Profiling, publicidad comportamental *online* y aplicaciones móviles

PID_00248577

Francisco Pérez Bes
Carlos Galán Cordero

Universitat Oberta de Catalunya

Índice

Introducción

Por todos es conocido que el tratamiento de grandes volúmenes de datos constituye un activo de inmenso valor estratégico, social y económico en el que, por diferentes razones, se encuentran interesados gobiernos, empresas, profesionales y ciudadanos. Las limitaciones técnicas que unos pocos años atrás ralentizaban la masiva utilización de las tecnologías de la información (capacidad de almacenamiento, potencia de cálculo y velocidad de transmisión, esencialmente) han desaparecido en la práctica, haciendo que el tratamiento y la recopilación masiva de datos (*big data analytics*), desde todo tipo de dispositivos y fuentes (*Internet of things*), constituya al tiempo nuestro presente y nuestro futuro más inmediato.

Incrementar la potencia de cálculo de los ordenadores, su capacidad de almacenamiento y la velocidad con la que pueden compartir información con miles o millones de otros elementos ha hecho aflorar posibilidades hasta hace poco impensables. El análisis estadístico (como base sobre la que se asienta el análisis predictivo) que se apoya en una ingente cantidad de datos (lo que, como más adelante veremos, constituye la esencia del *profiling*) es ya una realidad. La posibilidad de tratar datos desde dispositivos que podemos transportar fácilmente o, incluso, implantarnos nos permite tener acceso a una ilimitada gama de servicios a través de internet, siendo muestras de que una nueva realidad preside nuestras vidas.

Sin embargo, al haber desaparecido las barreras o limitaciones tecnológicas de antaño, la problemática derivada del tratamiento racional de los datos personales y de la protección de los derechos y las libertades de los individuos se incrementa, al tiempo que lo hacen aquellos tratamientos.

El *big data* ha hecho posible la elaboración de perfiles de usuarios de internet; esto es, la posibilidad de construir grupos de individuos (cientos, miles o millones) que comparten unas características comunes y a los que, en consecuencia, y en base a esas circunstancias en común, cabría aplicar un mismo tratamiento. Aunque esta realidad pudiera ser admisible en determinados supuestos (por ejemplo, en el tratamiento de enfermedades o en su prevención), no es menos cierto que la adscripción a un grupo, en base a un mero análisis masivo de datos, comporta ciertos peligros entre los cuales la injusticia o la discriminación son, por citar solo algunos, dos de los más significativos. A modo de ejemplo, dicho análisis masivo podría provocar que una determinada entidad tomara alguna medida que perjudicara a un individuo concreto, al formar este parte de un grupo con el que compartiera alguna similitud en otros aspectos.

Nuestra sociedad se ha vuelto tan dependiente de los medios tecnológicos que ya no es posible dar marcha atrás. Pasamos muchas horas de nuestra vida conectados a dispositivos tecnológicos (ordenadores portátiles, tabletas o móviles inteligentes) que constituyen ya una parte inseparable de nosotros mismos. Con ellos trabajamos, compramos, nos divertimos…, y en esa interacción hay siempre muchas organizaciones que, incesantemente y por el mero hecho de conectarnos a la red, tienen acceso a nuestros datos. Las administraciones públicas, los comercios *online*, las compañías operadoras de comunicaciones, los prestadores de servicios de la sociedad de la información, el sistema sanitario, financiero, etc., son todos ellos buenos ejemplos de cómo nuestros datos personales se distribuyen a través de una red con fines comerciales, donde sus destinatarios persiguen incesantemente saber más y más acerca de nosotros. Porque cuanto más sepan de nuestras costumbres, nuestros hábitos, nuestros gustos, en mejores condiciones estarán de ofrecernos productos o servicios que, presumiblemente, recibiremos con agrado. Es lo que se ha llamado *publicidad comportamental online* (en inglés, *online behavioural advertising*).

