



Universidad
Zaragoza

Trabajo Fin de Grado

El *profiling* en el Reglamento General de Protección de Datos

Autor/es

PABLO SOSTRES LARROSA

Director/es

José Félix Muñoz Soro

Facultad de Derecho / Universidad de Zaragoza
2018

ÍNDICE

SIGLAS Y ABREVIATURAS.....	2
I. INTRODUCCIÓN.....	3
II. EL <i>PROFLING</i> O ELABORACIÓN DE PERFILES.....	5
II. 1.- BREVE HISTORIA Y DEFINICIÓN DEL PROFILING	5
II.2- TIPOS DE <i>PROFILING</i>	9
II.3- RIESGOS DEL <i>PROFILING</i>	11
III. LA REGULACIÓN EN EL RGPD.....	13
III.1. PRINCIPIOS DE PROTECCIÓN CON INCIEDENCIA EN LA CREACIÓN DE PERFILES	15
III.1.1- LICITUD, LEALTAD Y TRANSPARENCIA	15
III.1.2- FINALIDAD DE RECOGIDA Y TRATAMIENTO	19
III.1.3.- MINIMIZACIÓN DE DATOS O <i>DATA MINIMISATION</i>	21
III.1.4- EXACTITUD.....	22
III.1.5.- SEGURIDAD.....	24
III.2- PREVISIONES ESPECÍFICAS: EL ARTÍCULO 22 RGPD	25
III.2.1- ALCANCE.....	25
III.2.2- CONTENIDO	27
III.2.3.- CONTROVERSIA, PROHIBICIÓN O DERECHO A OPONERSE	29
III.2.4.- EXCEPCIONES A LA “PROHIBICIÓN”	31
III.2.5- CONCLUSIONES RELATIVAS AL ARTÍCULO 22 RGPD.....	32
III.3. DERECHOS DEL AFECTADO.....	33
III.3.1. DERECHO A SER INFORMADO	33
III.3.2. DERECHO DE OPOSICIÓN	36
III.3.3. OTROS DERECHOS	37
IV. CONCLUSIÓN.....	39
BIBLIOGRAFÍA	41
ANEXOS	46
ANEXO I- Extracto del borrador del RGPD elaborado por el Parlamento Europeo .	46
ANEXO II- Ejemplo de datos personales utilizados en la toma de decisiones automatizadas	51

SIGLAS Y ABREVIATURAS

RGPD: 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). También mencionado como «Reglamento General de Protección de Datos», o por sus siglas inglesas al ser abordado por documentos en dicho idioma, «GDPR»

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (Texto consolidado. Última modificación: 5 de marzo de 2011)

WP29: Grupo de Trabajo del Artículo 29, por sus siglas en inglés *Article 29 Working Party*

ICO: *Information Commissioner's Office* Autoridad Independiente de Protección de Datos de Reino Unido.

AEPD: Agencia Española de Protección de Datos

TJUE: Tribunal de Justicia de la Unión Europea

TICs: Tecnologías de la información y la comunicación.

I. INTRODUCCIÓN

CUESTIÓN TRATADA

El presente trabajo aborda el estudio de la técnica de *profiling* o creación de perfiles desde un punto de vista jurídico y especialmente centrado en el impacto sobre el mismo producido tras la aprobación del Reglamento General de Protección de Datos, comenzado a aplicar el pasado 28 de mayo de 2018.

El RGPD contiene provisiones relativas al *profiling* que, si bien encuentran su antecedente más cercano en la ya lejana Directiva 95/46/CE aprobada hace más de 20 años, suponen un nuevo hito legislativo en tanto en cuando la materia es abordada de forma directa por primera vez en la historia legislativa europea.

Partiendo de una inicial puesta en contexto y explicación de la técnica de creación de perfiles, el núcleo duro del análisis se centrará en las previsiones del artículo 22 RGPD en materia de decisiones automatizadas vinculadas al *profiling*, así como en un desarrollo sobre los principios de protección y derechos del interesado que resultan de relevancia en el tema.

RAZÓN DE ELECCIÓN DEL TEMA Y JUSTIFICACIÓN DE SU INTERÉS

En materia legislativa y especialmente en el ámbito de la UE, veinte años suponen un gran lapso temporal: durante ese periodo nuestra Unión se ha enfrentado a dos grandes crisis y a una de las mayores recesiones de la historia del capitalismo a nivel mundial. Veinte años en el ámbito tecnológico, por otra parte, suponen todo un mundo.

Es en este panorama de constante cambio y evolución cuando nace el RGPD, fruto del propósito de sustituir a una directiva que trató de hacer frente a una revolución en su más tierna infancia. La nueva norma busca reforzar los derechos de los ciudadanos europeos en materia de privacidad a la par que aunar esta mayor protección con el desarrollo de la economía digital de nuestro tiempo.

La revolución (pues crecimiento parece un término insuficiente para definir este fenómeno) que ha supuesto el desarrollo de las tecnologías de la información y la comunicación posiblemente sea de una magnitud que incluso a día de hoy somos incapaces de comprender, una revolución a la que el legislador nunca (o casi nunca) ha

podido seguirle el ritmo, y menos cuando hablamos de regulación europea, donde el consenso fundamenta la adopción de nuevas normas y donde tan difícil es llegar al mismo.

En definitiva, el desarrollo de las nuevas tecnologías y, entre ellas, técnicas como la de *profiling*, supone toda una revolución cuyo alcance está aún por descubrir, pero cuyos interrogantes jurídicos comienzan a hacer acto de presencia.

METODOLOGÍA SEGUIDA EN EL DESARROLLO DEL TRABAJO

Tal y como puede desprenderse de la propia estructura de este análisis, el presente trabajo ha seguido muy de cerca las previsiones presentes en el RGPD realizando un análisis que sigue esencialmente el patrón de la norma, si bien centrado en ciertas disposiciones concretas (por ejemplo, artículos 5 y 6 en materia de principios de protección) y también en las expresiones presentes en los considerandos como fuentes de interpretación de la norma.

El principal obstáculo encontrado ha sido la falta de literatura sobre *profiling* en el marco legislativo europeo, muy posiblemente por la novedad del tema ya que, como se mencionaba anteriormente, no ha sido hasta el RGPD cuando el legislador ha abordado este campo de forma expresa. De esta forma, los documentos a partir de los cuales se ha reflexionado son esencialmente guías jurídicas de organismos europeos como el WP29 o de entidades gubernamentales entre las que destaca el ICO por su extensa labor divulgativa de las novedades en materia de protección de datos que ha supuesto la nueva norma europea. No obstante, algunos de estos documentos han sido considerados con una cierta cautela pues su carácter de *compliance* les ha obligado a adoptar una posición cautelosa frente a ciertas actuaciones que no necesariamente tiene por qué coincidir plenamente con los derechos y obligaciones contenidos en el RGPD.

Señalar de igual forma la especial relevancia de los documentos que han precedido al actual RGPD, especialmente los borradores y enmiendas del Parlamento Europeo y la Comisión, que han permitido observar las distintas posturas sobre el tema que poseían ambas instituciones así como las visiones que han logrado imponerse en el texto definitivo.

En segundo lugar, de especial relevancia habría resultado para el análisis observar la interpretación en sede judicial que se pueda realizar en materia de *profiling*, si bien debido de nuevo a la novedad de la norma esto ha sido imposible, ni tan siquiera extrapolando

conceptos de decisiones judiciales recaídas en base a previsiones de la Directiva 95/46/CE. El seguimiento de la actividad judicial, así como de la actividad legislativa de los Estados Miembros se postula como una interesante forma de analizar la concreción y acierto de lo expuesto a lo largo de este trabajo.

II. EL *PROFLING* O ELABORACIÓN DE PERFILES

II. 1.- BREVE HISTORIA Y DEFINICIÓN DEL PROFILING

La historia del *profiling*, perfilado o creación de perfiles en sus términos más amplios no es otra que la de la propia evolución de la sociedad. Desde su aparición en nuestro mundo, el ser humano se ha visto en la necesidad de reducir la complejidad de un entorno que le exige constantemente tomar decisiones. Es en este entorno donde aparece la categorización o generalización, por la cual todos procedemos a evaluar todo aquello que nos rodea con el objetivo de poder tomar decisiones racionales, algo que como Schauer¹ afirmaba, nos permite superar los obstáculos diarios de nuestra vida.

La clave reside, defiende el autor, en la base sobre la que cimentamos dichas categorizaciones, las cuales pueden resultar en la creación de un conocimiento acertado o no dependiendo de si para ello se ha partido de la experiencia y, a través de esta, de la estadística. Piénsese en los estereotipos raciales como ejemplo de una mala categorización basada en análisis subjetivos sin base fáctica, o, por el contrario, en la aversión general hacia ciertas especies animales (reptiles como las serpientes) debido a su potencial peligrosidad, independientemente de si en el caso concreto dicha regla resulta adecuada (siguiendo el ejemplo anterior, especies no venenosas e inofensivas para el ser humano). De esta forma, el *profiling* orgánico² (*profiling* realizado directamente por seres vivos) sería un ejemplo precursor de las actuales técnicas, un mecanismo de supervivencia que nos ha acompañado desde que el ser humano llegó a este mundo.

Aunque algunos autores hablan de casos en momentos históricos tan lejanos como el reinado del emperador Calígula o los años en los que actuó la Inquisición Española, el

¹ SCHAUER F., *Profiles, probabilities and stereotypes*, Harvard University Press, Cambridge, 2006

² HILDEBRANDT, M. *Defining profiling: a new type of knowledge?*, *Profiling the European Citizen*, Springer, 2008, pags 17-45.

florecimiento de las técnicas de creación de perfiles llegó en los años 70³ de la mano del FBI (*Federal Bureau of Investigation*) en su vertiente criminal. Expertos como el Dr. Douglas Kelly, psicólogo renombrado por su papel en los juicios de Núremberg, recuperaron los estudios de autores de siglos pasados, y con los conocimientos de la criminología y la psicología de la época trataron de poner en valor técnicas que poco tienen que ver con el análisis estadístico del *profiling* actual, pero que aspirarían a crear perfiles comportamentales de sujetos altamente peligrosos con el objetivo de identificar a los mismos incluso antes de la perpetración del propio delito. La mayoría de los autores contemporáneos consideran que dichas técnicas han quedado anticuadas y si bien mantienen un cierto peso en la investigación criminal, existen dudas acerca de su utilidad y grado de acierto en sus resultados.

Con la aparición de internet, la acumulación masiva de datos y el crecimiento exponencial de la potencia computacional, las técnicas de minería de datos y creación de perfiles han sufrido un salto cuantitativo en la medida en la que se parte de cantidades de datos nunca antes vistas, pero especialmente cualitativo ya que se logra una eficiencia y una profundidad o alcance en el análisis que hasta hace unos años sólo eran imaginable desde un punto de vista meramente teórico.

Las bases del análisis ahora efectuado distan mucho de los juicios sociales o estudios psicológicos de los que hablábamos anteriormente y se insertan en el marco de la evidencia matemática y estadística, pudiéndose comprobar de forma certera y cuasi absoluta la calidad del trabajo realizado y de las correlaciones halladas. La precisión que el análisis puede llegar a obtener, combinada con la velocidad en su obtención y con la cantidad masiva de datos analizados fundamentan los pilares de lo que ya se está denominando la cuarta revolución industrial⁴.

Al igual que ocurre con cualquier concepto jurídico, la definición y delimitación del objeto del estudio resulta de vital importancia, siendo en muchas ocasiones no coincidentes las acepciones que una palabra puede poseer a nivel social y jurídico. En el ámbito de las tecnologías de la comunicación y la información estas divergencias pueden llegar a alcanzar su cénit al ser conceptos complejos que muchas veces el propio

³ TURVEY, B.E., *Criminal profiling: an introduction to behavioural evidence analysis*, Elsevier, 2012, p. 34

⁴ OGURO, K. *Big Data - Key to the 4th Industrial Revolution*, 2016, Revista *Innovation in the Global Economy*, nº3, 2016.

legislador no llega a comprender en su totalidad y que se encuentran en constante cambio, por no decir que el anglicismo que presenta el campo de estudio complica todavía más una eventual traducción.

El *profiling* o la aplicación de técnicas de perfilado de datos podría definirse de forma general como el proceso por el cual se descubren correlaciones entre datos (normalmente de carácter masivo) con la posibilidad de que dichas correlaciones sean usadas para identificar o categorizar sujetos humanos -o no humanos- de forma individual o grupal y/o aplicar perfiles para individualizar o representar a un sujeto o identificar al mismo como miembro de un grupo concreto.

