Nº 86
Enero-Abril 2019

INSTITUTO DE DERECHO Y ÉTICA INDUSTRIAL

COMUNICACIONES
EN PROPIEDAD INDUSTRIAL Y DERECHO DE LA COMPETENCIA

Novedades sobre la investigación sanitaria: el Dictamen 3/2019 del Comité Europeo de Protección de Datos

La reforma del Reglamento CCP y la excepción de fabricación para la exportación. Estado de la cuestión

El Real Decreto-ley 23/2018, de 21 de diciembre. Novedades de la reforma de la Ley 17/2011, de Marcas

La elaboración de perfiles en el contexto del marketing personalizado

Informe de la Comisión Europea aplicación de las normas de competencia en el sector farmacéutico (2009-2017) Competencia en innovación

IDEI

DOCTRINA · LEGISLACIÓN · JURISPRUDENCIA

FUNDACIÓN CEFI
Centro de Estudios para el Fomento de la Investigación

SECCIONES

ACTUALIDAD · PROPIEDAD INDUSTRIAL
PROPIEDAD INTELECTUAL
COMPETENCIA · PUBLICIDAD · ÉTICA
LEGISLACIÓN Y NOTICIAS

INSTITUTO DE DERECHO Y ÉTICA INDUSTRIAL
Comunicaciones en Propiedad Industrial y Derecho de la Competencia

Comunicaciones en Propiedad Industrial y Derecho de la Competencia es una publicación especializada en Propiedad Industrial, Derecho de la Competencia y Competencia Desleal, aborda también cuestiones como la Publicidad y la Propiedad Intelectual en sus aspectos legislativo, doctrinal y jurisprudencial, así como en sus ámbitos nacional y comunitario europeo e internacional. Se dirige a un público especializado en estas materias (abogados, profesionales de los sectores implicados, docentes universitarios).

Nº 86 Enero-Abril 2019

IDEI

Esta publicación se haya incluida en:

BASE DE DATOS ISOC

Publicado por:

CEFI. Instituto de Derecho y Ética Industrial (IDEI)
Avda. del Brasil, 17, 9.º B • Tel.: 91 556 40 49 • 28020 Madrid • www.cefi.es

Directora: Nuria García García. *Directora General Fundación CEFI*
Documentalista: Victoria Gutiérrez Pérez. *Documentalista Fundación CEFI*

Depósito Legal: M-35.681-98
ISSN: 1579-3494

Imprime: Industria Gráfica MAE S.L.
Diseño de la portada: Caracteres

IV. PUBLICIDAD

LA ELABORACIÓN DE PERFILES EN EL CONTEXTO DEL *MARKETING* PERSONALIZADO

Fecha de recepción: 28 marzo 2019
Fecha de aceptación y versión final: 8 abril 20198

Laia Reyes Rico
Abogada Uría Menéndez

Resumen

La utilización de técnicas aplicadas de inteligencia artificial en el ámbito publicitario generalmente implica un tratamiento de datos personales, dado que dichas técnicas son empleadas para perfilar a los usuarios. En este sentido, el artículo analizará el alcance y los límites del perfilado previstos en la normativa de protección de datos (en particular, el Reglamento General de Protección de Datos 2016/679). Dicho análisis se abordará teniendo en cuenta la posición de las autoridades competentes en la materia frente a la realización de campañas de marketing ajustadas a los gustos y preferencias de los usuarios. En el artículo se diferenciarán los requisitos exigidos por la normativa aplicable dependiendo de la tipología de datos obtenidos y tratados (p.ej., si se tratan datos especialmente protegidos o anonimizados) y las herramientas utilizadas (p.ej. cookies) para llevar a cabo las actividades de perfilado.

Palabras Clave

Protección de datos, perfiles, inteligencia artificial, cookies y marketing.

Abstract

The use of applied artificial intelligence techniques in the marketing sector tends to involve some form of data processing, given that such techniques are used with the purpose of creating user profiles. This article will analyse the scope and limits of profiling activities according to the provisions set out in the data protection regulations (in particular, the General Data Protection Regulation 2016/679). This analysis will take into account the opinion of the data protection authorities on marketing campaigns tailored to users' tastes and preferences. The requirements set out in the applicable laws will be analysed separately depending on the categories of data obtained and processed (e.g.

if specially protected categories of data or anonymised data are processed) and the techniques used (e.g. cookies) to carry out the profiling activities.

Keywords

Data protection, profiling, artificial intelligence, cookies and marketing.

1. INTRODUCCIÓN

Las nuevas tecnologías abren –a un ritmo vertiginoso– un sinfín de posibilidades para las compañías, entre otros, en el sector del *marketing*. En este campo, una de las técnicas que más se está explotando es el *big data analytics* (i. e., el análisis de datos o información a gran escala) con el fin de elaborar perfiles sobre los usuarios y, así, poderles enviar comunicaciones comerciales y mostrarles anuncios personalizados.

Dado que esta práctica implica el tratamiento de datos personales de los usuarios, este artículo analizará el alcance y los límites del perfilado, tal y como se prevé en la normativa de protección de datos y cuáles son las facultades y los límites de las compañías para llevar a cabo dicha actividad. En particular, el artículo se centrará en analizar la posición de la normativa y las autoridades competentes en la materia sobre el *marketing* ajustado a los gustos y preferencias de los usuarios. Dicho análisis diferenciará los requisitos exigidos por la normativa aplicable dependiendo de la tipología de datos obtenidos y tratados (p.ej., si se tratan datos sensibles o datos anonimizados) y las herramientas utilizadas (p.ej., *cookies*) para llevar a cabo las actividades de perfilado.

2. USO DEL *BIG DATA ANALYTICS* EN EL SECTOR DEL *MARKETING*

El *big data analytics* consiste[1] en utilizar técnicas aplicadas de inteligencia artificial ("***IA***"), principalmente los algoritmos[2] de aprendizaje automático (*machine learning*), para analizar información agregada o datos a gran escala (big data). Con el fin de desgranar estos conceptos técnicos, cabe aclarar sucintamente que la IA se compone de *"sistemas que muestran un comporta-*

1. Autoridad del Reino Unido en materia de protección de datos (*"ICO"*): Big data, artificial intelligence, *machine learning* and data protection (pág. 8) (https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf). [Traducción al español de la versión original].

2. Autoridad francesa de protección de datos (*"CNIL"*): The ethical matters raised by algorithms and artificial intelligence, diciembre de 2017 (https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf). En esta guía se definen los algoritmos como *"La descripción de una secuencia finita e inequívoca de pasos o instrucciones para producir un resultado (output) a partir de datos de entrada (input)"* [Traducción al español de la versión original].

miento inteligente al analizar su entorno y al realizar acciones, con cierto grado de autonomía, para lograr un objetivo específico"[3]. Por su parte, el *machine learning* es una técnica de IA *"basada en mecanismos automatizados a través de los cuales los ordenadores pueden adquirir y aprender nuevos conocimientos y, por ello, pueden interactuar sin ser expresamente programados"*[4]. Por último, el big data es el *"conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos [o información] a [gran] escala"*[5].