Esta interacción tecnológica, hasta hace pocos años materializada en los ordenadores personales, se ha vuelto cada vez más portátil. Hoy en día, los teléfonos móviles inteligentes, junto con los *wearables* y sus aplicaciones móviles, constituyen ya el primer punto de contacto entre nuestra persona y el mundo exterior. El acceso a internet y a la miríada de servicios que ofrece, las comunicaciones vocales o textuales, la mensajería instantánea, la compartición en tiempo real de fotos, vídeos o locuciones, o la inmediatez en las reuniones que ocupan a personas ubicadas en diferentes zonas del globo terráqueo, son también parte de la realidad y nos convierten en seres dependientes de estos pequeños dispositivos, al tiempo que incrementamos los activos de datos de los promotores de tales nuevos servicios. Quien tenga acceso a los datos de nuestro teléfono móvil sabrá casi más sobre nosotros que nosotros mismos acerca de nuestros hábitos de vida (agenda y salud), de nuestras amistades (contactos, fotos y vídeos), de nuestras preferencias (historial de navegación), de nuestra ubicación y movimientos (GPS), de nuestras características físicas (biometría), de nuestra creencias políticas o ideológicas

Y aquí estamos. En estos primeros años del siglo XXI, nos encontramos, de este modo, con la necesidad de tratar adecuadamente y de forma simultánea las problemáticas tradicionales y los nuevos retos derivados de la nueva realidad.

Así las cosas, está claro que el derecho no puede quedar al margen de ese tratamiento.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por

(1)Conocida como Propuesta de Reglamento e-Privacy.

el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD en adelante), junto con el resto de normas que sirven de base jurídica al presente trabajo, muy especialmente la Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas[1]) y la Ley 34/2002[2], de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, entre otras[3], determinan conjuntamente los elementos esenciales que configuran el tratamiento de datos personales, y sus disposiciones resultan especialmente aplicables a dos figuras esenciales, el *responsable del tratamiento* y el *encargado del tratamiento*.

(2)Aunque a la fecha de redacción del presente trabajo se encuentra todavía en fase de anteproyecto, también se hará referencia a la futura nueva Ley Orgánica de Protección de Datos, en la versión que se ha hecho pública.

(3)Como por ejemplo, la Guía de la comisión europea; COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018.

Dichas normas, y otras que se irán mencionando a lo largo de las siguientes páginas, constituyen la referencia obligada y resultan de plena aplicación a aquellas actividades que guardan relación con el tratamiento de información a través de lo que se ha dado en llamar *big data*, *profiling*, publicidad comportamental *online* y las aplicaciones móviles, sujetos todos ellos del presente módulo.

Se hace necesario, por tanto, que analicemos las citadas normativas desde la óptica de los nuevos riesgos derivados del *profiling*, la publicidad comportamental o las aplicaciones móviles.

Nuestro propósito, por consiguiente, es examinar la problemática derivada de los antedichos conceptos y analizar de qué manera están siendo abordados por las regulaciones europeas o nacionales que resultan aplicables.

En el presente módulo se ha prescindido tratar cuestiones generales de protección de datos que ya han sido debidamente tratadas en otros módulos y otras asignaturas.

1. *Profiling*

Se entiende por *profiling* o «elaboración de perfiles» cualquier forma de tratamiento automatizado de los datos personales de una multiplicidad de individuos que posibilite la creación de perfiles personales. Esto es, se trata de procedimientos para facilitar la agrupación de tales individuos en conjuntos o categorías con características comunes, al objeto de sistematizar el análisis de sus datos y deducir patrones de comportamiento de sus miembros o, incluso, predecir cuestiones relacionadas con sus intereses, su nivel adquisitivo, su trabajo, sus preferencias personales, su ubicación, etc.

1.1. Los riesgos del *profiling*

Lo que hace especialmente delicado al *profiling* es que, partiendo de un volumen muy grande de información personal que se trata y agrupa en conjuntos diferenciados, y mediante la aplicación de los algoritmos de análisis adecuados, puedan tomarse decisiones específicas para algunos de aquellos grupos que comparten características comunes y, en consecuencia, con trascendencia para los individuos que los conforman.