Como se ha anticipado ya, es precisamente este carácter innovador del *Big Data* y el análisis conocido como *data mining* lo que ha supuesto una ruptura con las técnicas anteriores y un avance en materia de *profiling*. A este respecto, BEYER, M.A. y LANEY, D. (2012)⁵ definen en su obra *The Importance of 'Big Data': A Definition* el *Big Data* o datos masivos como un conjunto de datos tan grandes y variados que aplicaciones informáticas tradicionales de procesamiento de datos no son suficientes para tratar con ellos en un periodo de tiempo operacional, siendo necesario un análisis matemático y estadístico que se aleja de las técnicas tradicionales utilizadas hasta la fecha.

Precisamente éste análisis será el proporcionado mediante el *data mining*, que no es sino una etapa dentro de un proceso mayor llamado extracción de conocimiento en bases de datos (*Knowledge Discovery in Databases*) según MOLINA FÉLIX, L.C. (2002)⁶ en su obra “*Data mining: torturando a los datos hasta que confiesen*”. Lo que en verdad hace el *data mining* es reunir las ventajas de varias áreas como la estadística, la Inteligencia Artificial, o el procesamiento masivo, principalmente usando como materia prima las bases de datos, para hallar una serie de correlaciones que pueden ser usadas con fines muy diversos (lucha contra el fraude fiscal, técnicas de marketing, análisis de costes, etc.). Estas correlaciones no resultan aparentes al ojo humano y es imposible (o improbable) que puedan ser descubiertas mediante un examen manual humano de los mismos.

Puede identificarse ya una primera conexión entre *profiling* y *data mining*: el *profiling* añadiría al proceso de *data mining* el propósito de utilizar las correlaciones logradas en

⁵ BEYER, M.A., LANEY, D., *The Importance of 'Big Data': A Definition*, Gartner, 2012

⁶ MOLINA FÉLIX, L.C., “*Data mining: Torturando los datos hasta que confiesen*”, Prensas de la Universitat Oberta de Catalunya, 2002, <<http://www.uoc.edu/web/esp/art/uoc/molina1102/molina1102.html>>, consultado el 19 de mayo de 2018.

análisis anteriores u orientar esos mismos análisis hacia la identificación o categorización a un individuo mediante la identificación del mismo con un perfil de comportamiento, económico, social, etc. determinado.

En términos simplificados, el *profiling* permitiría a un analista categorizar a una serie de sujetos (piénsese por ejemplo en un grupo de consumidores de un determinado país) en base a una serie de correlaciones descubiertas a raíz de datos sobre su persona de acuerdo con un perfil basado en dichas correlaciones (por ejemplo, perfil de consumidores veganos concienciados con el medioambiente). A través de esta técnica, un sujeto (como podría ser una cadena de alimentación) sería capaz de identificar a otros (consumidores) como miembros de ese grupo concreto (consumidores veganos concienciados con el medioambiente).

Como puede observarse, esta definición resulta demasiado general y necesita ser concretada para que en un estudio desde el punto de vista legal como el aquí abordado pueda ser de utilidad.

La definición más interesante, circunscrita ya al ámbito de la protección de datos europeo, es la empleada por el Grupo de Trabajo del Artículo 29 (WP29)⁷: el término *profiling* hace referencia a cualquier forma de procesamiento automatizado de datos personales con el propósito de analizar o predecir la personalidad o ciertos aspectos personales relativos a una persona natural, en particular el análisis y predicción de la salud de una persona, su situación económica, su rendimiento en el trabajo, sus preferencias o intereses personales, comportamiento o localización y desplazamientos. La definición usada por el WP29 ha sido la que el legislador europeo ha reflejado de forma literal en el artículo 4.4) del RGPD y será con la que trabajemos en adelante en este análisis.

Señalar que el *profiling* puede entrar o no en el ámbito de protección material del RGPD dependiendo de si los datos tratados o resultantes pueden ser categorizados como datos personales, es decir, toda información sobre una persona física identificada o identificable (art. 4.1) del RGPD).

Obviamente el fin económico-comercial del *profiling* hace que cuanto más identificada quede una persona física, mayor utilidad posea el análisis realizado: piénsese en un

⁷ WP29, *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation*, 2013 <http://www.medialaws.eu/wp-content/uploads/2013/05/20130513_advice-paper-on-profiling_en.pdf>

análisis de datos tendente a encontrar perfiles de individuos tendentes a pagar un mayor precio por un producto X, cuanto más se concrete la tendencia de pago de precios mayores (hasta el punto de poder afirmarse que un individuo concreto e identificado está dispuesto a pagar un determinado precio), mayor es el beneficio económico que puede proporcionar la información a la empresa, que diseñará políticas de precio orientadas hacia el perfil de dicho consumidor. Los datos más valiosos en materia de uso económico –pero también político, social o sanitario- obtenidos mediante técnicas de *profiling* poseerán tan alto grado de concreción que será imposible negar que sean datos personales.

II.2- TIPOS DE *PROFILING*

El *profiling* por sí mismo no es otra cosa que una técnica concreta de recolección y análisis de datos, los cuales pueden ser usados posteriormente con fines muy diversos, desde la elaboración de campañas de marketing a la evaluación de candidatos en procesos de selección o la detección precoz de potenciales riesgos en la salud de una persona. Atendiendo a dichos fines se pueden distinguir dos tipos principales de creación de perfiles⁸.

1. *Profiling* orientado a la evaluación, puntuación o calificación de individuos y de su conducta

La obtención de patrones de conducta generales⁹ permite analizar si existen –y en caso de existir, cuantificar- desviaciones o anomalías respecto de dichos patrones cuyo análisis puede ser de interés. Estas técnicas de minería de datos presentan una especial relevancia en temas económicos (por ejemplo, la obtención de patrones de comportamiento en materia de consumo de energía eléctrica doméstica), pero es en el campo militar y policial donde primero se desarrollaron programas: puede citarse como ejemplo el programa

⁸ La clasificación expuesta pone el foco en la repercusión relativa a la protección de datos de las técnicas de *profiling*, si bien si atendemos a todas las posibles aplicaciones del *profiling* o a las distintas técnicas empleadas por el mismo, una clasificación que pretendiese poseer carácter exhaustivo carecería de sentido.

⁹ La idea se basa en la existencia de «*predefined patterns of normal behaviour*» o traducido de forma literal, patrones predefinidos de comportamiento normal, término empleado por Fanny Coudert, profesora de la Universidad de Lovaina y miembro del *Research Unit KU Leuven Centre for IT & IP Law (CiTiP)* en su obra *When video cameras watch and screen: Privacy implications of pattern recognition technologies* (2010) para definir aquellas conductas tomadas referencialmente como normales por un sistema de prevención de riesgos basado en inteligencia artificial.

desarrollado en 2016 por IBM con el objetivo de distinguir verdaderos refugiados solicitantes de asilo de potenciales terroristas ocultos tras falsas identidades¹⁰.

La evaluación del individuo, de sus gustos, sus comportamientos y sus hábitos ha supuesto la aparición de grandes oportunidades empresariales relativas a la posibilidad de personalizar la experiencia del usuario de forma que se adapte a sus condiciones específicas: desde fijar precios personalizados en base a la elasticidad de su demanda individual a ofrecer sugerencias de compra basadas en transacciones anteriores.

2. *Profiling* orientado a la inferencia o predicción de información

Uno de los aspectos más relevantes de las técnicas de minería de datos es precisamente el relativo a la obtención de nueva –y normalmente muy sensible- información personal a partir de datos que no siempre poseen el carácter en origen de personales.

Piénsese a modo de ejemplo de las técnicas utilizadas por la cadena estadounidense de supermercados Target¹¹. La empresa descubrió utilizando técnicas de minería de datos que las consumidoras embarazadas consumían durante los últimos dos tercios de su embarazo, entre otros, un mayor número de productos cosméticos carentes de aromas artificiales o suplementos nutritivos con altas dosis de calcio y magnesio; empleando esta información, procedió a realizar una campaña publicitaria orientada hacia mujeres en estadios avanzados de embarazo, potenciales consumidores de productos de demanda cruzada como ropa de bebé. En este caso concreto, la aplicación de técnicas de *profiling* permitió al supermercado identificar a sus clientas como parte de un colectivo concreto, permitiéndole inferir un dato tan sensible como es el de encontrarse en estados avanzados del embarazo.

Compruébese en este caso como, de no existir una regulación propia relativa a las técnicas de *profiling*, el usuario habría otorgado su consentimiento para que la empresa recabase una serie de datos cuyo carácter podría no ser estrictamente personal (como puede ser el número de veces al mes que ha consumido un determinado producto), pero que mediante el tratamiento efectuado ha dado lugar a una información personal especialmente

¹⁰ TUCKER, P., *Refugee or Terrorist? OBM Thinks Is Software Has the Answer*. <<http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-hasanswer/125484/>> Consultado el 05 de abril de 2018.

¹¹ GIL, E. “Big data, privacidad y protección de datos”, Imprenta Nacional de la AEPD, 2016, pero también HILL, K. *How target figured out a teen girl was pregnant before her father did*, Revista Forbes <<https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#214bee5f6668>>, fecha de consulta 30 de marzo de 2018.

privada¹² que en ningún momento el sujeto habría transmitido a su actual tenedor. De esta forma, el supermercado habría “sorteado” los requisitos propios de la obtención del consentimiento¹³ que normas anteriores al RGPD exigían a las entidades que recopilaban dicha información.

II.3- RIESGOS DEL *PROFILING*

En la era tecnológica en la que nos encontramos, todo usuario pondera por un lado la pérdida de privacidad y el intrusismo solicitado (en el mejor de los casos) por las empresas y agentes económico-sociales y, por otro, los beneficios que le reporta acceder a compartir sus datos personales.

El resultado es siempre el mismo. El aislamiento social que puede producir no aceptar los términos y condiciones de redes sociales como Facebook o la imposibilidad de uso de aplicaciones móviles, servicios de compra o incluso de acceso a ciertas webs acaba provocando que los usuarios acepten prestar su consentimiento para casi cualquier tipo de uso solicitado. Parte de la doctrina habla del “mito del consentimiento”¹⁴, o de la errónea concepción del mismo que el legislador estatal y europeo ha adoptado, ya que el titular de dichos derechos pocas veces se encuentra totalmente informado, bien por temas de tiempo bien por temas de capacidad, siendo por tanto el consentimiento otorgado por éste una mera adhesión a unas condiciones cuyo alcance no se llega a comprender, y que en caso de ser rechazadas suponen el aislamiento del sujeto.

El *profiling* reporta unos beneficios para el sujeto innegables, desde la sugerencia de obras literarias en librerías web como Amazon libros a ofertas hoteleras con las características deseadas por un potencial comprador, no obstante, todo ello indudablemente a cambio de un precio. El uso ilegítimo de datos personales ha cobrado fuerza como preocupación entre españoles y europeos tal y como han mostrado los eurobarómetros elaborados por Kantar Media para la UE en los últimos años: para el año 2016, 8 de cada 10 ciudadanos

¹² En el RGPD y referido al caso concreto mencionado de los supermercados Target se puede asimilar este tipo de información a los datos englobados en el artículo 9 dentro de las categorías especiales, donde se menciona de forma explícita datos biométricos y relativos a la salud del individuo, endureciendo los requisitos necesarios para su tratamiento frente a cualquier otro tipo de datos.

¹³ BRANDÃO, E. Y OTROS, *Predicting the risk associated to pregnancy using data mining*, ALGORITMI Research Centre, Universidade do Minho, Guimarães, Portugal, 2015.

¹⁴ MUÑOZ SORO, J.F; LALANA, D. “El mito del consentimiento y el fracaso del modelo individualista de protección de datos”, Cizur Menor (Navarra): Aranzadi, 2013.

Europeos encuestados¹⁵ (82%) consideraban importante que el uso de técnicas de seguimiento de su actividad online (como el uso de *cookies*)¹⁶ se base exclusivamente en su consentimiento, si bien únicamente un 60% actuaba en consecuencia realizando modificaciones en su configuración de privacidad.