Una vez explicados estos términos, hay que apuntar que el uso de estas técnicas de *big data analytics* implica un tratamiento de datos personales o de información agregada o anonimizada. En particular, en el sector de la publicidad, estas herramientas de IA se suelen nutrir de datos personales para generar perfiles de los usuarios (si bien estos algoritmos se pueden utilizar con otros fines, como por ejemplo para adoptar decisiones automatizadas o con fines estadísticos). En otras palabras, en este contexto, las herramientas de IA son usadas mayoritariamente para inferir con exactitud el perfil de los usuarios (a título enunciativo, qué tipo de ropa o destino de vacaciones les pueden interesar) basándose, por ejemplo, en sus hábitos de navegación por diferentes sitios web o en los movimientos de sus transacciones bancarias. Este seguimiento de los usuarios, prolongado en el tiempo, permite construir un determinado perfil sobre un cliente y, así, ajustar la publicidad a sus características.

Aunque los algoritmos de aprendizaje automático –y, con ello, las predicciones sobre los perfiles de los usuarios– mejoran cuantos más datos se recaban y cuanto más tiempo se tratan dichos datos, la normativa aplicable exige ciertas garantías para poder llevar a cabo dichos tratamientos de datos personales (i. e., la creación de perfiles), ya que el *big data analytics* tiene un fuerte impacto[6] sobre la privacidad. La normativa que establece cuáles son las facultades y los límites de las empresas para llevar a cabo perfilados con fines publicitarios está compuesta por el Reglamento General de Protección de Datos 2016/679 (el "***RGPD***") y la nueva Ley Orgánica 3/2018 de Protección de Datos Personales y Garantías de los Derechos Digitales (la "***LOPD***").

3. Grupo de Expertos de la Comisión Europea de IA: A definition of AI: main capabilities and scientific disciplines, the European Commission's High-Level Expert Group on Artificial Intelligence, 18 de diciembre de 2018 (https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december.pdf [Traducción al español de la versión original].

4. CNIL: The ethical matters raised by algorithms and artificial intelligence, diciembre de 2017.

5. Agencia Española de Protección de Datos: Código de Buenas Prácticas en Protección de Datos para Proyectos Big Data (el *"Código de Big Data"*), sección I.1. (pág. 3), (https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf).

6. Entre los riesgos que presenta la implementación de técnicas de big data analytics, el ICO ha destacado, en su guía sobre big data (pág. 9) anteriormente citada, los siguientes: *"a) El uso de algoritmos, la opacidad del proceso, c) la tendencia a obtener datos de forma masiva, d) la reutilización de los datos y e) el uso de nuevas categorías de datos"* [Traducción al español del texto original].

Además, si dichos perfilados se nutren de datos personales obtenidos a través de tecnologías de seguimiento y obtención de la huella digital (incluyendo *cookies* y tecnologías similares) o si los perfiles se utilizan para enviar comunicaciones comerciales por medios electrónicos[7] ajustadas a las preferencias de los usuarios (i.e., publicidad comportamental), existe una norma especial que resultaría de aplicación. Esta norma es la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (la "***LSSI***"), que será revisado por el borrador de Reglamento europeo sobre la privacidad y las comunicaciones electrónicas (el "***Reglamento de e-Privacy***").

De acuerdo con lo anterior, y con el fin de que las compañías puedan maximizar los beneficios brindados por las tecnologías que aplican IA[9] para tratar datos personales, en particular para generar perfiles en el marco de las campañas de *marketing*, a continuación se analizan los límites establecidos por la citada normativa y las pautas fijadas por las autoridades competentes en materia de protección de datos[10].

3. CREACIÓN DE PERFILES

El punto de partida debe ser conocer qué actividades implican la elaboración de perfiles y, en consecuencia, que las compañías puedan identificar cuándo deben adoptar, además de todas las obligaciones impuestas por la normativa de protección datos, las garantías específicas para perfilados que exige el RGPD. Para ello, se explica a continuación el significado de la acción de perfilar.

El concepto de perfilar o de crear perfiles sobre personas físicas se define en el RGPD[11] como *"toda forma de* ***tratamiento automatizado*** *de* ***datos personales*** *consistente en utilizar datos personales para* ***evaluar*** *determinados* ***aspectos personales*** *de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, sa-*

7. El envío de comunicaciones comerciales por vía postal se regula por la normativa de protección de datos. Las llamadas con fines comerciales (tanto automatizas como no automatizadas) se regulan en una norma especial (el art. 96 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias) y, de forma complementaria, por la normativa de protección de datos.

8. El texto actual del borrador del Reglamento de e-Privacy es el que se muestra en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=ES.

9. Además, el Grupo de Expertos de la Comisión Europea en IA publicará en abril de este año unas Directrices Éticas sobre una IA confiable. El borrador de dichas Directrices se puede localizar en el siguiente enlace: https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai.

10. Esas autoridades son la Agencia Española de Protección de Datos (*"AEPD"*) y el Comité Europeo de Protección de Datos *("CEPD"*, o en inglés, el European Data Protection Board), que es el organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la UE y que promueve la cooperación entre las autoridades de protección de datos de la UE. Con la entrada en vigor del RGPD, el CEPD ha sustituido al Grupo de Trabajo del Artículo 29 (el *"GT29"*).

11. El RGPD define la elaboración de perfiles en su art. 4.4.

lud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física". De acuerdo con dicha definición, el perfilado es una categoría de tratamiento de datos que tiene lugar si concurren estos dos requisitos: a) que el tratamiento de datos se lleve a cabo de forma automatizada y b) que dicho tratamiento tenga por objeto evaluar a una persona física o a un grupo de individuos.

Tratar un dato de forma automatizada implica procesar dicho dato con herramientas tecnológicas, por ejemplo a través de algoritmos de *machine learning*. Cabe aclarar que, dado que el RGPD no exige que el perfilado conlleve un tratamiento *"únicamente"* automatizado, la participación humana en el proceso de perfilado no determina la inexistencia de una elaboración de perfiles.

Por su parte, el término *evaluar* implica –tal y como señala el GT29 en su *Guía de Perfilados*[12]*– hacer un juicio sobre una persona o "hacer predicciones o sacar conclusiones sobre una persona, aspectos personales de una persona física"*. En este sentido, la mera clasificación de las personas por características como, por ejemplo, la ciudad de residencia, edad o sexo no implicaría necesariamente la elaboración de un perfil. La elaboración de perfiles conlleva crear *"nuevos"* datos personales que no han sido directamente facilitados por los propios interesados, con el fin de hacer predicciones o deducciones estadísticas sobre su capacidad de realizar una tarea, sus intereses o su comportamiento futuro.