Parece lógico pensar que el tratamiento automatizado de grandes volúmenes de datos, *big data*, y la subsiguiente elaboración de perfiles pueden ayudar a tomar decisiones oportunas en ciertos contextos.

> Por ejemplo, una adecuada elaboración de perfiles a partir de grandes volúmenes de datos de individuos puede ayudar a la ciencia a determinar la probabilidad de impacto de una enfermedad en particular en una población concreta, tomando como base sus hábitos, comportamientos, etc.

No obstante, como veremos más adelante, la conjunción de ambos procedimientos puede implicar significativos riesgos para los titulares de los datos tratados y analizados, riesgos que pueden estar relacionados con el respeto a los derechos personalísimos a la intimidad, pero también con los perjuicios derivados de una decisión no adoptada en base a exclusivos condicionantes personales, sino por la mera pertenencia a un grupo con el que se comparten ciertos caracteres.

Uno de los riesgos más señalados por la doctrina lo constituye el peligro de discriminación (Garriga, 2015), toda vez que la realización de perfiles favorece la aparición de estereotipos sociales que, a la postre, pueden llegar a determinar tanto la atribución de privilegios o derechos como, por el contrario, una exclusión social (Lyon, 1984).

Referencias bibliográficas

Ana Garriga (2015). *Nuevos retos a la protección de datos*. Dykinson.

David Lyon (1984). *Surveillance Studies. An Overview*. Malden: Polity Press.

Las modernas técnicas informáticas de inmersión en el comportamiento de los individuos o en sus aptitudes profesionales son capaces de establecer correlaciones entre distintas características. El uso de aquellas, a juicio de Rigaux, guarda importantes semejanzas con el racismo (De Rigaux, 1990), lo que provoca la aparición de normas de conducta y tratamientos diferenciados para los distintos grupos que han podido formarse. El autor citado señala que tales previsiones desembocan habitualmente en discriminaciones porque:

> «[...] en la creencia de descubrir en el sujeto ciertos signos anunciadores de su comportamiento futuro, el perfil instaura una forma de determinismo incompatible con el atributo más preciado de la libertad, la elección de un futuro autodeterminado.»
>
> François De Rigaux, *op. cit.* En la publicación de Ana Garriga «Nuevos retos para la protección de datos personales».

Referencias bibliográficas

Françoise de Rigaux (1990). *La protection de la vie privée et des autres biens de la personalité*. Bruxelles: Bruyant.

Los efectos más perjudiciales de la elaboración de perfiles se dan cuando los individuos afectados, a los que se ha atribuido un determinado comportamiento, se incorporan a las llamadas «listas negras»[4] (morosos, sanciones administrativas, laborales o penales, negligencias, adscripción política o ideológica, indicios de peligrosidad basados en comportamientos públicos, conductas inadecuadas, salud, etc.).

(4)Véase el *Documento de trabajo* sobre *listas negras*, adoptado el 3 de octubre de 2002 por el Grupo de Trabajo sobre Protección de Datos de la Unión Europea: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_es.pdf>.

1.2. Respuestas

Como respuesta a estas problemáticas, el Comité de Ministros del Consejo de Europa adoptó el 23 de noviembre de 2010 la *Recomendación sobre la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal en el contexto de la creación de perfiles*. Esta recomendación señala las dos consecuencias más significativas de la realización de perfiles:

1) Posibilita la inclusión de las personas en categorías predeterminadas sin que tengan conocimiento de ello. Esto puede llevar consigo una problemática asociada consistente en falta de transparencia y falta de precisión en los algoritmos.

2) Posibilita la generación de nuevos datos personales, no proporcionados por el interesado originariamente.