Y es que los temores anteriores no son en ningún caso infundados. En marzo de 2018 saltaba a la luz el llamado escándalo *Cambridge Analytica*, un caso de recolección masiva de datos a través de perfiles de la red social Facebook, en la cual los datos personales de más de 50 millones de usuarios (de los cuales sólo una pequeña parte había prestado su consentimiento) fueron utilizados por terceros en la elaboración de perfiles socio-político-demográficos que podrían haber jugado un papel crucial en la campaña electoral del actual presidente norteamericano de acuerdo con las hipótesis de la FTC o la campaña por el Brexit de acuerdo con las de la Comisión Electoral de Reino Unido¹⁷.

Todos estos escándalos ponen de manifiesto una preocupante realidad: el volcado masivo de información personal en la web está provocando la aparición de técnicas de mercadotecnia agresiva cuyo altísimo grado de precisión pone en riesgo ya no sólo los derechos del consumidor, sino incluso las libertades propias de los estados democráticos de derecho.

¹⁵ KANTAR MEDIA, *Flash Eurobarometer 443: e-Privacy*, EU Open Data Portal <https://data.europa.eu/euodp/data/dataset/S2124_443_ENG>, consultado el 23 de abril de 2018.

¹⁶ Si bien se observa una generalizada preocupación por el uso de este tipo de técnicas, aproximadamente un 46% de los encuestados en el *Flash Eurobarometer 443* declaraban considerar aceptable que se rastreara su información personal cuando ello les proporcionase acceso ilimitado a determinados sitios web, en un claro ejemplo de cómo una gran parte de los ciudadanos se encuentra dispuesta a sacrificar parte de su privacidad a cambio de ciertos beneficios que no se encuentran íntimamente relacionados con la información que se está ofreciendo a las empresas.

Al respecto puede resultar interesante la opinión de MUÑOZ SORO, J.F., y OLIVER-LALANA, A.D. en su obra “Derecho y cultura de protección de datos, un estudio de la privacidad en Aragón” (2012), donde queda patente que existe una muy distinta valoración en la sociedad actual de los bienes en cuestión cuando hablamos del uso de las TIC. Los autores señalaban que únicamente un 47% de la población analizada en su obra opina que el auge de las nuevas tecnologías supone una amenaza para la privacidad.

¹⁷ *Pressure grows on PM over Brexit Cambridge Analytica scandal*, periódico The Guardian, <<https://www.theguardian.com/politics/2018/mar/26/pressure-grows-on-pm-over-brexit-cambridge-analytica-scandal-theresa-may>>, así como *Facebook may have violated FTC privacy deal, say former federal officials, triggering risk of massive fines*, periódico The Washington Post <<https://www.washingtonpost.com/news/the-switch/wp/2018/03/18/facebook-may-have-violated-ftc-privacy-deal-say-former-federal-officials-triggering-risk-of-massive-fines/>>, consultados ambos el 29 de marzo de 2018.

III. LA REGULACIÓN EN EL RGPD

Si bien es el Reglamento General de Protección de Datos la norma que mayor repercusión (y controversia) ha causado en lo referente a las técnicas de *profiling*, sería incorrecto afirmar que no existe precedente en la Directiva 95/46/EC de protección de datos.

« (41): Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al **tratamiento automatizado de los datos** que la conciernan, al menos en el caso de las **decisiones automatizadas** a que se refiere el apartado 1 del artículo 15; [...] »

De la lectura del extracto anterior —considerando nº 41 de la Directiva— podemos observar que desde los primeros antecedentes legales de protección de datos, al legislador europeo le han preocupado especialmente los riesgos vinculados con técnicas de perfilado de datos en aquello a lo que la toma de decisiones automatizadas se refiere.

Y es que en la directiva no encontramos mención alguna al *profiling* o perfilado de datos, si bien el mismo era antecedente de forma habitual en el tipo de conductas que precisamente el artículo 15.1 del texto trataba de regular.

«Artículo 15

Decisiones individuales automatizadas

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. [...] »

El *profiling* en sí mismo quedaba fuera de la regulación y únicamente se incidía en los posibles efectos negativos que el mismo podía producir, teniendo en mente el legislador situaciones como las descritas en apartados anteriores, en las que mediante el análisis automatizado de datos se trataba de otorgar una calificación crediticia a un individuo, por ejemplo.

Desde esta primigenia redacción, la evolución de las TIC y de la forma de consumo basada en internet ha supuesto un nuevo horizonte con importantes y hasta ahora desconocidos riesgos que fueron tenidos en cuenta por el Parlamento Europeo a la hora de elaborar el texto que ha entrado en vigor el 1 de mayo de 2018.

Ya en mayo de 2013, el WP29 en su documento guía en materia de creación de perfiles¹⁸ advertía de cómo el *profiling*, pese a que en origen había sido considerado un proceso neutro, podía tener un significativo impacto en los derechos básicos del individuo relativos a la protección de datos. En opinión del grupo de trabajo, era necesario que el nuevo texto incorporase una definición de *profiling* o creación de perfiles y una regulación propia sobre el mismo.

Las perspectivas y preocupaciones expuestas contrastan en cierta manera con la cristalización final en el texto definitivo del RGPD.

El legislador, si bien define el *profiling* en el artículo 4.4 RGPD y traslada las conclusiones anteriores a los considerandos (especialmente 70, 71 y 72), relega en los principios generales del texto la protección que parecía proponer el WP29 en sus propuestas consultivas, reproduciendo en cierta manera lo expuesto por la Directiva 95/46/EC en su artículo 15.1 al vincular el *profiling* a la toma de decisiones automatizadas.

« (60): [...]. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. [...] »

« (63): [...]. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. [...] »

« (70): Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse

¹⁸WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017, <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826>

explícitamente al interesado y presentarse claramente y al margen de cualquier otra información. »

« (72): La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto. »

De esta forma, será mediante la aplicación de los artículos 5 a 7 (principios generales) cuando podamos hablar de protección jurídica frente a abusos en el uso de técnicas de *profiling* contrarias al espíritu de la norma, quedando la provisión del artículo 22 RGPD circunscrita a una serie de supuestos específicos, es decir, cuando el uso de dichas técnicas resulte en la toma de decisiones automatizadas.

III.1. PRINCIPIOS DE PROTECCIÓN CON INCIDENCIA EN LA CREACIÓN DE PERFILES

III.1.1- LICITUD, LEALTAD Y TRANSPARENCIA

«Artículo 5- Principios relativos al tratamiento

1. Los datos personales serán:

a) tratados de manera **lícita, leal y transparente** en relación con el interesado («licitud, lealtad y transparencia»); [...] »

La **licitud** de la que habla el artículo 5.1 a) RGPD es concretada en el artículo siguiente, estableciéndose que el tratamiento de datos personales será lícito si se cumple alguna de las seis condiciones en dicho artículo descritas:

A. el interesado otorgó su consentimiento

B. el tratamiento es necesario para

1. La ejecución de un contrato/ medidas precontractuales en el que el interesado es parte

2. El cumplimiento de una obligación legal aplicable al responsable del tratamiento;
3. Proteger intereses vitales del interesado o de otra persona física;
4. El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
5. La satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero

Establecido el consentimiento como piedra angular del sistema, especialmente relevante es en materia de *profiling* la condición relativa a la ejecución de un contrato, puesto que en multitud de ocasiones encontramos este tipo de requisitos vinculados al uso de aplicaciones móviles. Sirva como ejemplo Home Connect¹⁹ del grupo BSH, la cual requiere de la recopilación de datos personales relativos al uso de electrodomésticos, consumo energético o incluso hábitos alimenticios para la ejecución del contrato de control remoto y gestión digital de los electrodomésticos marca Bosch.

La vinculación de gran cantidad de *apps* a esta condición del artículo 6.1.b) RGPD está ocasionando que comiencen a observarse casos en los que prestaciones accesorias de un contrato de compraventa (como puede ser el de un frigorífico de la marca anterior) abran la puerta al uso de datos personales y elaboración de perfiles sin necesidad de obtener un consentimiento explícito y específico para dicho tratamiento. El cliente accede en lo relativo a la ejecución del contrato y ello supone base legal suficiente como para considerar lícito el tratamiento de datos personales.

Mención especial merece la mención al **interés legítimo** del artículo 6 RGPD como supuesto de licitud del tratamiento pues, en la mayoría de los casos, ha sido y será la vía utilizada por los entes del sector privado para justificar el tratamiento de datos personales de los ciudadanos europeos.

La regulación del actual artículo 6 RGPD se asemeja a la contenida en el artículo 7 de la Directiva 95/46/EC, sobre la cual el WP29 dictaminó una serie de matizaciones²⁰ que son extrapolables hasta cierto punto a la noción de interés legítimo del texto legal aquí

¹⁹ BSH, *Data Privacy Policy for the Home Connect website*, <<http://www.home-connect.com/global/meta-pages/data-protection>> consultado el 3 de abril de 2018.

²⁰ WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 2014 <<http://www.dataprotection.ro/servlet/ViewDocument?id=1086>>

estudiado. En resumen, el Grupo de Trabajo habla de la necesidad de elaborar una ponderación entre sus intereses legítimos (los del responsable del tratamiento) y los derechos fundamentales y libertades del afectado, distanciando la responsabilidad de la prueba de esta ponderación de la responsabilidad del ciudadano y depositándola en manos del responsable del tratamiento.

A la hora de concretar esta ponderación, tanto el ICO como la *Data Protection Network*²¹ coinciden en la necesidad de realizar un triple juicio, examinando en primer lugar el fin del tratamiento de datos personales, la necesidad del mismo (es decir, si podría lograrse los objetivos perseguidos utilizando una técnica menos lesiva para los derechos de los afectados) y finalmente la proporcionalidad en sentido estricto (¿son los intereses legítimos del individuo de entidad superior a los de la empresa?). A modo ilustrativo, el WP29 especifica que el análisis anterior debe tener en cuenta tanto el nivel de detalle del análisis realizado como el impacto que el mismo puede suponer en la esfera jurídica del individuo.

Si bien hay una gran área gris en lo que a intereses legítimos se refiere, los dos organismos anteriores coinciden en que el interés legítimo del responsable del tratamiento suele estar justificado en casos como el de elaboración de *diu diligence*, procesado de datos relativos a empleados con el propósito de mejorar sus condiciones laborales o prevención del fraude (estos dos últimos ejemplos recogidos de forma expresa en el considerando nº 47 del RGPD).

Señalar finalmente que la nueva redacción del RGPD en materia de intereses legítimos ha abierto la puerta a considerar intereses de terceros con los que no exista una relación contractual que suponga el tráfico de datos personales (como puede ser la sociedad en su conjunto), permitiendo una justificación del interés legítimo en unos términos significativamente más amplios que los de la Directiva 95/46/EC.

La **lealtad** es un concepto jurídico altamente indeterminado y especialmente en el marco de la recolección y tratamiento de protección de datos, y suele relacionarse con las

²¹ La Data Protection Network es una red de expertos en materia de derecho digital con sede en Londres, Reino Unido. Sus documentos suelen orientarse hacia materias de *compliance* de entes empresariales y en su documento *Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation*, 2017 <<https://smartmessenger.co.uk/media/104621/dpn-guidance-a4-publication.pdf>>, analizan en profundidad aspectos relativos al interés legítimo que pueden ser de utilidad en este punto.

expectativas ²²del usuario especialmente en los casos en los que el procesamiento encuentra base legal en su consentimiento. De esta forma, las previsiones razonables del usuario en base a la información que se le ha ofrecido sobre procedimientos y usos de los datos recolectados deben ser tenidas en cuenta a la luz del artículo 5.1 a) RGPD. Señalar que la lealtad se encuentra estrechamente vinculada a la protección de datos, tal y como puede observarse en la redacción de la propia Carta de los derechos fundamentales de la Unión Europea.

«Artículo 8- Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan
2. Estos datos se tratarán de **modo leal**, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. [...] »

Finalmente, la **transparencia** se articula como el tercero de los pilares del artículo 5 RGPD e implica el suministro de información concisa, transparente, inteligible y fácilmente accesible para el propio usuario²³. La regulación del artículo 5.1 a) RGPD encuentra su desarrollo con los artículos 12, 13 y 14 RGPD, que serán mencionados posteriormente al hablar de los derechos del interesado.

²² ICO, *Big data, artificial intelligence, machine learning and data protection*, 2017, <<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>> consultado el 11 de abril de 2018.