Una vez aclarado qué es perfilar, cabe señalar que –tal y como se indicaba anteriormente– existe otra actividad muy común en el ámbito de la publicidad: la toma de *"decisiones automatizadas"*, que –en ocasiones– se confunde con el perfilado. No obstante, la adopción de decisiones automatizadas tiene un ámbito de aplicación distinto al del perfilado. En particular, las decisiones automatizadas son las acciones adoptadas a través de medios tecnológicos sin la participación de seres humanos. Las decisiones automatizadas pueden llevarse a cabo con o sin la elaboración de perfiles, y la elaboración de perfiles, a su vez, puede no conllevar la toma de decisiones automatizadas. Por ejemplo, una decisión automatizada sería la inclusión en determinados sitios web de anuncios sobre restaurantes de Valencia a usuarios que se conecten a dicha web desde una dirección IP[13] ubicada en dicha ciudad. Esta inclusión de publicidad en línea, de forma automática, no implicaría la elaboración de un perfil del usuario residente

12. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (las *"Guía de Perfilados"*), adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018 por el GT29 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053).

13. La dirección IP o el Internet Protocol es un número que identifica a una interfaz en red de un dispositivo.

en Valencia (ya que no se realizaría una evaluación sobre el usuario, simplemente se detectaría la dirección de IP conectada desde Valencia). Sin embargo, si durante dos años se monitorizan los hábitos de navegación (i. e., se perfila) de dicho usuario por distintos sitios web de restaurantes para determinar qué tipo de comida prefiere (p. ej., detectando que tiene tendencia a acceder a ofertas y descuentos de restaurantes japoneses) con el fin de mostrarle anuncios en línea ajustados a su perfil, la inclusión de esta publicidad sí supondría la adopción de decisiones automatizadas basadas en el perfil del usuario. Por lo tanto, en este último caso, sí tendría lugar la generación de un perfil.

4. REQUISITOS PARA PODER PERFILAR CON FINES DE *MARKETING*

El perfilado es un tratamiento de datos en sí mismo. En ocasiones los perfilados se convierten en una especie de *"tratamientos no informados"* para los usuarios, ya que las compañías tienden a subsumirlos en otros tratamientos (p.ej., el envío de comunicaciones comerciales). No obstante, el perfilado es una actividad de tratamiento independiente que generalmente está directamente relacionada (pero no integrada) o es necesaria para llevar a cabo otros tratamientos. Este sería el caso, por ejemplo, del envío de *marketing* personalizado, ya que para llevar a cabo dicho envío sería necesario que, previamente, se haya realizado un perfilado. En este supuesto, por lo tanto, se habrían dado dos tratamientos diferenciados de datos (en primer lugar, el perfilado y, en segundo lugar, el envío de *marketing*).

Dado que el perfilado es una categoría de tratamiento de datos, las compañías que creen perfiles deben cumplir con todos los requisitos exigidos por el RGPD para poder tratar datos personales. No obstante, el RGPD incluye garantías adicionales y específicas para la creación de perfiles En línea con lo anterior, las compañías que creen perfiles deben cumplir, en primera instancia, con todos los requisitos exigidos por el RGPD para tratar datos personales. Adicionalmente, el RGPD incluye garantías específicas para la creación de perfiles (ya que es un tratamiento de datos que podría ser más intrusivo). En este sentido, para que las compañías realicen perfilados lícitos, leales y transparentes[14], deberían adoptar los requisitos que se exponen a continuación.

14. El RGPD, en su art. 5.1.a) señala –como principio general– que los datos deben ser *"tratados de manera lícita, leal y transparente en relación con el interesado"*.

4.1. Existencia de una base jurídica

Antes de comenzar a tratar un dato se debe comprobar si existe una base jurídica. Las bases jurídicas para llevar a cabo los tratamientos de datos están tasadas en el art. 6 del RGPD (existencia de una obligación legal, consentimiento del cliente, interés legítimo de la compañía, etc.). En otras palabras, si no se reúne al menos una de las circunstancias expuestas en el citado artículo, no se pueden tratar datos personales. En el contexto de la elaboración de perfiles con fines de *marketing*, las dos bases jurídicas (de las enumeradas en el art. 6 del RGPD) que, como norma general, podrían ser de aplicación son a) el consentimiento inequívoco de los clientes o b) la existencia de un interés legítimo de la compañía que va a realizar el perfilado.

Respecto de estas dos bases jurídicas, la que más zozobras genera (y, por ello, en la que nos centraremos) es la determinación de cuándo existe un interés legítimo y cuándo no. Para abordar la cuestión de una manera práctica hay que, o bien acudir a los Considerandos del RGPD que establecen presunciones de existencia de interés legítimo, o bien *"rescatar"* informes, opiniones o resoluciones de las autoridades de protección de datos en las que se haya generado un precedente sobre la existencia de un interés legítimo en un determinado escenario.

Siguiendo el planteamiento anterior, hay que tener en cuenta que el Considerando 47 del RGPD señala que *"el tratamiento de datos personales con fines de* ***mercadotecnia directa*** *puede considerase realizado por* ***interés legítimo****"*. Además, dicha presunción ha sido corroborada por, entre otras autoridades, el GT29 –en su Guía de Perfilados[15] – y por la AEPD en ciertas guías e informes[16] .

15. La Guía de Perfilados del GT29, sección B.6 (pág. 16), señala que *"La elaboración de perfiles se permite si es necesaria para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero"*.

16. En el Código de Big Data de la AEPD (págs. 10 y 11) se indica que *"[...] Una de las cuestiones básicas y previas es el primer elemento del análisis, la existencia de un interés legítimo del responsable. El Dictamen menciona varios casos en los que dicho interés puede existir, tales como la libertad de información y expresión, las actividades de marketing o publicidad, prevención del fraude o mal uso de servicios, seguridad, finalidades científicas, estadísticas o de investigación. El Dictamen hace también mención a la personalización de ofertas comerciales y actividades de marketing online y offline"*.

Asimismo, la AEPD ha confirmado la aplicación del interés legítimo para llevar a cabo perfilados, entre otras, en la sección V de su Informe del Gabinete Jurídico núm. 195/2017 (el *"Informe 195/2017"*) (https://www.aepd.es/media/informes/2017-0195-interes-legitimo-portabilidad-y-blanqueo.pdf): *"Por todo ello, sería posible amparar en el artículo 6.1 f) del Reglamento general de protección de datos el tratamiento por parte de la entidad de la información de que disponga en relación con los productos y servicios contratados por sus clientes para evaluar su solvencia a efectos de ofrecerle nuevos productos que impliquen financiación, siempre que el cliente haya sido informado con la debida separación acerca de este tratamiento y tenga en todo caso la posibilidad de ejercer específicamente su derecho de oposición respecto del mismo"*.

No obstante, tal y como han matizado las citadas autoridades, el interés legítimo no eximiría del deber de recabar el consentimiento inequívoco en dos casos: a) en los supuestos en los que los perfilados implicasen el tratamiento de datos especialmente protegidos[17] o b) si dichos perfilados fuesen muy complejos o intrusivos[18].