Las resoluciones de la XXXV Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (2013), en relación con el *profiling*, fueron igualmente contundentes:

> «Reafirmando la Declaración de Uruguay de 2012 sobre Profiling, la XXXV Conferencia Internacional de Autoridades de Protección de Datos y Privacidad anima a todos los actores que hacen uso de *profiling*:
>
> **1)** A determinar claramente la necesidad de cada operación específica de *profiling* y de asegurar las garantías adecuadas antes del inicio de la misma.

2) A limitar, en consonancia con los principios de privacidad basada en el diseño, los supuestos y el volumen de datos recogidos hasta el nivel que resulte necesario en función de la finalidad lícita perseguida y para que, en su caso, los datos sean suficientemente puestos al día y exactos, para los fines previstos.

3) A asegurarse de que los perfiles y los algoritmos subyacentes están sujetos a validación continua, con el fin de permitir la mejora de los resultados y la reducción de los falsos positivos o falsos negativos.

4) A informar a la sociedad sobre las operaciones de *profiling*, en la mayor medida posible, incluyendo el modo en el que los perfiles son ensamblados y los fines para los que son utilizados, con el fin de asegurar que los individuos son capaces de mantener el control sobre sus propios datos personales en la mayor y más adecuada medida posible.

5) A garantizar que los afectados son informados de sus derechos de acceso y rectificación, en particular con respecto a las decisiones que tengan significativos efectos legales en las personas o que afecten a sus beneficios o a su estatus, así como que se provea de intervención humana cuando resulte adecuado, especialmente en la medida en la que el poder predictivo del *profiling* se incrementa debido a algoritmos cada vez más eficaces.

6) A garantizar que todas las operaciones de *profiling* están sujetas a una supervisión adecuada.»

En resumen, como así se ha dicho:

«Las previsiones sobre individuos basadas en datos masivos [*big data*] pueden ser utilizadas en la práctica para castigar a la gente por sus propensiones y no por sus acciones» (Mayer-Schönberger y Cukier, 2013).

Referencia bibliográfica

Viktor Mayer-Schönberger, Kenneth Cukier (2013). *Big data. La revolución de los datos masivos*. Turner Noema.

1.3. El RGPD y el *profiling*

Consciente de esta realidad (y sus peligros), el apartado primero del art. 22 del RGPD, siguiendo con lo ya establecido en la antigua directiva y su transposición en el artículo 13 de la LOPD (decisiones individuales automatizadas, incluida la elaboración de perfiles), otorga a los usuarios el derecho a no verse afectados por una decisión que solo se base en un análisis de esta naturaleza:

«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 art. 4.4 del RGPD define la «*elaboración de perfiles*» del siguiente modo:

«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, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de dicha persona física.»

La primera expresión de la potencial *peligrosidad* de la creación de perfiles la encontramos en el considerando 60 del RGPD, lo que parece superarse con la exigencia de información suficiente al afectado, que deja al usuario la decisión final sobre si con sus datos se va a proceder a elaborar perfiles, quitando ese «poder» al organismo correspondiente. Dicho considerando señala (las negritas son nuestras):

> «Se debe además **informar al interesado** de la existencia de la **elaboración de perfiles** y de las **consecuencias** de dicha elaboración.» Dicha exigencia deberá ponerse en relación con lo señalado en el considerando 63, en virtud del cual «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**.»

Claro está que, en la práctica, lo habitual será que la información que sirva de base para la elaboración de esos perfiles se obtenga de fuentes abiertas, como es el caso de las redes sociales o similares plataformas. Así pues, en el caso de que los datos de carácter personal fueran obtenidos del afectado a través de redes de comunicaciones electrónicas o en el marco de la prestación de un servicio de la sociedad de la información, el RGPD permite que el responsable pueda dar cumplimiento del deber de información del artículo 13 del RGPD facilitando al afectado una información básica, e indicándole una dirección electrónica a través de la cual pueda acceder a información adicional.