²³ El propio WP29 deja constancia en “*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*” acerca de la toma de indicaciones señaladas por la *Office of the Australian Information Commissioner* en su publicación “*Consultation draft: Guide to big data and the Australian Privacy Principles*” de mayo de 2016. El legislador europeo ha tomado ejemplo del australiano en sede de transparencia en tanto en cuando han seguido las recomendaciones relativas señaladas por el WP29, acogiendo como conclusión propia que la misma tecnología que presenta nuevos riesgos para el usuario le debe permitir también hacer uso de las nuevas oportunidades y medios de acceso a cuestiones y avisos relativos a su privacidad.

III.1.2- FINALIDAD DE RECOGIDA Y TRATAMIENTO

«Artículo 5

1.Los datos personales serán: [...]

b) recogidos con **finés determinados, explícitos y legítimos**, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); [...] »

La redacción expuesta ha sido ampliamente criticada por autores como Hildebrandt²⁴ (2013) o Zarsky²⁵ (2017) a la luz de la propia esencia del *Big Data*: el descubrimiento de correlaciones imposible de ser apreciadas anteriormente mediante la exploración de archivos masivos de datos.

Señalan estos autores que en muchas ocasiones, el valor añadido creado no es fruto de una búsqueda concreta y específica, de un análisis con un propósito claro y definido, sino más bien de un hallazgo que difícilmente podía haber sido anticipado. Las características de este tipo de técnicas dificultan el encaje con las previsiones del artículo 5.1. b), salvo que se definan propósitos escasamente definidos y suficientemente amplios de uso y tratamiento de los datos personales, lo cual es altamente probable que pueda ser calificado como fraude de ley. Señalar que en prácticamente ningún caso podría ampararse un tratamiento con fines empresariales posteriores en la excepción contenida en el propio artículo 5.1.b) (tratamiento ulterior con fines estadísticos) a la luz del considerando nº 162 pues el mismo establece que el resultado del análisis estadístico en ningún caso puede desembocar en la obtención de datos personales y es precisamente en este marco en el que nos encontramos.

²⁴ HILDEBRANDT, M. *Slaves to Big Data. Or Are We?*, Revista de internet, derecho y política, Universitat Oberta de Catalunya, vol. 17, Octubre de 2013, ISSN 1699-815, pag. 27. <<http://www.raco.cat/index.php/IDP/article/viewFile/303366/393038>>, consultado el 22 de abril de 2018.

²⁵ ZARSKY, T.Z., “*Incompatible: The GDPR in the Age of Big Data*”, Seton Hall Law Review, Vol. 47, No. 4(2), 2017.

El propio WP29, consciente de las limitaciones que puede suponer la redacción tanto de la Directiva como del actual Reglamento, emitió una opinión en 2013²⁶ en la que clarificaba que el posterior tratamiento de datos recolectados en un primer momento respondiendo a un propósito distinto al original no se encuentra per se prohibido, sino que la regulación presenta la suficiente flexibilidad como para que deba estudiarse caso por caso, siendo en todo caso necesario el cumplimiento de los principios generales de la norma.

Si bien el propósito del WP29 era intentar presentar que la regulación no lleva apareja la rigidez que suele achacársele, el propio Foro Económico Mundial²⁷ ha expresado su preocupación en tanto en cuando las posibilidades que el tratamiento de datos ofrecen al desarrollo de la empresa se ven muchas veces limitadas por el temor a estar incumpliendo una normativa que en raras ocasiones suele destacar por su claridad y concreción.

Zarsky, en defensa de una postura alejada de posiciones moderadas, rechaza culpar al legislador de 2016 de esta supuesta incompatibilidad con los principios del *Big Data* pues no sólo encontramos limitaciones relativas al fin del tratamiento y recogida de datos en los trabajos preliminares del WP29, sino también en la Directiva 95/46/EC así como en la Carta europea de Derechos Humanos en su artículo 8.2. Cualquier intento de apartarse de esta piedra angular del sistema de protección de datos europeo habría resultado en una normativa susceptible de ser llevada ante el TJUE.

A la hora de la realidad, la propuesta del ICO²⁸ (Information Commissioner's Office de Reino Unido) parece la más acorde con el espíritu de la norma, especialmente teniendo en cuenta el considerando nº 50. La posibilidad de tratamiento sucesivo dependerá de la compatibilidad de la finalidad del tratamiento posterior con el original, siendo necesario el vínculo entre ambos, las expectativas razonables del usuario, las consecuencias de este segundo tratamiento y la existencia de mecanismos de protección y salvaguarda. Las condiciones del mismo deberán ser analizadas a la luz de los principios de protección que se están tratando en esta sección, especialmente lo relativo al uso leal.

²⁶ WP29. *Opinion 03/2013 on purpose limitation*, 2013. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, consultado el 24 de abril de 2018.

²⁷ Foro Económico Mundial, *Unlocking the value of personal data: from collection to usage*, Industry Agenda, p.4 <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf>, consultado el 24 de abril de 2018.

²⁸ ICO, *Big data, artificial intelligence, machine learning and... cit.* p.18

III.1.3.- MINIMIZACIÓN DE DATOS O *DATA MINIMISATION*

«Artículo 5

1.Los datos personales serán: [...]

c) **adecuados, pertinentes y limitados** a lo necesario en relación con los fines para los que son tratados («minimización de datos»); [...] »

El artículo 5.1.c) RGPD posee una doble dimensión: por un lado, impone restricciones a la amplitud y categoría de datos recolectados y, por otro lado, limita de igual forma la duración de almacenamiento de dicha información por parte del responsable del tratamiento, quien no puede retenerla a perpetuidad. Teóricamente presenta un principio de protección bastante obvio: la recolección de una menor cantidad de datos personales necesariamente ha de traducirse en una mayor dificultad de puesta en riesgo de la privacidad del usuario, no obstante, el eterno equilibrio entre riesgos y oportunidades pone en entredicho este principio.

La minimización de datos se basa en lo que podría describirse como una “limpieza” de información personal mediante la cual el tratamiento al que se someten dichos datos sólo utiliza los que resultan relevantes para el fin del estudio, desechando los que no guardan relación con el mismo y que el legislador parece considerar –erróneamente- irrelevantes o triviales.

La redacción de este apartado, así como del resto del RGPD en el que se menciona este concepto de minimización de datos, adolece de los mismos defectos que se señalaba en el apartado anterior: la minimización de datos puede llegar a ser contraria al propósito de uso de este tipo de técnicas en materia de creación de perfiles. Como aducíamos anteriormente, la recolección de datos masivos no responde a un “por si acaso” tal y como señala de forma bastante desafortunada SAINZ, C.A. o DEL ÁLAMO, J.M. en su “Código de buenas prácticas en protección de datos para proyectos *Big Data*”, (2016)²⁹, sino que responde a las necesidades intrínsecas del análisis, al desconocimiento e imposibilidad de previsión de los posibles patrones que pudieran hallarse.

²⁹ SAINZ, C.A.; ACED, E.; DEL ÁLAMO, J.M. y otros, *Código de buenas prácticas en protección de datos para proyectos Big Data*, 2016, Prensas Oficiales de la AEPD, p. 17

Cierto es que un argumento como el anterior llevado a su extremo nos llevaría a concluir que la cantidad de datos a recopilar y analizar es infinita (lo cual sí posee un cierto sentido matemático y estadístico³⁰), algo que equivaldría al conocimiento total y absoluto del individuo pues todas las facetas del mismo habrían sido analizadas.

La raíz del problema se encuentra en la abstracción del principio aquí tratado y en la errónea concepción de que las técnicas de creación de perfiles basadas en procesos de *data mining* requieren una serie de recursos concretos para producir el resultado esperado y que todo recurso apartado de lo lógicamente considerado como necesario es trivial e innecesario.

III.1.4- EXACTITUD

«Artículo 5

1. Los datos personales serán: [...]

d) **exactos** y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); [...]

En aras de cumplir los principios de lealtad y transparencia mencionados en apartados anteriores, el tratamiento de datos deberá velar por la exactitud de los mismos pues en caso contrario, las técnicas de creación de perfiles darán como resultado información incorrecta sobre el individuo, la cual al ser tomada como base para posteriores decisiones poseerá un impacto directo sobre el mismo.

Si bien el legislador ha tratado de limitar o al menos contener la intrusión de los recolectores de datos en la esfera privada del individuo, en este punto se adopta un planteamiento distinto orientado a evitar los importantes perjuicios que puede suponer el

³⁰ ZHANG, D.S.G.; KEQUIN LI, M. *Key Technologies for Big Data Stream Computing*, Tsinghua University of Beijing, 2017.

profiling viciado por aspectos tan diversos como la antigüedad de los datos (y por tanto su falta de actualización) o el error de correspondencia con un individuo concreto.

En última instancia, controlar la exactitud de la información recogida supone la aplicación de métodos técnicos, organizativos, matemáticos y/o estadísticos que reduzcan al máximo el riesgo de error, término expresamente utilizado en el considerando 71 y que parte de la adecuada noción de que la exactitud total es una meta poco realista con el carácter masivo de los datos aquí tratados.

El WP29³¹ ha señalado la especial conexión entre el principio contenido en el artículo 5.1.d) RGPD con los deberes de transparencia e información al afectado de forma que la puesta en conocimiento de los datos personales tratados pueda servir para que el afectado compruebe si los mismos son correctos.

Esta propuesta, si bien acorde con el espíritu de la norma al convertir al individuo de a pie en el centro del control, resulta poco realista cuando es considerada en nuestro contexto actual puesto que escaparía de las posibilidades del usuario el comprobar de forma sistemática que todos los datos tratados son exactos, por no decir que parece derivar el control de exactitud hacia el mismo, lo cual en ningún caso puede ser considerado una práctica acorde a derecho a la luz del RGPD (recordemos que el artículo 5.2 establece la responsabilidad proactiva del responsable del tratamiento).

Finalmente, un aspecto interesante es el tratado por el ICO en su documento *Overview of the General Data Protection Regulation*³² acerca de los errores: ¿puede mantenerse en la lista de bases de datos una recopilación de errores, bien del individuo bien del responsable del tratamiento a la luz del artículo 5.1.d)? Un ejemplo de los mismos podrían ser formularios mal introducidos y posteriormente corregidos, compras canceladas, previsiones incumplidas, etc. Parece ser opinión del organismo que este tipo de información puede ser almacenada sin problema siempre y cuando se base en situaciones históricas, efectivamente producidas.

³¹ WP29, *Guidelines on Automated individual decision-making and Profiling... cit.* p. 14

³² ICO, *Overview of the General Data Protection Regulation*, 2017, <<https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf>>, consultado el 25 de abril de 2018.

III.1.5.- SEGURIDAD

«Artículo 5

1. Los datos personales serán: [...]

f) tratados de tal manera que se garantice una **seguridad adecuada** de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). [...] »

La seguridad ha sido uno de los principios fundamentales de la legislación europea en materia de protección de datos desde sus inicios. El RGPD incide de manera profusa en dicha regulación y desarrolla elementos como el concepto de “seguridad desde el diseño” con los cuales hace frente a los riesgos omnipresentes que el tratamiento de datos supone ante posibles brechas en la seguridad que comprometan la privacidad del individuo, una preocupación que a fecha de este trabajo cobra mayor importancia que nunca pues el pasado año 2017 fue categorizado como el año en el que mayor número de ciberataques fueron realizados contra empresas, en una cifra que dobló la cifra de 2016³³.

Al no existir un impacto directo en lo relativo al *profiling* y ser por sí mismo merecedor de su propio trabajo, no realizaremos un comentario más extenso en materia de seguridad más allá de las previsiones comentadas en capítulos conexos.

³³ 2017 was 'worst year ever' in data breaches and cyberattacks, thanks to ransomware, noticiario digital Techrepublic, <<https://www.techrepublic.com/article/2017-was-worst-year-ever-in-data-breaches-and-cyberattacks-thanks-to-ransomware/>>, consultado el 25 de abril de 2018.

III.2- PREVISIONES ESPECÍFICAS: EL ARTÍCULO 22 RGPD

III.2.1- ALCANCE

«Artículo 22- **Decisiones individuales automatizadas**, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. [...] »

El análisis del artículo 22 RGPD debe comenzarse planteando una cuestión de suma importancia ¿es lo mismo *profiling* que toma de decisiones individuales automatizadas? El propio artículo 22 en su título parece indicar lo mismo al hablar de «decisiones individuales automatizadas, incluida la elaboración de perfiles». Sin embargo, debemos afirmar que no, ambos conceptos son sustancialmente distintos.