• Respecto del primer caso, hay que decir que los perfilados pueden generar datos de categoría especial por inferencia, al combinarse con otros datos, a partir de datos que no son especialmente protegidos. Por ejemplo, tal y como señala el GT29 en su Guía de Perfilados, *"es posible inferir el estado de salud de una persona a partir de los registros de su compra en combinación con datos sobre la calidad y el contenido enérgico de los alimentos"*[19]. Por lo tanto, cuando se traten categorías de datos especialmente protegidos para llevar a cabo los perfilados, se debería valorar si dicho tratamiento podría ser lícito y, en su caso, recabar el consentimiento expreso de los afectados.

• En relación con el segundo supuesto, para determinar si un perfilado es excesivamente complejo, el GT29 en su Guía de Perfilados sugiere que se evalúen los siguientes aspectos[20]: a) el nivel de detalle del perfil, b) la exhaustividad del perfil, c) las consecuencias de elaboración del perfil y d) las garantáis destinadas a garantizar la lealtad[21], la no discriminación y la precisión del proceso de elaboración de perfiles.

Asimismo, tanto el GT29 como la AEPD se han pronunciado con distintos ejemplos prácticos sobre qué tipo de perfilados deberían ser considerados complejos. Así, el GT29 en su Guía de Perfilados ha interpretado que un perfilado muy intrusivo podría ser aquel que conllevase el *"seguimiento de un usuario en distintos sitios web, ubicaciones, dispositivos móviles"*[22]. En este mismo sentido, la AEPD ha señalado que un perfilado complejo

17. El tratamiento de los datos especialmente protegidos se regula en el art. 9 del RGPD.

18. El Código de Big Data de la AEPD, sección II.1. (pág. 11) dispone lo siguiente: *"[...] No obstante, advierte, que aun existiendo ese interés legítimo, éste no es base suficiente para la ejecución de complejos perfilados de clientes que representarían una intrusión significativa en su privacidad. Estaríamos en este caso en un impacto sobre los interesados que hay que tener en cuenta en el mencionado análisis de balance. Por tanto, la existencia de un interés legítimo no es base suficiente, pero sí necesario en el análisis. Habrá que tener en cuenta el impacto del tratamiento en los derechos fundamentales y libertades de los interesados"*.

19. Guía de Perfilados del GT29, sección C (pág. 16).

20. Guía de Perfilados del GT29, sección B.6. (pág.16).

21. En el resumen del Proyecto de Directrices Éticas sobre una IA Confiables, Grupo de expertos de alto nivel sobre inteligencia artificial, Comisión Europea, 18 de diciembre de 2018 (https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence), se indica lo siguiente acerca de la lealtad de los perfilados: *"Las actividades de perfilados no se pueden llevar a cabo de forma desleal ni generar discriminación, por ejemplo al denegar a las personas el acceso a oportunidades de empleo o dirigirse a ellas con productos demasiado arriesgados o costosos o que se produzca que se ofrezcan a ciertos clientes productos menos atractivos que a otros"*.

22. Guía de Perfilados del GT29, sección B.6 (pág. 16).

sería aquel en el que se tratan datos obtenidos de fuentes externas a las de la compañía que lleva a cabo la acción de perfilado[23].

4.2. Informar sobre el perfilado

La información es el deber pendular de la protección de datos por excelencia. De ahí que todo tratamiento de datos, incluyendo el perfilado, deba ser informado. Esta obligación implica que las compañías que llevan a cabo perfilados deben informar de dicho tratamiento con claridad y trasparencia (i. e., incluyendo expresiones que permitan a los usuarios tener expectativas razonables de que se va a generar un perfil). Para dar cumplimiento a este principio, las compañías (tal y como recomienda la AEPD) tienen la opción de poner a disposición de los clientes la información señalada por la normativa, en particular en el art. 11 de la LOPD y en los arts. 13 y 14 del RGPD, a través de dos capas informativas. La primera capa incluiría los puntos esenciales del tratamiento, mientras que la segunda capa facilitaría la información completa sobre el tratamiento de los datos.

En relación con las particularidades de dicho deber en el caso de que se realicen perfilados, la LOPD señala que la existencia de perfilados ha de incluirse en la primera capa[24]. Además, en una segunda capa, las compañías deben a) especificar[25] las consecuencias del perfilado (p. ej., la adopción de una decisión sobre la base del perfil generado) y b) detallar el nivel de dicho perfilado (p. ej., si se analizan solo los productos y servicios contratados o si también se tienen en cuenta los movimientos de las cuentas bancarias)[26].

23. Informe 0195/2017 de la AEPD, sección V: *"La primera consecuencia de lo antedicho es que debería excluirse de la aplicación del artículo 6.1 f) del Reglamento general de protección de datos los supuestos en que la entidad acudiera para la realización del perfilado a fuentes distintas de las que se derivasen de la relación del cliente con la entidad. De este modo, a juicio de esta Agencia, cualquier perfilado de los clientes que se llevase a cabo como consecuencia de enriquecer los datos de que dispone la entidad en virtud de su relación con el cliente con información procedente de otras fuentes requeriría o bien la solicitud del producto o servicio por el interesado, conforme ya se ha indicado, o bien que el mismo preste su consentimiento para el tratamiento"*. A su vez, el Informe del Gabinete Jurídico de la AEPD núm. 173/2018 (el *"Informe 173/2018"*) (https://www.aepd.es/media/informes/2018-0173-comunicaciones-comerciales.pdf) (sección IV) señala lo siguiente: *"[...] Sin embargo, esto no quiere decir que los responsables del tratamiento puedan remitirse al artículo 7, letra f), como fundamento jurídico para supervisar de manera indebida las actividades en línea y fuera de línea de sus clientes, combinar enormes cantidades de datos sobre ellos, provenientes de diferentes fuentes, que fueran inicialmente recopilados en otros contextos y con fines diferentes, y crear –y, por ejemplo, con la intermediación de corredores de datos, también comerciar con ellos– perfiles complejos de las personalidades y preferencias de los clientes sin su conocimiento, sin un mecanismo viable de oposición, por no mencionar la ausencia de un consentimiento informado [...]"*.

24. Artículo 11.2 de la LOPD en relación con los arts. 13 y 14 del RGPD.

25. Considerando 60 del RGPD.

26. Informe 0195/2017 de la AEPD, sección VII: *"Deberá detallarse de forma más minuciosa el tratamiento que va a llevarse a cabo, y particularmente, el hecho de que los datos transaccionales van a ser empleados para la elaboración de perfiles"*.

4.3. Otorgar un derecho de oposición específico

En el caso de que los perfilados se basen en el interés legítimo de las compañías (y no en el consentimiento de los clientes), se debe otorgar –de forma incondicional[27]– a los afectados un derecho de oposición de forma explícita[28], que ha de ser presentado al margen de cualquier otra información, para que los afectados puedan oponerse a que sus datos sean utilizados para elaborar perfiles con fines de *marketing*. Dicho derecho de oposición debe ser facilitado en el momento de la recogida[29] de los datos, en todo caso, y –posteriormente– en cualquier momento y sin coste alguno[30] . De acuerdo con los criterios de la AEPD, dicho derecho de oposición debería otorgarse mediante una casilla no premarcada (acompañada de una leyenda en la que se indique, por ejemplo, *"No deseo que se cree un perfil"*) que se incluya en el formulario en el que se van a recabar los datos. Es decir, el usuario tiene que conocer claramente que tiene un derecho a oponerse a que realicen perfilados sobre él con fines de *marketing*.

