2019. https://ctxt.es/es/20200601/Firmas/32582/cuerpo-tecnologia-datos-control-coronavirus-futuro-antonio-lafuente.htm

MAYER, Jonathan, MUTCHLER, PATRICK Y MITCHELL, John C. 2016. «Evaluating the privacy properties of telephone metadata». *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, 113, n.º 20. https://doi.org/10.1073/pnas.1508081113

OHM, Paul. 2010. «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization». *UCLA Law Review*, Vol. 57: 1701-1777. https://ssrn.com/abstract=1450006

PIÑAR MAÑAS, José Luis. 2010. «Concepto de datos de carácter personal: Título I. Disposiciones Generales. artículo 3». En *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, dirigido por Antonio Troncoso Reigada, 183-213. Madrid: Civitas.

RALLO LOMBARTE, Artemi. 2017. «De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018)». *Revista de derecho político*, n.º 100: 639-669. https://doi.org/10.5944/rdp.100.2017.20713

SWEENEY, Latanya. 1997. «Weaving Technology and Policy Together to Maintain Confidentiality». *Journal of Law, Medicine & Ethics*, 25 (2-3): 98-110. https://doi.org/10.1111/j.1748-720X.1997.tb01885.x

—— 2000. «Uniqueness of Simple Demographics in the U.S. Population». *Laboratory for Int'l Data Privacy* (Carnegie Mellon University), Working Paper LIDAP-WP4.

—— 2002. «k-anonymity: a model for protecting privacy». *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10 (5): 557-570. https://doi.org/10.1142/S0218488502001648

VARTANIAN, Thomas P. y LEDIG, Robert H. 2000. «Scrape It, Scrub it and Show It: The Battle Over Data Aggregation». http://www.ffhsj.combancmail/bmarts/abaart.htm

DATOS, DATOS, DATOS: EL DATO PERSONAL, EL DATO NO PERSONAL, EL DATO PERSONAL COMPUESTO, LA ANONIMIZACIÓN, LA PERTENENCIA DEL DATO Y OTRAS CUESTIONES SOBRE DATOS

Data, data, data: Personal data, non-personal data, composite personal data, anonymization, data ownership and other data issues

Andoni Polo Roca
Abogado

http://dx.doi.org/10.18543/ed-69(1)-2021pp211-240