Ya en la definición de elaboración de perfiles contenida en el artículo 4.4) sorprende a la vista del artículo 22 RGPD la falta de toda alusión a la toma de decisiones, lo cual lleva a la conclusión que el concepto de perfilado de datos juega un papel relevante en el marco del artículo 22 sólo en medida en que se trata de un tratamiento automatizado de datos³⁴, lo cual viene avalado por lo descrito en el considerando 71, el cual incluye al *profiling* en esta última categoría: «[...] Este tipo de tratamiento incluye la elaboración de perfiles [...]».

De esta forma, el *profiling* constituiría la base sobre la cual se llegarían a tomar las decisiones individuales automatizadas tratadas por dicho artículo, quedando fuera del ámbito material del mismo el *profiling per se*. La relevancia de esta distinción es manifiesta: el *profiling* queda por tanto permitido de acuerdo con el RGPD siempre y cuando cumpla los requisitos propios para el tratamiento de datos personales estudiados en apartados anteriores.

³⁴ LEE, P. *Let's sort out this profiling and consent debate once and for all*, 2018

Esta concepción, menos restrictiva que la prevista para el supuesto del artículo 22, contrasta con las previsiones sobre *profiling* expresadas por el legislador en el considerando 71:

«(71): [...] Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas. »

Y es que en los borradores del RGPD, la Comisión Europea³⁵ mantenía una regulación del *profiling* muy similar a la definitiva, en la que el mismo sólo era restringido en tanto en cuando fuera utilizado como base para la toma de decisiones individuales automatizadas. Sin embargo, esta no era la postura del Parlamento Europeo, que abogaba por introducir una prohibición genérica del *profiling* de acuerdo a la cual el mismo sólo se encontraría permitido si se cumplía con lo contenido en el articulado.

Las enmiendas 38, 39, 136 y 158³⁶ entre otras del documento mencionado anteriormente ejemplifican cómo el Parlamento Europeo realizó una clara distinción entre «*profiling*» y «*medidas basadas en el profiling*», justificando la inclusión del *profiling per se* en la prohibición general de tratamiento de datos personales en la realidad fáctica: las empresas creaban perfiles de consumidores sin contar con su conocimiento, menos con su consentimiento.

«Amendment 158- Justification

[...] Including the requirement that the data subject must consent to the profiling prevents what often happens in practice, namely that profiles are created without the data subject's knowledge. [...] »

De esta forma, si bien prevaleció el carácter más permisivo de la propuesta de la Comisión, la norma arrastra la visión del Parlamento Europeo, la cual es todavía posible de ver en los considerandos del texto definitivo, pero no en la regulación cristalizada en el actual artículo 22 RGPD.

³⁵ Comisión Europea, *DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7 0025/2012 – 2012/0011(COD))*, 16 de enero de 2013.

³⁶ En el Anexo I pueden observarse las diferencias entre las distintas redacciones utilizadas en los borradores del RGPD.

III.2.2- CONTENIDO

El **tratamiento automatizado** es el primero de los elementos del artículo analizado e implica la falta de presencia o intervención humana en la toma de decisiones, es decir, la toma de las mismas en base a un juicio realizado computacionalmente de acuerdo con las especificaciones del programa subyacente.

La intervención humana, elemento diferenciador en este artículo y cuya ausencia es necesaria para la aplicación del mismo, ha sido descrita en los trabajos del WP29 como “no simbólica”³⁷, de manera que el responsable del tratamiento no pueda evitar que le sean aplicables las previsiones legales del artículo 22 RGPD introduciendo previsiones de intervención humana carentes de aporte al proceso de toma de decisiones.

La influencia del ser humano por tanto debe ser manifiesta, ya que en caso contrario seguiríamos operando con la presunción de que no ha intervenido en el proceso, así como proceder de un individuo con la competencia y autoridad propias de la toma de decisiones referida.

Recurriendo a la analogía tan a menudo empleada por el legislador europeo, en casos de concesión de créditos en los que se utilizan técnicas de *profiling*, la decisión de concesión o no del mismo no se verá afectada por las restricciones del artículo 22 cuando el empleado bancario encargado de la misma sea quien finalmente juzgue si se concede o no dicho crédito. Ello no implica que su juicio pueda basarse en la conclusión alcanzada por el software de calificación crediticia, si bien debe tenerse en cuenta que si es el único factor considerado, en opinión del WP29 deberán respetarse los extremos fijados en el artículo aquí estudiado.

El segundo de los requisitos que establece el artículo 22 es el relativo al efecto de dichas decisiones, el cual debe ser **jurídico o le afecte significativamente de modo similar**. Pese a la relevancia de este extremo, el texto no define cuándo nos encontramos ante un efecto jurídico o similar, si bien busca proteger al individuo de decisiones que posean un impacto significativo en su esfera jurídica. El WP29 ha englobado en este supuesto decisiones relativas al acceso a ayudas sociales o la implantación de medidas de seguridad o prevención (en una clara referencia a las actividades policiales) a modo de ejemplo.

³⁷WP29, *Guidelines on Automated individual decision-making and Profiling ...cit* pág. 14

La inseguridad jurídica aumenta cuando nos centramos ya en los efectos similares a los jurídicos de los que nos habla el artículo. El considerando nº 71 retoma los ejemplos típicos de los que se ha hablado a lo largo de todo el trabajo (denegación automática de una solicitud de crédito en línea en la que no medie intervención humana alguna) pero no incluye mención alguna a qué debemos considerar como decisión susceptible de producir efectos significativos similares a los jurídicos.

En aras de la prevención de violaciones en los derechos de ciudadanos europeos, los responsables del tratamiento de datos personales deberán considerar como sujetas al artículo 22 prácticamente todas las decisiones que cumplan con el primero de los requisitos mencionados (carácter automatizado de la decisión) pues la amplitud del segundo de los requisitos determina la inoperancia del mismo. A modo de justificación, señalar que el WP29 considera que producen efectos similares a los jurídicos decisiones tan diversas como el alquiler de una bicicleta durante dos horas o la concesión de un préstamo respaldado por garantía hipotecaria, ambos con un grado de impacto en los intereses de los ciudadanos radicalmente distinto.

De la lectura de este apartado también se extrae una conclusión relevante: las prácticas de marketing y publicidad, basadas habitualmente en decisiones automatizadas radicadas en el análisis de datos personales del individuo, quedan fuera del ámbito material del artículo 22 RGPD en tanto en cuando no se traduzcan en decisiones que afecten a los derechos e intereses del usuario (como podría ser en el caso de que consista en la fijación de un precio personalizado). El WP29 así lo reconoce expresamente en el documento anteriormente mencionado, lo cual no implica que el RGPD contenga previsiones directamente aplicables en esta materia, pese a no ser objeto de este análisis.

Finalmente, señalar que en ningún caso se condiciona la aplicación del artículo a la condición de que los efectos producidos sobre el individuo sean negativos o perjudiciales para el mismo, por lo que de la lectura del mismo se extrapola que en una situación en la que el sujeto se vea beneficiado por la aplicación de estas técnicas, el responsable del tratamiento se ve sujeto a las mismas restricciones que en caso contrario³⁸.

³⁸ Al respecto se pueden observar propuestas como la de la *American Chamber of Commerce to the European Union*, que en su documento *Our position: Working Party 29 draft Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* <https://www.amchameu.eu/system/files/position_papers/amchameu_comments_wp29_draft_guidelines_on_profiling_final.pdf> sugiere que no se entiendan incluidos en el término “efectos significativos similares a los jurídicos” aquellos efectos que sean positivos o beneficiosos para los ciudadanos como puede ser el mejor acceso a ayudas públicas o una mejora de las condiciones de contratación. Se sugiere también que,

III.2.3.- CONTROVERSIA, PROHIBICIÓN O DERECHO A Oponerse

La redacción del artículo 22 RGPD ha suscitado dudas acerca de si nos encontramos ante una prohibición establecida al responsable del tratamiento de datos o un derecho del individuo a no ser sometido al tipo de decisiones aquí previstas.

La divergencia entre ambas posturas radica en efectos jurídicos muy diferentes: por un lado, la interpretación del mismo como una prohibición impediría de partida la toma de decisiones basadas únicamente en el tratamiento automatizado de datos, salvo que fueran de aplicación las excepciones del apartado 2º, mientras que la consideración del apartado 1º como un derecho del ciudadano implicaría la legalidad de la decisión así como la validez de la toma de la misma en tanto en cuando no fuera impugnada por el usuario, titular del derecho.

En este sentido, la segunda de las interpretaciones puede derivarse de la terminología utilizada por el legislador europeo ya que cuando se han recogido prohibiciones en el RGPD, se ha utilizado expresamente el término «prohibición», como es el caso del artículo 9.1:

«Artículo 9- Tratamiento de categorías especiales de datos personales

1. **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, [...] »

El actual artículo 22 presenta una clara similitud³⁹ en su redacción con el ya derogado artículo 15 de la Directiva de 1995, artículo que fue incorporado a los ordenamientos jurídicos nacionales habitualmente como un derecho del interesado, no como una prohibición. Sirva de ejemplo el artículo 15.1 de la *UK Data Protection Act* o el artículo 13.2 de nuestra LOPD.

«Artículo 13- Impugnación de las valoraciones

[...]

cuanto menos, aquellas decisiones automatizadas que resulten positivas se vean beneficiadas de una regulación más laxa que la actual.

³⁹ STARAN, E., HORDERN, V. *Automated Decision-Making Under the GDPR – A Right for Individuals or A Prohibition for Controllers?*, Hogan Lovells, 2017.

2. El afectado **podrá impugnar** los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. [...] »

Una interpretación en este sentido se encontraría alineada con los derechos de información recogidos en el artículo 13.2. f) o 14.2.g) RGPD, existentes precisamente para alertar al individuo de que se está tomando una decisión que produce efectos sobre su persona en los términos del artículo 22.1 RGPD. Como resulta obvio, esta es el análisis defendido por el sector privado puesto que la consideración del artículo 22 como una prohibición general constreñiría las posibilidades de actuación empresarial en el marco de la mecanización y automatización de los servicios prestados.

Sin embargo, esta no ha sido la interpretación que ha realizado el WP29. El Grupo de Trabajo dictaminó en su documento guía sobre el artículo 22 RGPD que nos encontramos ante una prohibición general y que, por tanto, sólo pueden realizarse las conductas descritas en dicho artículo cuando es de aplicación alguna de las tres excepciones del apartado segundo. Su opinión, en tanto órgano consultivo europeo, reviste de un importante peso y por tanto debemos entender que prevalece, si bien, como se ha comentado, no está exenta de polémica.

III.2.4.- EXCEPCIONES A LA “PROHIBICIÓN”

«Artículo 22- Decisiones individuales automatizadas, incluida la elaboración de perfiles [...]

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado. [...] »

Sobre la primera de las excepciones (**celebración o ejecución de un contrato**) realizaremos un par de comentarios y por el resto nos referiremos a lo expuesto en sede de licitud del tratamiento (apartado III.1.1). El WP29 ha relacionado la necesidad de la que nos habla la letra a) del artículo 22.2 con términos como los de eficiencia o justicia, de forma que pueda hablarse de la necesidad del tratamiento automatizado de datos como única base en la toma de decisiones automatizadas en casos en los que el uso de estas técnicas permita reducir tiempos en la prestación de servicios o suponga la satisfacción de las obligaciones contractuales con un mayor grado de precisión o calidad.

Pese a ello, el responsable del tratamiento debe efectuar un juicio de proporcionalidad en el que no sólo tenga en cuenta si la técnica de *profiling* utilizada es necesaria, sino que además constituye la opción menos intrusiva o perjudicial para los derechos del afectado de entre todas las posibles.

En lo relativo a la **autorización por la ley europea o de un estado miembro**, el WP29 apenas realiza mención alguna más allá de citar los supuestos recogidos en el considerando nº 71 del RGPD, es decir, casos de control fiscal y prevención del fraude o supuestos relativos a la seguridad o la fiabilidad de un servicio prestado. El análisis de esta excepción cobrará una mayor relevancia cuando comiencen a aflorar las regulaciones nacionales en desarrollo de las normas que recoge el marco general del RGPD.

Finalmente, la letra c) hace referencia al **consentimiento explícito del interesado**, un término que nos redirige al artículo 7 de la norma pero que exige además una manifestación clara y que se haga constar de forma expresa por parte del interesado, quedando atrás fórmulas relativas al consentimiento implícito que tanto florecieron desde la entrada en vigor de la Directiva de 1995 pero que han quedado ya desfasadas en lo que a protección de datos personales se refiere. De esta forma, bajo el RGPD todo consentimiento debe ser libre, específico, informado e inequívoco, pero además en el campo de las decisiones automatizadas se necesita que sea conste expresamente.