4.4. Otras particularidades que se aplican a los perfilados

Además de los dos *"pilares esenciales"* de las obligaciones impuestas por el RGPD para realizar perfilados con fines de *marketing* (i. e., comprobar que existe una base jurídica, informar acerca del perfilado y, si el perfilado se basa en la existencia de un interés legítimo, otorgar un derecho de oposición), existen otras garantías del RGPD que operan cuando se llevan a cabo perfilados, tal y como se detalla seguidamente:

• Derechos de los afectados sobre los perfiles que se han elaborado sobre ellos. El RGPD otorga, entre otros, el derecho a los afectados a acceder y a rectificar los datos personales que las compañías tratan sobre ellos y a ejercitar el derecho de portabilidad. Con frecuencia las compañías se plantean si el ámbito de aplicación de estos derechos se extiende a los perfiles que se han generado sobre los usuarios. En relación con los derechos de acceso y de rectificación, dichos derechos cubren el acceso a los datos tratados por el responsable para la elaboración de perfiles (los *"datos de entrada"*), así como a los datos de salida (el perfil y los detalles sobre los segmentos a los que se ha asignado al interesado o la puntuación que se le ha otorgado)[32]. Contrariamente, el derecho de portabilidad[33] no se

28. Art. 21.2 del RGPD.
29. Art. 21.4 del RGPD.
30. Art. 12.2. del RGPD.
31. Considerando 70 del RGPD.
32. En los arts. 15 a 22 del RGPD se establecen los derechos que el RGPD otorga a los interesados: acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad y derecho a no ser objeto de decisiones basadas únicamente en decisiones automatizadas que produzcan efectos jurídicos en los interesados o que le afecten significativamente de modo similar.
33. Guía de Perfilados del GT29 (pág. 19).

extendería a los datos del perfil creado. En el caso del derecho de rectificación, cabe señalar que el art. 16 del RGPD otorga además a los interesados el derecho a poder realizar una declaración complementaria[34] respecto de su perfil.

• Implementación de garantías para que los perfiles sean exactos y conservados durante un periodo de tiempo limitado. Las compañías deben asegurarse de que han establecido medidas sólidas[35] para verificar y garantizar que los perfiles son precisos y están actualizados. Además, es importante señalar que los perfilados (como el resto de datos) no deben ser conservados por las compañías de forma indefinida[36]. Por ello, se deben implementar procedimientos para que los perfiles solo sean conservados durante periodos de tiempo determinados y breves, atendiendo –especialmente– al grado de intromisión del perfilado.

• Evaluaciones de impacto y nombramiento de un delegado de protección de datos (*el data protection officer* o, por sus siglas en inglés, el *"DPO"*). La elaboración de perfiles conllevaría la obligación, como regla general, de realizar una evaluación de impacto (*privacy impact assessment*, por sus siglas en inglés, *"PIA"*) de acuerdo con las directrices publicadas por la AEPD[38]. Además de realizar una PIA, las compañías que elaboren perfilados deberían nombrar a un DPO[39] , cuyo nombramiento deberá ser comunicado al registro de DPO de la AEPD.

34. En el Anexo a las Directrices sobre el derecho de portabilidad del GT29, adoptado el 13 de diciembre de 2016 y revisadas y adoptadas el 5 de abril de 2017 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233), se incluye la siguiente definición sobre el derecho de portabilidad (pregunta núm. 1): *"La portabilidad de los datos proporciona a los interesados la capacidad de obtener y reutilizar sus datos para sus propios fines y en diferentes servicios. Este derecho mejora su capacidad para mover, copiar o transferir datos personales fácilmente de un entorno informático a otro, sin impedimentos"*.

35. Guía de Perfilados del GT29 (pág. 20).

36. El art. 5.1. d) establece un principio general de que los datos deben mantenerse exactos.

37. El art. 28 de la LOPD indica que los responsables y los encargados deberán valorar si procede realizar una PIA, entre otras circunstancias, *"cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o su comportamiento, su solvencia financiera, su localización o sus movimiento"*.

38. La AEPD publicó una guía sobre qué es una evaluación de impacto y cómo debe llevarse a cabo: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf.

39. El art. 34 de la LOPD señala que se deberá nombrar a un delegado de protección de datos en el caso de que:

a) *"Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio"* y/o

b) *"Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos"*.

5. PERFILADOS O DECISIONES AUTOMATIZADAS CON EFECTOS JURÍDICOS EN EL INTERESADO

La norma[40] establece una prohibición general con el fin de que las compañías no implementen mecanismos en los que sea un algoritmo únicamente (sin intervención humana) el que tome una decisión o elabore un perfil, y que dichas decisiones o perfilados tengan efectos jurídicos en los usuarios o que *"les afecte significativamente de modo similar"*. No obstante, dicha regla general acepta excepciones (como que el afectado otorgue su consentimiento expreso) siempre que se implementen garantías adicionales establecidas en el RGPD.

En este sentido, cabe preguntarse si en el sector del *marketing* se toman decisiones automatizadas o se elaboran perfiles basados únicamente en tratamientos automatizadas que a) *"tengan efectos jurídicos"* en los usuarios o b) que les *"afecten significativamente de modo similar"*. Respecto del primer supuesto, resulta difícil –al menos actualmente– pensar que pueda ser de aplicación en el sector de la publicidad[41]. No obstante, el GT29 llama la atención sobre la posibilidad de que –aunque excepcionalmente– ciertas decisiones o elaboraciones de perfiles automatizadas (sin intervención humana) puedan tener *"efectos significativamente similares"* en las personas. Para discernir si existe dicho riesgo, el GT29 indica que se han de tener en cuenta los siguientes factores[42]: a) el nivel de intrusismo del proceso de elaboración de perfiles, incluido el seguimiento de las personas en diferentes sitios web, dispositivos y servicios; b) las expectativas y deseos de las personas afectadas; c) la forma en que se presenta el anuncio; o d) el uso de conocimientos sobre las vulnerabilidades de los interesados.

En relación con ello, el GT29 advierte de que un tratamiento que pueda tener poco impacto sobre las personas en general podría tener un efecto significativo en determinados grupos de la sociedad, como grupos minoritarios, adultos vulnerables[43] o niños[44]. Es más, en el caso de estos últimos, el GT29 hace hincapié en que pueden ser especialmente susceptibles e influenciables en el entorno en línea, particularmente respecto de la publicidad compor-

40. El art. 22 del RGPD.

41. En la Sección 4.B) de la Guía de Perfilados del GT29 (pág. 24), se señala que las decisiones de presentar publicidad dirigida basada en la elaboración de perfiles no tendrá un efecto significativamente similar en las personas: *"Por ejemplo, un anuncio de una popular tienda de moda en línea basado en un sencillo perfil demográfico «mujeres de la región de Bruselas con edades comprendidas entre los 25 y los 35 años que probablemente estén interesadas en la moda y en determinadas prendas de vestir"*.