A modo ejemplificativo, la *Independent Comissioners Office* británica alude⁴⁰ a cesar en el uso de las llamadas cláusulas *pre-ticked*, casillas ya rellenadas en las que el usuario en lugar de otorgar su consentimiento mediante un acto o manifestación de voluntad positiva (como sería el ahora exigido), debía en todo caso realizar dicho acto para no otorgarlo, ya que si procedía sin modificar los términos indicaba que estaba conforme a las condiciones que le eran expuestas.

III.2.5- CONCLUSIONES RELATIVAS AL ARTÍCULO 22 RGPD

Podemos observar pues una diferencia fundamental entre las bases para entender lícito el tratamiento de datos personales en casos de mero *profiling*, y cuando dicho *profiling* sirve de base para la toma de decisiones automatizadas en los términos del artículo 22 RGPD.

Mientras que el *profiling* puede efectuarse en varios casos sin consentimiento del interesado (tal y como se ha descrito en el apartado III.1.1 de este trabajo), normalmente aludiendo a los intereses legítimos del responsable del tratamiento del artículo 6.1.f), la regulación relativa al *profiling* del artículo 22 es mucho más restrictiva, configurándose dicha norma como una prohibición general (aunque como se ha visto, discutida) que en el caso más común y frecuente va a requerir del consentimiento del ciudadano en unos términos más restrictivos respecto de la regulación europea anterior.

La divergencia en el tratamiento de estas dos facetas de una misma técnica hemos comprobado que generó una distinta concepción del tema en sede europea. Por un lado, la Comisión Europea abogó por una regulación muy similar a la definitiva, mientras que

⁴⁰ ICO, *Consultation: GDPR consent guidance*, 31 de marzo de 2017. <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>>, consultado el 28 de abril de 2018.

el Parlamento Europeo propuso restringir en mayor medida las técnicas de *profiling* fuera de lo que actualmente se recoge en el artículo 22.

No resulta descabellado pensar que, a la vista del gran número de escándalos relativos al uso de técnicas de *profiling* que salpican la actualidad, la postura oficial europea evolucione en la dirección planteada por el Parlamento y hacia una mayor restricción en el uso de técnicas de elaboración de perfiles.

III.3. DERECHOS DEL AFECTADO

III.3.1. DERECHO A SER INFORMADO

Tal y como se comentaba en la sección de principios de protección (III.1), la transparencia es uno de los pilares fundamentales del RGPD, estableciéndose nuevas obligaciones de información hacia el sujeto cuyos datos personales se están tratando.

El núcleo duro del derecho a ser informado se encuentra en los artículos 13 y 14 RGPD, dependiendo de si el sujeto prestó o no su consentimiento al tratamiento. Ambos artículos replican las previsiones relativas al *profiling*, indicando que el sujeto deberá ser notificado de «la existencia de decisiones automatizadas, incluida la elaboración de perfiles, [...], y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado».

Al igual que suele ocurrir en todas las previsiones estudiadas en este trabajo, el texto anterior suscita importantes dudas, en este caso acerca del alcance y profundidad de la información que debe ser suministrada. El legislador europeo especifica en el considerando nº 64 que dicha información debe permitir conocer al ciudadano europeo «la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento».

La primera cuestión que se nos plantea es si las obligaciones de información versan sobre todo tipo de técnicas de creación de perfiles o, si al igual que ocurría en el artículo 22, sólo son exigibles en la medida en la que las mismas sean utilizadas para la toma de decisiones automatizadas. La primera de las opciones (someter a todo tipo de *profiling* a estas exigencias legales) parece ser la defendida por el WP29⁴¹ y encuentra su fundamento

⁴¹ WP29, *Guidelines on Automated individual decision-making and Profiling...* cit. p. 14

en el tenor literal del considerando nº 60, cuando se habla de que «se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración».

No obstante, el WP29 no entra a valorar que los requisitos de información que se desprenden del considerando nº64 y del concepto de «lógica aplicada» (artículos 13.2.f) y 14.2.g) RGPD) no aparecen en el considerando nº 60 cuando se habla de las obligaciones de información del *profiling per se*. Por otro lado, el lenguaje utilizado es similar al del artículo 22 RGPD (e incluso los artículos 13 y 14 se refieren al mismo) donde se vinculan estas técnicas a la toma de decisiones automatizadas, lo cual reforzaría una postura tendente a entender que no se comprende el *profiling* no asociado a las mismas en estos artículos 13 y 14.

Pese a ello y a consecuencia de lo que el WP29 ha dictaminado, los responsables del tratamiento deberán considerar todo tipo de *profiling* como sujeto a esta obligación, lo cual es una conclusión acorde con los considerandos, pero que se aleja del tenor literal de los artículos 13 y 14 en una interpretación que a mi parecer resulta excesiva.

En términos generales, los autores⁴² de estudios en materia de *compliance* con el RGPD han entendido que del tenor literal del texto no se desprende la obligación de comunicar al sujeto afectado datos técnicos concretos relativos al algoritmo concreto que se encuentra detrás de la toma de decisiones automatizadas (algo que resultaría especialmente sensible en términos empresariales) sino más bien una explicación simplificada del tipo de información utilizada, la causa de su relevancia y las implicaciones de las conclusiones alcanzadas.

No obstante, parte de la literatura matemática y estadística ha señalado ya que este objetivo, si bien loable, es prácticamente inalcanzable con los últimos avances como los relativos al *deep learning*⁴³, donde la complejidad del modelo es tal que la comprensión por parte de un ciudadano medio se postula como un objetivo poco realista.

Las redes neuronales (modelo computacional basado en un gran conjunto de unidades neuronales artificiales, de forma aproximadamente análoga al comportamiento observado

⁴² SLAUGHTER AND MAY, *Tracking, watching, predicting... lawfully responsible profiling under the GDPR*, 2017, <<https://www.slaughterandmay.com/media/2536527/profiling-under-the-gdpr-september-2017.pdf>>, consultado el 12 de mayo de 2018.

⁴³ GOODMAN, B., FLAXMAN, S., *European Union regulations on algorithmic decision-making and a “right to explanation”*, Prensa de la Universidad de Oxford, 2016, p.7.

en los axones de las neuronas en los cerebros biológicos) presentan el caso extremo al ser descritas como una “caja negra” en la que ni siquiera sus programadores son plenamente conscientes de la secuencia lógica llevada a cabo en la obtención de un determinado resultado. Pese a que el WP29 ha manifestado que la complejidad del tratamiento no es excusa para dejar de proveer información al sujeto afectado, en temas redes neuronales una descripción somera de la lógica aplicada es, de acuerdo con varios autores, directamente imposible⁴⁴.

El ICO⁴⁵ se ha manifestado a favor de esta postura, añadiendo al planteamiento anterior que toda comunicación que sobrepase un nivel meramente divulgativo (y que por tanto entre en la lógica técnica o matemática tras el programa utilizado) incumpliría las exigencias de claridad y transparencia que predica el Reglamento, por no decir que podría llegar a suponer una violación de los derechos de propiedad intelectual que se encuentran tras el software⁴⁶.

A diferencia de los anteriores organismos, el WP29 en sede de recomendaciones sí contempla la posibilidad de comunicar a los afectados una compleja explicación matemática relativa al funcionamiento del algoritmo subyacente a la técnica aplicada cuando la misma vaya a ser estudiada por expertos. Al no profundizarse sobre el tema, cuesta imaginar supuestos en los que este tipo de información sea relevante⁴⁷ y su compatibilidad con las previsiones relativas al copyright señaladas anteriormente.

⁴⁴ Este tipo de opiniones son las presentes en obras como “Inteligencia Artificial y derecho de «explicación» en el Reglamento Europeo de Protección de Datos” de LÓPEZ CALVO, J. Diario La Ley, Nº 16, Sección Ciberderecho, Editorial Wolters Kluwer, 2018.

El propio autor señala que en la práctica el derecho de explicación podría ser imposible de cumplimentar, incluso para sistemas que parecen relativamente simples en la superficie, como las aplicaciones y los sitios web que utilizan aprendizaje profundo para publicar anuncios o recomendar canciones. Las computadoras que ejecutan esos servicios se han programado y lo han hecho de una manera que no podemos entender y menos explicar, ni siquiera por aquellos que crearon la aplicación.

⁴⁵ ICO, *Feedback request – profiling and automated decision making*, 2017, p.15 <<https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>>, consultado el 9 de mayo de 2018.

⁴⁶ A este respecto, el considerando nº 63 del RGPD establece que el derecho de información no debe afectar negativamente a «los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener como resultado la negativa a prestar toda la información al interesado.». La preocupación del legislador acerca de la vulneración de derechos de propiedad intelectual sorprende en tanto en cuando entendemos que tal nivel de profusión haría indudablemente incomprensible la información facilitada al sujeto al carecer éste de la formación o tiempo necesarios para su comprensión en la gran mayoría de los casos.

⁴⁷ Tal vez el WP29 tuviera en mente supuestos en los que el ejercicio de los derechos del usuario se ejercite por asociaciones o agrupaciones que posean los medios suficientes como para el estudio detallado de los

Finalmente y a la luz de la interpretación de los preceptos expuesta, obvio resulta que esta obligación de información sólo abunda en la protección del usuario en la medida en la que el mismo no era consciente de que se estaban realizando técnicas de creación de perfiles sobre su persona o no conocía el alcance de las mismas. Por ello, la previsión del artículo sólo supone un plus de seguridad al afectado por el tratamiento en los supuestos en los que se estaban llevando a cabo técnicas de *profiling* no vinculadas a la toma de decisiones automatizadas ya que, de acuerdo con el artículo 22 RGPD, cuando el *profiling* ha servido de base para este tipo de decisiones el usuario ha debido dar su consentimiento explícito (artículo 22.2.c)) o ha tenido que ser informado por otra vía⁴⁸.

III.3.2. DERECHO DE OPOSICIÓN

Recogido en el artículo 21 del RGPD, el derecho de oposición supone la negativa del afectado por el tratamiento de datos personales al mismo si la licitud de dicho tratamiento se ha justificado de acuerdo con lo previsto en las letras e) (tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos) o f) (satisfacción de intereses legítimos del responsable) del artículo 6 RGPD.

Al igual que los artículos 13 y 14, el artículo 21 menciona expresamente (aunque de forma meramente enfática) la creación de perfiles basada en estos supuestos. Tal y como sucede con cualquier otro tipo de tratamiento, es necesario realizar una ponderación entre los intereses legítimos, derechos y libertades del afectado y los del responsable del tratamiento, remitiéndonos a lo expuesto en sede de licitud basada en intereses legítimos (III.1.1. Licitud, lealtad y transparencia).

De forma similar debemos señalar que el derecho de oposición sólo puede ser ejercido en materia de *profiling* en casos en los que el mismo no se encuentra vinculado a la toma de decisiones automatizadas en tanto en cuando en dicho supuesto no puede ser considerado lícito un tratamiento justificado de forma distinta a la del artículo 22.2 RGPD.

No obstante, sí que merece la pena detenernos en la previsión específica en materia de mercadotecnia directa del apartado 2º y 3º del artículo 21 RGPD ya que, a diferencia de

mismos, si bien no es el supuesto que el legislador parece tener presente al hacer al individuo el centro del ejercicio de este tipo de derechos.

⁴⁸ Por citar un ejemplo, en el caso del artículo 22.2.a), el usuario no ha prestado su consentimiento pero ha debido ser informado de forma fehaciente de que en ejecución de un contrato se estaban realizando técnicas de *profiling* y se le ha debido suministrar información acerca de su alcance.

lo que ocurría en el apartado anterior, el responsable del tratamiento no debe realizar ponderación o juicio alguno sino que la solicitud debe ser cumplida de forma automática. De esta forma, cuando un sujeto se oponga a que sus datos sean utilizados con fines de mercadotecnia directa (y en un gran número de ellos se habrán utilizado técnicas de creación de perfiles) el responsable del tratamiento deberá cesar en el mismo sin posibilidad de oposición o alegación alguna por su parte.

El WP29 ha categorizado esta acción del 21.2 como incondicional, recordando que el considerando nº 70 expresamente recoge la gratuidad del ejercicio del derecho.

III.3.3. OTROS DERECHOS

Bajo este epígrafe se engloban una serie diversa de derechos del sujeto recogidos en el RGPD que, por su escasa diferencia en materia de *profiling* respecto de otro tipo de tratamiento de datos van a ser abordados de forma conjunta.

En primer lugar, el artículo 15 RGPD recoge el llamado **derecho de acceso** por el cual el interesado puede obtener confirmación acerca de si se está realizando un tratamiento de sus datos personales, así como acceder a los mismos y a una serie de información que es básicamente la contenida en los artículos 13 y 14 ya que se replica el tenor literal de los preceptos comentados en el apartado previo. Como previsión específica, el WP29⁴⁹ señala que el sujeto tiene derecho tanto a acceder al perfil creado como a los datos a partir de los cuales se ha elaborado dicho perfil, conclusión lógica pero que permite observar que en este ámbito se realiza la misma interpretación del concepto de *profiling* que en sede de los artículos 13 y 14 al no vincularse (por el WP29) con el supuesto del artículo 22 RGPD.

En segundo lugar, el RGPD también prevé un **derecho de rectificación** en su artículo 16 que trata de atajar de forma poco realista el supuesto en el que el responsable del tratamiento esté utilizando datos personales erróneos de un sujeto y/o haya creado un perfil que no se corresponde con la realidad. De acuerdo con el WP29, ello permitiría al sujeto intervenir en el proceso de creación de perfiles para optimizar el output del mismo, una intervención que como decimos resulta alejada de la realidad. Para ejemplificarlo, se ha procedido a descargar a fecha de 12 de mayo de 2018 toda la información personal

⁴⁹ WP29, *Guidelines on Transparency under Regulation 2016/679*, 2017, <http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025>, consultado el 11 de mayo de 2018.

contenida por Facebook del autor de este trabajo, usuario de la red social desde 2013. El resultado han sido aproximadamente 100 megabytes de información y 65.000 ficheros HTML distintos⁵⁰.

De forma similar se recoge en el artículo 17 RGPD la posibilidad de **suprimir dichos datos** (derecho al olvido) o de **limitar el alcance** del tratamiento de acuerdo con el artículo 18. En la mayoría de estos casos, el ejercer los derechos de los artículos 17 y 18 supondrá que el responsable del tratamiento busque en el artículo 6 RGPD otra vía de licitud para el mismo, siendo el derecho de oposición del artículo 21 RGPD una vía en la práctica más efectiva⁵¹ para impedir el tratamiento de datos personales cuando ya se han iniciado las acciones de *profiling*.

Incompleto sería finalizar este apartado sin señalar las novedades introducidas por el artículo 80.1 RGPD al reconocer de forma expresa la posibilidad de ejercicio de este tipo de derechos por parte de una entidad, organización o asociación sin ánimo de lucro. El legislador europeo recoge aquí la legitimación necesaria para ejercer lo que en el ámbito anglosajón se viene conociendo como *class actions* y que permitiría una tutela jurídica previsiblemente más eficaz al poder actuarse de forma conjunta y no individualmente⁵².

Como señalábamos en apartados anteriores, en la mayoría de casos los ciudadanos carecen del tiempo, medios o conocimiento suficiente como para poder ejercer de forma satisfactoria unos derechos cuyo alcance y contenido suelen resultar desconocidos. La acción pública se articula por tanto como un buen instrumento que permita atajar los inconvenientes señalados al poder contar la hipotética asociación de los medios e instrumentos más idóneos para hacer valer la tutela judicial efectiva de los afectados⁵³.

⁵⁰ En este sentido, en MUÑOZ SORO, J.F y OLVIER-LALANA, A.D., “Derecho y cultura de la protección...cit p. 12 indican que menos del 5% de los ciudadanos consultados en el CIS 2008/09 habían ejercitado en alguna ocasión los derechos de rectificación, oposición y acceso reconocidos en la LOPD.

⁵¹ LEONARD, P., *Customer data analytics: privacy settings for ‘Big Data’ business*, Revista *International Data Privacy Law*, Vol. 4, No. 1, Prensa de la Universidad de Oxford, 2014.

⁵² KANE, P., *GDPR: Collective Actions Under the Privacy Banner*, WSGR Newsletter, 2018, <<https://www.wsgrdataadvisor.com/2018/03/gdpr-collective-actions/>>, consultado el 25 de mayo de 2018.

⁵³ Aunque no es materia directa de este trabajo, de interés puede resultar el estudio del caso Maximilian Schrems v. Facebook Ireland Limited (ECLI:EU:C:2018:37), donde un particular trató de reclamar contra la red social por violación de los derechos relativos al tratamiento de datos personales de más de 25.000 personas que cedieron al mismo el ejercicio de sus acciones legales.

Tanto el Abogado General como el TJUE posteriormente vinieron negando la legitimación de Schrems a la hora de reclamar a Facebook por dichas violaciones, si bien las argumentaciones estuvieron fundadas en la prohibición del *fórum shopping* o elección del foro más favorable. Una reflexión crítica de dicha sentencia sería conveniente a la vista de la regulación de las *class actions* que realiza el artículo 80.1 RGPD.

IV. CONCLUSIÓN

Al igual que ocurre con toda técnica vinculada con las TICs, el *profiling* supone en definitiva un continuo equilibrio entre privacidad y beneficios asociados con el tratamiento de datos personales. Con el objetivo de trasladar las potestades de control al ciudadano, el legislador europeo ha configurado un marco jurídico en el que cobran relevancia las obligaciones de transparencia, licitud y lealtad y se refuerzan las exigencias legales de recogida y tratamiento de datos.

Acorde a esta visión, el *profiling* ha sido recogido en la norma de forma que se trata de atajar sus posibles incidencias en la esfera privada del afectado por el tratamiento, de forma especialmente restrictiva cuando el mismo aparece vinculado a la toma de decisiones automatizadas. En caso contrario, cuando hablamos de creación de perfiles *per se*, el marco jurídico es el general de todo tratamiento, si bien el Grupo de Trabajo del Artículo 29 ha dictaminado expresamente que ciertos derechos como es el de acceso o de información sean extensibles a este tipo de *profiling* independientemente de su vinculación con la toma de decisiones automatizadas. Dicha postura, tal y como se ha relatado, parece exceder de la interpretación literal de la norma pero que recuerda los planteamiento del Parlamento Europeo en las primeras versiones del RGPD.

Personalmente creo que la labor realizada por el WP29 dista mucho de ser la que debería haber sido, o mejor dicho, la que la sociedad demanda. No sólo destaca por escueta (apenas 34 páginas de entre las cuales 28 suponen un aporte material), sino que en ciertos aspectos de la regulación realizan interpretaciones que se alejan del tenor literal de la norma sin explicación o razonamiento alguno, como es el caso de la consideración del artículo 22 RGPD como una prohibición general.

Dada su condición de órgano consultivo europeo en materia de protección de datos y del gran peso que supone a la hora de interpretar el texto (especialmente considerando la inexistencia de jurisprudencia), considero que las opiniones emitidas por organismo deberían haber profundizado en mayor grado en una regulación cuyos interrogantes quitan el sueño a grandes y pequeñas empresas. Una crítica parecida puede hacerse a la AEPD, responsable de la traducción de los documentos del WP29 (no traducidos a fecha de depósito del presente trabajo).

Ambos organismos deberían tomar ejemplo del ICO británico (organismo que desgraciadamente no vamos a poder incluir entre los europeos a la vista del proceso de

Brexit en un futuro cercano) puesto que el mismo ha realizado una intensa labor de clarificación y difusión de las novedades del RGPD así como de la interpretación de muchos de sus preceptos.

Sirva como ejemplo el comunicado emitido por la presidenta del WP29, Andrea Jelinek el pasado 21 de marzo de 2018⁵⁴ a consecuencia del escándalo de *Cambridge Analytica*, donde se limitaba a señalar que el WP29 apoyará las investigaciones del ICO, delegando en el mismo las labores de inspección y control que deberían corresponderle a la UE.

Aunando líneas de pensamiento expuestas a lo largo de todo el trabajo, el optar por una interpretación más restrictiva de unos preceptos que no destacan por su especial claridad no se traduce en una mayor protección jurídica del ciudadano ante los fenómenos de *profiling* sino en el levantamiento de nuevas trabas para las empresas y entes que encuentran en las técnicas de *profiling* ventajas competitivas que en abundantes casos se traducen en beneficios para la sociedad en general.

Si de verdad se aspira a proteger a los ciudadanos europeos ante los posibles riesgos y peligros que entraña el uso de tratamientos tipo *data mining*, la prohibición de toma de decisiones automatizadas puede ser un correcto punto de inicio, pero la regulación debería enfocarse hacia prohibir todo efecto discriminatorio producido sobre los individuos, indiferentemente del tipo de tratamiento utilizado. Lo que realmente afecta al mismo no es el hecho de que la concesión de un crédito le haya sido denegada por un ser humano o por un software, sino que le haya sido denegada exclusivamente por motivos como su estatus social, aspectos concretos de su personalidad, su color de piel o su trayectoria académica.

Esta concepción se encuentra detrás de la norma (como puede observarse de la lectura de los considerandos) pero no tiene reflejo alguno en el cuerpo central del RGPD.

En definitiva y retomando un plano más general, la nueva regulación supone la entrada de forma expresa de la creación de perfiles en el panorama legal europeo, una regulación que plantea importantes interrogantes tanto desde un punto de vista teórico como práctico y cuyo éxito puede permitir atajar las importantes deficiencias en materia de protección de la privacidad a las que se enfrenta el ciudadano europeo del siglo XXI.

⁵⁴ WP29, *Cambridge Analytica statement of the Article 29 Chair*, 2018, <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=617458>, consultado el 23 de mayo de 2018.

BIBLIOGRAFÍA

BRANDÃO, E. Y OTROS, *Predicting the risk associated to pregnancy using data mining*, Algoritmi Research Centre, Universidade do Minho, Guimarães, Portugal, 2015.

CRISTEA UNIVARU, L.N., «La protección de datos de carácter sensible en el ámbito europeo», Prensas de la Universitat Abat Oliba CEU, 2017, pags 221-319.

DATA PROTECTION NETWORK, *Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation*, 2017 <<https://smartmessenger.co.uk/media/104621/dpn-guidance-a4-publication.pdf>>, consultado el 25 de abril de 2018.

FORO ECONÓMICO MUNDIAL, *Unlocking the value of personal data: from collection to usage*, Industry Agenda, <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf>, p.4, consultado el 24 de abril de 2018.

GIL, E. « Big data, privacidad y protección de datos», Imprenta Nacional de la AEPD, 2016 <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Big_Data_Privacidad_y_proteccion_de_datos.pdf>, consultado el 23 de abril de 2018.

GOODMAN, B., FLAXMAN, S., *European Union regulations on algorithmic decision-making and a “right to explanation”*, Prensa de la Universidad de Oxford, 2016, p.7

HILDEBRANDT, M., *Defining profiling: a new type of knowledge?*, *Profiling the European Citizen*, Springer, 2008, pags 17-45.

HILDEBRANDT, M. *Slaves to Big Data. Or Are We?*, Revista de internet, derecho y política, Universitat Oberta de Catalunya, vol. 17, Octubre de 2013, ISSN 1699-815, pag. 27. <<http://www.raco.cat/index.php/IDP/article/viewFile/303366/393038>>, consultado el 22 de abril de 2018.

El *profiling* en el Reglamento General de Protección de Datos

ICO, *Big data, artificial intelligence, machine learning and data protection*, 2017, <<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>> consultado el 11 de abril de 2018.

ICO, *Overview of the General Data Protection Regulation*, 2017, <<https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf>>, consultado el 25 de abril de 2018.

ICO, *Consultation: GDPR consent guidance*, 31 de marzo de 2017. <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>>, consultado el 28 de abril de 2018

ICO, *Feedback request – profiling and automated decision making*, 2017, p.15 <<https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>>, consultado el 9 de mayo de 2018

KUMAR SINGH, VISHNU SWAROOP, *Data Security and Privacy in Data Mining: Research Issues & Preparation*, International Journal of Computer Trends and Technology, nº 4I volume 2º, pags. 194 a 223, 2013.

LEE, P. *Let's sort out this profiling and consent debate once and for all*, 2018 <<https://privacylawblog.fieldfisher.com/2017/let-s-sort-out-this-profiling-and-consent-debate-once-and-for-all>>, consultado el 7 de mayo de 2018.