42. Guía de Perfilados del GT29 (págs. 23 y 24).

43. La Guía de Perfilados del GT29, sección IV. B (pág. 24) indica que en el siguiente tratamiento podría tener un efecto significativo en el siguiente escenario: *"Por ejemplo, alguien que tenga o que pueda tener dificultades financieras y que reciba anuncios de préstamos a tipos de interés elevados podría suscribirse a estas ofertas y posiblemente aumentar su deuda"*.

44. A efectos de la LOPD un *"niño"* es una persona menor de catorce años (art. 7 de la LOPD).

tamental[45]. Por ello, el GT29 concluye, a este respecto, que las compañías deberán abstenerse en general de elaborar perfiles sobre los niños con fines de publicitarios[46].

6. ENVÍO DE COMUNICACIONES COMERCIALES PERSONALIZADAS POR MEDIOS ELECTRÓNICOS

Si los perfiles elaborados, además, se utilizan con el fin de enviar comunicaciones comerciales por medios electrónicos (p. ej., e-mails o sms) ajustadas al perfil de los usuarios (i. e., publicidad comportamental), las compañías deberían –además– cumplir con la LSSI (y, en particular, con el art. 21). Dicha norma constituye una norma especial[47], por lo que debe acudirse a ella y –de forma complementaria al RGPD– para resolver las cuestiones relativas al envío de comunicaciones comerciales.

La LSSI, como regla general, exige recabar el consentimiento expreso (*opt-in*) de los usuarios para poder enviar comunicaciones comerciales. No obstante, si se cumplen todos los requisitos expuestos en esta sección, no será necesario recabar el consentimiento expreso de los usuarios. En dichos supuestos, dado que existiría un interés legítimo, tan solo sería necesario informar sobre el sector de actividad específico sobre el que se van a remitir comunicaciones comerciales y ofrecer un derecho de oposición (opt-out) a la recepción de *marketing* en el momento de la recogida de los datos y en cada comunicación comercial que se realice con posterioridad. La forma más apropiada de otorgar dicho derecho sería incluyendo una casilla no premarcada en el formulario de recogida de los datos con el fin de que el usuario tenga la oportunidad de marcarla si no desea recibir comunicaciones comerciales.

A continuación, se detallan las premisas que se deben cumplir para que el envío de comunicaciones comerciales pueda basarse en el interés legítimo de las compañías:

• Que el receptor sea cliente de la entidad. El destinatario del *marketing* debería ser cliente de la entidad. Por lo tanto, si el destinatario ya hubiera cesado la relación negocial o contractual con la compañía, el envío de *marketing* exigiría un consentimiento expreso.

45. La Guía de Perfilados del GT29, sección V (pág. 32), señala que: *"Por ejemplo, en los juegos en línea, la elaboración de perfiles puede utilizarse para dirigirse a jugadores que según el algoritmo sean más propensos a gastar dinero en los juegos, así como para ofrecer más publicidad personalizada. La edad y la madurez de los niños pueden afectar a su capacidad para entender la motivación que hay detrás de este tipo de mercadotecnia o sus consecuencias"*.

46. Considerandos 38 y 75 del RGPD.

47. Vid. Considerandos 95 y 173 del RGPD, así como los Informes del Gabinete Jurídico de la AEPD núm. 173/2018, núm. 164/2018 https://www.aepd.es/media/informes/2018-0164-comunicaciones-comerciales-por-medios-electronicos.pdf y núm. 195/2017.

• El *marketing* debe ser sobre productos y/o servicios del remitente. El interés legítimo para el envío de publicidad solo se aplicaría si se envía *marketing* sobre la entidad con la que el cliente ha contratado los productos y servicios. Contrariamente, si una entidad desease enviar comunicaciones comerciales sobre productos y servicios de otras sociedades del grupo o terceros (partners con los que se mantengan acuerdos comerciales) necesitaría, como regla general, recabar el consentimiento expreso (*opt-in*) de los clientes.

• El *marketing* debería promocionar solo productos y servicios similares a los ya contratados. El término *"similar"* ha sido interpretado por la AEPD de forma restrictiva. A modo de ejemplo, la AEPD puntualizó que si un cliente ha contratado productos financieros, no tendría *"una expectativa razonable"* de que las ofertas sobre seguros sean *"similares"* a los productos financieros que ya hubiera contratado[48]. Por ello, si una entidad quisiese enviar *marketing* sobre seguros a un cliente que hubiese contratado otro tipo de productos financieros, debería recabar su consentimiento expreso.

• El perfilado previo en el que se base el remitente para personalizar las comunicaciones debería ser sencillo. Si el perfilado no es muy complejo (i. e., se basa solo en datos obtenidos del cliente y no de terceras fuentes), la AEPD ha considerado que no sería necesario recabar el consentimiento expreso de los clientes.

En el contexto de los perfilados para el envío de *marketing* personalizado, una cuestión que genera muchas inquietudes es si sería necesario dar un derecho de oposición diferenciado para que los usuarios se puedan oponer, por un lado, a la realización de perfilados y, por otro, al envío de comunicaciones comerciales. Ello, además, implicaría que se deberían poner a disposición de los usuarios dos casillas (distintas) no premarcadas con el fin de que los usuarios se pudiesen oponer solo a ser objeto de perfilados con la intención de seguir recibiendo *marketing* (no personalizado). Para aclarar esta cuestión, se podría acudir al único pronunciamiento de la AEPD –al respecto– en el que matizó que *"debería ser posible que el interesado pueda oponerse a este tratamiento [el perfilado] aun cuando no se haya opuesto a recibir otro tipo de ofertas de la entidad"*[49]. No obstante, sería razonable defender que, en los casos en los que los perfilados solo se lleven

48. En el Informe 195/2017, sección IV, se señala lo siguiente: *"De este modo, no cabría duda de que sería posible la oferta de otros productos relacionados con el ahorro o el crédito, pero sería necesario establecer ya un primer análisis restrictivo cuando la acción de publicidad se refiriese a servicios que pudieran encajar en el concepto amplio de "servicios financieros", como sucedería en el caso de los seguros. Finalmente, la ponderación a la que estamos haciendo referencia no operaría cuando se tratase de publicidad u oferta de productos o servicios que no guardan relación con la actividad de la entidad, sino que la acción publicitaria deriva de la existencia de un determinado acuerdo con el anunciante al que se refiriese la publicidad o afectase a productos o servicios no financieros pero ofrecidos por empresas del grupo o participadas por la entidad"*.

49. AEPD: Informe 195/2017, sección V.

a cabo con el fin de enviar *marketing* personalizado, solo sería necesario otorgar un único derecho de oposición a los clientes (aunque esta opción aún no ha sido validada, de forma expresa, por la AEPD). En cualquier caso, además de otorgar el derecho de oposición, habría que otorgar al cliente información detallada sobre dicho perfilado (p. ej., si se analizan solo los productos y servicios contratados o si también se tienen en cuenta los movimientos de las cuentas bancarias).