LEI XU, CHUNXIAO JIANG, JIAN WANG Y OTROS, *Information Security in Big Data: Privacy and Data Mining*, Institute of Electrical and Electronics Engineers Magazine, nº 2, pags 1149-1167, 2014.

LEONARD, P., *Customer data analytics: privacy settings for 'Big Data' business*, Revista *International Data Privacy Law*, Vol. 4, No. 1, Prensa de la Universidad de Oxford, 2014

MUÑOZ SORO, J.F; OLIVER-LALANA, D. « El mito del consentimiento y el fracaso del modelo individualista de protección de datos », Cizur Menor (Navarra): Aranzadi, 2013.

MUÑOZ SORO, J.F.; OLIVER-LALANA, D. « Derecho y cultura de protección de datos: un estudio sobre la privacidad en Aragón », Dykinson (Madrid), 2012.

OGURO, K. *Big Data - Key to the 4th Industrial Revolution*, 2016, Revista *Innovation in the Global Economy*, nº3, 2016.

PRIVITAR LTD., *Delivering big data analytics under the general data protection regulation*, 2015, <https://cdn2.hubspot.net/hubfs/2156179/Privitar_Live_Folder/PDF_Files/Privitar_GDPRPBD.pdf?t=1476889649956>, consultado el 11 de abril de 2018.

ROGERS, D. y A., SECURATO, J.R., *About psychological variables in application scoring models*, Revista de administración de empresas, vol.55 no.1 São Paulo, 2015.

SAINZ, C.A.; ACED, E.; DEL ÁLAMO, J.M. y otros, « Código de buenas prácticas en protección de datos para proyectos *Big Data* », Prensas Oficiales de la AEPD, 2016, p. 17.

SCHAUER F., *Profiles, probabilities and stereotypes*, Harvard University Press, Cambridge, 2006

STARAN, E., HORDERN, V. *Automated Decision-Making Under the GDPR – A Right for Individuals or A Prohibition for Controllers?*, Hogan Lovells, 2017.

SLAUGHTER AND MAY, *Tracking, watching, predicting... lawfully responsible profiling under the GDPR*, 2017, <<https://www.slaughterandmay.com/media/2536527/profiling-under-the-gdpr-september-2017.pdf>>, consultado el 12 de mayo de 2018.

TURVEY, B.E., *Criminal profiling: an introduction to behavioural evidence analysis*, Elsevier, 2012, p. 34.

VALLETTI, T., WU, J., *Big Data vs Small Data: Costumer Profiling with data requirements*,

El *profiling* en el Reglamento General de Protección de Datos

<http://www.haas.berkeley.edu/groups/marketing/sics/pdf_2016/paper_vw.pdf>, consultado el 28 de marzo de 2018.

ZHANG, D.S.G.; KEQUIN LI, M. *Key Technologies for Big Data Stream Computing*, Tsinghua University of Beijing, 2017.

ZARSKY, T.Z., *Incompatible: The GDPR in the Age of Big Data*, Seton Hall Law Review, Vol. 47, No. 4(2), 2017.

DOCUMENTOS DEL WP29

WP29, *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation*, 2013 <http://www.medialaws.eu/wp-content/uploads/2013/05/20130513_advice-paper-on-profiling_en.pdf>, consultado el 13 de mayo de 2018.

WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017, <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826> consultado el 21 de abril de 2018.

WP29, *Guidelines on Transparency under Regulation 2016/679*, 2017, <http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025>, consultado el 11 de mayo de 2018.

WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 2014 <<http://www.dataprotection.ro/servlet/ViewDocument?id=1086>>, consultado el 2 de mayo de 2018

WP29. *Opinion 03/2013 on purpose limitation*, 2013. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, consultado el 24 de abril de 2018.

LEGISLACIÓN

Comisión Europea, *DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7 0025/2012 – 2012/0011(COD))*, 16 de enero de 2013

Reglamento (UE) 2016/679 (RGPD) 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)

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

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

OTROS

BSH, *Data Privacy Policy for the Home Connect website*, <<http://www.home-connect.com/global/meta-pages/data-protection>> consultado el 3 de abril de 2018.

KANTAR MEDIA, *Flash Eurobarometer 443: e-Privacy*, EU Open Data Portal <https://data.europa.eu/euodp/data/dataset/S2124_443_ENG>, consultado el 23 de abril de 2018.

TUCKER, P., *Refugee or Terrorist? OBM Thinks Is Software Has the Answer*. <<http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-hasanswer/125484/>> Consultado el 05 de abril de 2018.

ANEXOS

ANEXO I- Extracto del borrador del RGPD elaborado por el Parlamento Europeo



EUROPEAN PARLIAMENT

2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2012/0011(COD)

16.1.2013

*****I**

DRAFT REPORT

on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Jan Philipp Albrecht

Amendment 38

Proposal for a regulation Recital 58

Text proposed by the Commission

(58) Every natural person should have the right not to be subject to **a** measure **which is** based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.

Amendment

(58) Every natural person should have the right not to be subject to **profiling** or measures based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject. **Such measures should not lead to discrimination, concern children, or produce legal or significant effects for the data subject without human intervention.**

Or. en

Justification

As is the case with any collection, processing and use of data, a general ban is introduced on profiling as defined in Article 4 and it is only permissible where provided for by law, i.e. either by means of the data subject's consent or a statutory provision. Consent will primarily be an option in the private sector (including contracts), whereas statutory permission will especially but not only be relevant in the public sector. Including the requirement that the data subject must consent to the profiling prevents what often happens in practice, namely that profiles are created without the data subject's knowledge. See related amendments to Articles 4(3b), 14(1)(g), (ga), (gb), 15(1), 20.

Amendment 131

Proposal for a regulation

Article 14 – paragraph 1 – point g) a (new)

Text proposed by the Commission

Amendment

(ga) where applicable, information about the existence of profiling, of measures based on profiling, and of mechanisms to object to profiling;

Or. en

Justification

This provision is moved from Article 20(4) on profiling to Article 14 on information obligations, in order to ensure all information obligations are covered under one article. The addition of "mechanisms to object..." is relevant to ensure information about standards such as Do Not Track. See related amendments to Articles 4(3b), 14(1)(g), and (gb), 15(1), 20(4).

Amendment 136

Proposal for a regulation

Article 15 – paragraph 1

Text proposed by the Commission

Amendment

1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

1. The data subject shall have the right to obtain from the controller at any time, on request, ***in clear and plain language***, confirmation as to whether or not personal data relating to the data subject are being processed, ***and as to the existence of profiling and measures based on profiling in respect of the data subject*** the controller shall provide the following information:

Or. en

Justification

In order to ensure an informed consent to profiling activities, these need to be defined and regulated. See related amendments to Articles 4(3b) 14(1)(g), (ga) and (gb), 20.

Amendment 138

Proposal for a regulation Article 15 – paragraph 1 – point h)

Text proposed by the Commission

(h) the ***significance and*** envisaged consequences of ***such processing, at least in the case of measures referred to in Article 20.***

Amendment

(h) the envisaged consequences of ***profiling and of measures based on profiling;***

Or. en

Justification

In order to ensure an informed consent to profiling activities, these need to be defined and regulated. See related amendments to Articles 4(3b) 14(1)(g), (ga) and (gb), 20.

Amendment 158

Proposal for a regulation Article 20– paragraph 1

Text proposed by the Commission

Measures based on ***profiling***

1. ***Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.***

Amendment

Profiling

1. ***The processing of personal data for the purposes of profiling, including in relation to the offering of electronic information and communication services, shall only be lawful if it:***

Or. en

Justification

As is the case with any collection, processing and use of data, a general ban is

introduced on profiling as defined in article 4, and it is only permissible where provided for by law, i.e. either by means of the data subject's consent or a statutory provision. Consent will primarily be an option in the private sector (including contracts), whereas statutory permission will especially, but not only be relevant in the public sector. Including the requirement that the data subject must consent to the profiling prevents what often happens in practice, namely that profiles are created without the data subject's knowledge. See related amendments to Articles 4(3b) 14(1)(g), (ga) and (gb), 15(1).

ANEXO II- Ejemplo de datos personales utilizados en la toma de decisiones automatizadas

Tablas extraídas del trabajo *About psychological variables in application scoring models* de ROGERS, D. y A., y SECURATO, J.R.⁵⁵

Tabla 1- Variables sociodemográficas utilizadas por entidades de crédito a la hora de calificar la confianza crediticia que merece un potencial cliente.

VARIABLE	DESCRIPTION
AGE	Age (years)
MALE	Gender (male or female)
FROM	State of origin (birth)
SCHOOL	Level of education
MARITAL	Marital Status
NPEOPLE	Number of people living in house
FINANCIALDEP	Number of financial dependents
RESTATUS	Status of the residence (own or not)
SCHOOLSPOUSE	Level of education of spouse
RETYPE	Type of property (house, apartment, etc.)
RETIME	Period (years) living in the residence
JOB	Current occupation (job)
JOBTIME	Period in the occupation stated
JOBSPOUSE	Occupation of spouse
INCOME	Gross monthly income
INCOMESPOUSE	Gross monthly income of spouse
INCOMEFAMILY	Gross monthly income of family
NVEHICLES	Number of vehicles owned
VRVEHICLES	Estimated value of the vehicles stated
PROPERTY	Number of properties
VRPROPERTY	Estimated value of the properties stated
INVESTMENTS	Existence of financial investments

⁵⁵ ROGERS, D. y A., SECURATO, J.R., *About psychological variables in application scoring models*, Revista de administración de empresas, vol.55 no.1 São Paulo Jan./Feb. 2015.

Tabla 2- Escalas psicológicas utilizadas por entidades de crédito a la hora de calificar la confianza crediticia que merece un potencial cliente.

CONSTRUCT	VARIABLE	DESCRIPTION
Meaning of money scale	TRANSC (0.66)	Positive meaning assigned to money in the broadest social context. When associated with spirituality, money builds a better world, generating social prosperity
	INEQUALITY (0.84)	Negative meaning assigned to money in the broadest social context. Money generates inequality, social exclusion and domination
	HARMONY (0.83)	Positive meaning assigned to money. Money brings happiness, joy, wellbeing and harmony among people
	CONFLICT (0.83)	Negative meaning assigned to money in the context of interpersonal relationships. Money generates disharmony and conflicts among people
	ALTRUISM (0.76)	Personal altruistic and optimistic disposition regarding money in interpersonal relationships. Using own money to fund science, culture, arts and help people
	SUFFERING (0.67)	Personal difficulty dealing with money. Pessimistic and negative feelings related to money, such as depression, anxiety and impotence
	MMSNEG (0.88)	Negative meaning assigned to money (INEQUALITY + CONFLICT + SUFFERING)
	MMSPOS (0.84)	Positive meaning assigned to money (TRANSC + HARMONY + ALTRUISM)
Self-efficacy	SELFEFFICACY (0.81)	Schwarzer's (1992) General Self-Efficacy Scale, which proposes measuring the belief that individuals have regarding their ability to organize and perform actions required to handle a wide range of challenging situations, including those in the future, in an effective manner, that is, achieving specific goals proposed
Locus of control (Lenvenson scale)	INTER (0.68)	Subscale Internality, which measures the degree to which individuals believe they keep track of their lives
	OPOWER(0.77)	Subscale Other Powerful People, which measures the perception that this control is in the hands of powerful people
	CHANCE (0.74)	Subscale Chance, which refers to the perception of being controlled by chance, luck or fate
Optimism	OPTIMISM (0.60)	Life Orientation Test (LOT) proposed by Scheier <i>et al.</i> , (1994) which aims to measure the degree of favorable expectations that people have about future events that will occur in their lives

CONSTRUCT	VARIABLE	DESCRIPTION
Self-esteem (Rosenberg scale)	LOWSE (0.70)	Subscale that seeks to obtain the degree of feeling of incompetence, inadequacy in life and inability to overcome challenges
	HIGHSE (0.78)	Subscale that seeks to express the degree of confidence and competence
	SELFESTEEM (0.81)	Self-evaluation, expressing an attitude of approval or disgust of oneself, including a self-judgment regarding competence and value (LOWSE + HIGHSE)
Compulsive buying	SCORECB (0.73)	The Faber and O'Guinn Scale (1992) attempts to measure the tendency to buy in a repetitive and chronic manner, which becomes a primary response to negative events or feelings. Such purchases are likely to be beyond needs and resources
	CLASIFCB (-)	= 1 if SCORECB \leq - 1.34; = 0 otherwise