Por otro lado, los arts. 23.3 y 23.4 de la LOPD exigen que, antes de realizar envíos de *marketing* basados en el interés legítimo de las compañías (y no en el consentimiento[50]), se lleve a cabo una comprobación[51] sobre si dichos usuarios constan en los ficheros comunes de exclusión publicitaria (i. e., las llamadas *"listas Robinson"*[52]). Además, las compañías deberán informar[53] acerca de la existencia de dichos ficheros de exclusión publicitaria cuando un interesado manifieste su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales.

7. PERFILADOS REALIZADOS A TRAVÉS DE *COOKIES* O MECANISMOS DE OBTENCIÓN DE LA HUELLA DIGITAL

La monitorización (i. e., el seguimiento) de la navegación de los usuarios en los sitios web de las compañías es una práctica muy extendida. Estas prácticas permiten a las empresas recopilar todos los hábitos de navegación y, entre otras cosas, perfilar a los usuarios. Las técnicas de seguimiento de la navegación en sitios web más populares (hasta la fecha) son las *cookies*, que son ficheros que se almacenan en el ordenador del usuario que crea el propio sitio web del proveedor de servicios de la sociedad de la información. Sin embargo, esta tecnología ha sido superada por otras técnicas de seguimiento de los usuarios más avanzadas que obtienen la huella digital de los dispositivos de los usuarios.

Estas técnicas, conocidas como *fingerprinting*[54] (p. ej., *canvas fingerprinting, webRTC* o audio *fingerprint*), recopilan información específica del navegador web

50. El art. 23.4 de la LOPD dispone que *"No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla"*.

51. El art. 23.4 de la LOPD señala que *"A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente"*.

52. AEPD: Informe 173/2018.

53. Art. 23.3 de la LOPD.

54. AEPD: Estudio fingerprinting o huella digital del dispositivo (el *"Estudio sobre Fingerprinting"*) (https://www.aepd.es/media/estudios/estudio-fingerprinting-huella-digital.pdf). En la pág. 4 de este estudio, la AEPD define el fingerprinting como *"Una recopilación sistemática de información sobre un determinado dispositivo remoto con el objetivo de singularizarlo y, de esa forma, poder hacer un seguimiento de la actividad del usuario con el fin de perfilarlo. [...] Dicho en términos más comprensibles, la huella digital del dispositivo es un conjunto de datos extraídos del terminal del usuario que permiten individualizar de forma unívoca dicho terminal"*.

y/o dispositivo de navegación del usuario. Dicha combinación de información es la que permite construir un identificador para reconocer al usuario de forma unívoca[55].

La utilización de este tipo de tecnologías para obtener datos personales se regula por la LSSI (como ley especial) y, de forma complementaria, por la normativa de protección de datos. Además, el borrador de Reglamento de e-Privacy identifica de forma expresa este tipo de tecnologías y establece una regulación extensa sobre su uso[56]. La inclusión de *cookies* o tecnologías de obtención de la huella digital (propias o de terceros) con el fin de llevar a cabo perfilados exige que los titulares de los sitios web recaben el consentimiento[57] informado de los usuarios de acuerdo con los requisitos señalados en el art. 22.2 de la LSSI y la interpretación de él que publicó la AEPD en la guía para el uso de *cookies*[58].

Dicha publicación será actualizada en un futuro próximo, aunque la AEPD ya adelantó unas pautas sobre los cambios que ha introducido el RGPD en el marco del uso de *cookies* y tecnologías similares y obtener el consentimiento de los usuarios. Sin perjuicio de lo anterior, el sistema de incluir dos capas para informar del uso de *cookies* y tecnologías similares sigue siendo el mismo. Es decir, para poder utilizar estas tecnologías se debería incluir un primer banner (o *pop-up*) que debería redireccionar a una segunda capa informativa (i. e., la política completa de *cookies*).

Sin perjuicio de lo anterior, la AEPD –en las Pautas sobre *Cookies*– ha recomendado que se refuercen los mecanismos para obtener el consentimiento[60] y la información que hay que facilitar a los usuarios[61]. En relación con el deber de informar en el contexto de los perfilados, la AEPD ha puntualizado que dicho

55. La AEPD indica en su Estudio sobre Fingerprinting, pág. 5, que *"Las técnicas más avanzadas permiten registrar los movimientos que realiza el usuario a través de la página web con el ratón, examinando en que partes de la pantalla [el usuario] se detiene por más tiempo"*.

56. Vid. Considerando 20 del proyecto de Reglamento de e-Privacy.

57. Respecto a la obtención del consentimiento, cabe señalar que hasta la fecha se ha aceptado que el consentimiento fuese inequívoco (i. e., una acción positiva por parte del usuario, por ejemplo, al *"continuar navegando"* para aceptar el uso de las *cookies*). No obstante, sería necesario obtener el consentimiento expreso para recabar datos que requieren, de acuerdo con el RGPD, un consentimiento expreso del titular del dato (p. ej., datos de salud).

58. AEPD: Guía sobre el uso de las *cookies* (http://www.interior.gob.es/documents/10180/13073/Guia_*Cookies*.pdf/7c72c988-1e55-42b5-aeee-f7c46a319903).

59. Rubí Navarrete, Jesús (AEDP): *"El RGPD y la ley de servicios de la sociedad de la información y de comercio electrónico"* (las *"Pautas sobre Cookies"*), en 10.ª Sesión Anual Abierta de la AEPD (https://www.aepd.es/agencia/transparencia/jornadas/common/10-sesion/4-jesus-rubi.pdf).

60. La AEPD, en las Pautas sobre *Cookies*, considera que para otorgar el consentimiento sobre el uso de las *cookies* se deberían habilitar tres botones: a) uno para aceptar todas las *cookies*, b) otro para configurarlas (panel de configuración de *cookies*) y c) otro para rechazarlas de forma granular (es decir, un rechazo de *cookies* por finalidades). En relación con la fórmula de *"seguir navegando"* para consentir el uso de las *cookies*, la AEPD considera que podría seguir siendo válida si se refuerza la toma de decisiones sobre las *cookies*. En cualquier caso, la inclusión de un botón para aceptar las *cookies* y la opción de *"seguir navegando"* son incompatibles, ya que inducen al usuarios a error en la forma en la que manifiestan su consentimiento.

61. En el banner de *cookies* se debería informar acerca de a) la identidad del responsable del tratamiento, b) la finalidad de las *cookies* (i. e., publicitarias, analíticas, de elaboración de perfiles) y c) del tipo de datos (p. ej., monitorización de hábitos de navegación y elaboración de perfiles).

tratamiento debería ser informado en el banner de *cookies* (i. e., en la primera capa). En este sentido, se deberían incluir expresiones que indiquen claramente que se monitorizan los hábitos de navegación y que la finalidad de las *cookies* o de las tecnologías similares es elaborar perfiles[62], excluyendo cualquier tipo de información que induzca a confusión o desvirtúe la claridad del mensaje (p. ej., *"usamos cookies para personalizar su contenido y crear una mejor experiencia para usted"* o *"para mejorar su navegación"* o similares). Asimismo, las compañías deben facilitar mecanismos (como, por ejemplo, paneles de configuración de *cookies* o tecnologías similares) que permitan a los usuarios rechazar las *cookies* de forma granular o por finalidades. Ello implicaría que los prestadores de servicios de los sitios web deberían permitir que los usuarios pudiesen desactivar –de forma conjunta– todas las *cookies* o tecnologías similares que compartan una misma finalidad (p. ej., utilizadas con fines de perfilado).

8. USO DE DATOS ANONIMIZADOS PARA MEJORAR LAS HERRAMIENTAS APLICADAS DE IA

Las herramientas de IA y, en particular, los algoritmos de aprendizaje automático, para ser más independientes y más exactos, necesitan ser *"entrenados"* y enriquecerse de datos personales. Por ello, muchas compañías nutren sus algoritmos de datos anonimizados o seudonimizados. No obstante, dicha práctica ha de llevarse a cabo de acuerdo con la normativa de protección de datos.

Para analizar con rigor este tema, hay que aclarar que los datos anonimizados no tienen el mismo régimen que los datos seudonimizados. Los datos anonimizados son aquella información que no permite reidentificar a la persona física a la que pertenecen (p. ej., las chicas de 30 a 35 años acceden a las redes sociales desde sus *smartphones* con mayor frecuencia que desde sus ordenadores portátiles). Sin embargo, los datos seudonimizados[63] son aquellos que sí permiten reconocer a la persona física a la que pertenecen (p. ej., el cliente 495 suele acceder a las redes sociales desde su smartphone, y con dicho código se podría llegar a una identifica-

62. AEPD: Pautas sobre *Cookies*.

63. El RGPD define en su art. 4.5. la seudonimización como: *"el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"*.

64. El Informe 195/2017 de la AEPD, sección VIII, señala lo siguiente respecto a los procesos de anonimización y de pseudonimización: *"[...] tanto la anonimización como la seudonimización de los datos personales llevarán aparejada la existencia de dos tratamientos sucesivos: el que supone la propia anonimización o seudonimización a partir de los datos personales de que dispone el responsable y el que se lleve a cabo posteriormente con los datos ya anonimizados o seudonimizados.* ***La diferencia entre ambos supuestos estribará en el hecho de que mientras la normativa de protección de datos no será de aplicación a este segundo tratamiento si los datos han sido anonimizados, sí resultará aplicable en caso de que se haya producido únicamente una seudonimización".***

ción). Esta distinción es importante, ya que el RGPD establece que a la información agregada o anonimizada no le es de aplicación la normativa de protección de datos, mientras que a la seudonimizada, sí. No obstante, ello no quiere decir que exista un *"cheque en blanco"* para anonimizar los datos y tratarlos con los fines que una compañía desee. Al respecto, la AEPD ha puntualizado que la anonimización es un tratamiento en sí mismo[64]. Ello implica que las compañías necesitarían una base jurídica para anonimizar dichos datos e informar a los afectados sobre dicho tratamiento en todo caso[65].

Además, la AEPD publicó una guía[66] sobre los procesos de anonimización en la que se concluía que, dada la rápida evolución de la tecnología, hay que tener en cuenta que los procesos realizados pueden no ser definitivos e irreversibles. Por ello, la AEPD recomienda que los procesos de anonimización sean revisados periódicamente y se evalúen (incluso realizando las PIA) los posibles nuevos riesgos que puedan surgir como consecuencia de diferentes factores, riesgo residual de datos anonimizados, nuevas fuentes de datos a cruzar, nuevas tecnologías, etc.[67]

Por lo tanto, partiendo de la asunción de que el proceso de anonimización no puede asegurar la imposibilidad de reidentificación de las personas en términos absolutos, se deben implementar las garantías jurídicas necesarias para preservar los derechos de los interesados[68]. En este sentido, algunos de los aspectos que deben tener en cuenta las compañías, tal y como recomienda la AEPD,

65. El Informe195/2017 de la AEPD, sección VIII, señala lo siguiente respecto al deber de informar en los procesos de anonimización y de pseudonimización: "En todo caso, como se ha indicado para los supuestos anteriormente indicados, será preciso informar a los interesados acerca de los tratamientos que van a tener lugar y garantizar el adecuado ejercicio por aquéllos de su derecho de oposición, al operar éste, según el artículo 21 del reglamento, en los supuestos en que el tratamiento se funde en la regla del equilibrio de derechos e intereses prevista en el artículo 6.1 f) del reglamento".

66. AEPD: Orientaciones y garantías en los procedimientos de anonimización de datos personales (la *"Guía de Anonimización"*) (https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf).

67. La AEPD en su Código de Big Data, sección IV.4. (pág. 30) dice lo siguiente: *"Se deben establecer medidas adicionales de seguridad en todos los elementos que intervienen en el proceso de la anonimización, como auditorías periódicas de las fuentes de información, de los canales de transmisión de la información, de las localizaciones físicas de las fuentes de información, etc., aplicando los estándares, sellos y buenas prácticas en seguridad y privacidad de la información. Este marco integral debería incluir un procedimiento de detección y notificación de posibles brechas de privacidad que pudieran surgir, como casos de re-identificación"*.

68. En la Guía de Anonimización, sección 8 (pág. 24), la AEPD indica que *"No es posible considerar que los procesos de anonimización garanticen al 100% la no reidentificación de las personas, por lo que será necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen. Es recomendable la adopción de códigos de conducta en las organizaciones para facilitar la aplicación de la legislación vigente, así como la obtención de certificaciones, sellos o etiquetas que permitan demostrar a terceros su adecuado cumplimiento, de forma que la privacidad se pueda convertir en valor referencial de las mismas"*.

son los siguientes[69]: a) la suscripción de acuerdos de confidencialidad y b) un contrato entre el responsable del tratamiento originario y el destinatario de la información anonimizada.

9. CONCLUSIONES

Como ha quedado reflejado en este artículo, una de las ventajas más destacables de las técnicas aplicadas de IA en el ámbito de la publicidad es que éstas permiten que las compañías puedan conocer el perfil exacto de los usuarios, con el fin de enviarles comunicaciones comerciales ajustadas a sus preferencias.

No obstante, dicha actividad debe llevarse a cabo cumpliendo con la normativa aplicable en materia de protección de datos y, en el caso de que se envíen comunicaciones comerciales por medios electrónicos o los datos personales se recaben a través de *cookies* o tecnologías similares, las compañías deben cumplir –también– con la normativa de servicios de la sociedad la información.

La elaboración de perfiles, si no es compleja, puede basarse en el interés legítimo de las empresas (i.e., sin necesidad de recabar el consentimiento de los usuarios). No obstante, en dichos casos, las compañías deben informar sobre la elaboración de perfiles y otorgar a los usuarios un derecho de oposición específico sobre dicha actividad.

69. Guía de Anonimización de la AEPD, sección 5 (págs. 21 y 22).

ISSN: 1579-3494

FUNDACIÓN CEFi
Centro de Estudios para el Fomento de la Investigación