Observación

Teniendo en cuenta experiencias previas, cabe la posibilidad de abordar esta problemática desarrollando alguna plataforma semejante a la utilizada por la Alianza Europea de Publicidad Digital Interactiva (EDAA, por sus siglas en inglés) en relación con la publicidad comportamental, donde el usuario pueda encontrar información adicional, de manera unificada y, a ser posible, contrastada por el regulador, y que, en todo caso, deberá contener la preceptiva información señalada en los arts. 13 y 14 del RGPD. (Véase <http://www.youronlinechoices.com/es/>).

Y según se señala en el artículo 10.1.a) de la Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico, cuando dice que:

> «El prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información: su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva...»

Tal información básica deberá contener, al menos, la identidad del responsable del tratamiento o de su representante, en su caso; la finalidad del tratamiento y el modo en que el afectado podrá ejercitar los derechos establecidos en los artículos 15 a 22 del RGPD. Además, análogamente a lo que sucede con otros tipos de tratamientos de datos personales, el consentimiento del afectado se erige en elemento configurador de la legitimidad de los tratamientos[5], como así recomienda el Resumen del dictamen del Supervisor Europeo de Protección de Datos (SEPD) sobre la Propuesta de Reglamento relativo a la Privacidad y las Comunicaciones Electrónicas (Reglamento e-Privacy[6]), cuando señala:

[5] Aunque en ocasiones pueda resultar perjudicial para el interesado en el caso de que el responsable imponga cláusulas abusivas que produzcan un desequilibrio claro y en el que el usuario no tenga realmente una verdadera libertad de libre elección al sufrir un perjuicio en caso de negación del consentimiento.

[6] DOUE C 234/3 de 20 de julio de 2017.

> «Las normativas legales relativas al consentimiento de los usuarios legales deben ser reforzadas. Se debe solicitar el consentimiento de los individuos que están utilizando los servicios, se hayan suscrito a ellos o no, y de todas las partes que intervienen en la comunicación.»

Además de ello, el SEPD, reforzando la protección de datos debida, plantea varias objeciones al texto de la Propuesta de Reglamento de e-privacy (https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation). Más concretamente:

- El acceso a las páginas web no debe estar condicionado a que los individuos se vean forzados a «consentir» que sigan su rastro a través de las páginas

web. En otras palabras, el SEPD insta a los legisladores a asegurar que el consentimiento sea dado genuina y libremente.

- La propuesta no puede garantizar que los navegadores (y otros programas en el mercado que permiten las comunicaciones electrónicas) estén configurados por defecto para evitar el seguimiento de los pasos digitales de las personas.

- Las excepciones relativas al seguimiento de la ubicación de los equipos terminales son demasiado amplias y carecen de las salvaguardas adecuadas.

Cuestiones todas ellas que el SEPD hace extensivas a la actividad de realización de perfiles a partir de los datos.

Como se ha dicho, si el tratamiento de los datos tuviera como objetivo la elaboración de perfiles, la información básica a proporcionar a su titular debería contemplar, asimismo, esta exigencia. Es decir, será necesario que se indique al afectado, de forma clara, previa, visible y comprensible, que sus datos personales se recaban con la finalidad de elaborar perfiles en base al comportamiento como usuario, informándole de su derecho a oponerse a la adopción de decisiones individuales automatizadas que pudieran producir efectos jurídicos sobre él o afectarle significativamente[7].

(7)Así se expresa también el artículo 21 del anteproyecto de LOPD, en su versión del 19 de junio de 2017.

Por tanto, el RGPD deja claro que es posible la elaboración de perfiles bajo ciertos supuestos y siempre que se satisfagan una serie de cuestiones recogidas en la propia norma. A saber:

- **Considerandos 60 y 63 del RGPD / Artículos 13 y 14 del RGPD.** Esencialmente, informar previamente al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Aunque el RGPD no especifique qué debe entenderse por «consecuencias», hay que interpretar que se trata, precisamente, del objetivo concreto que la entidad persigue esa realización de perfiles[8]. La elaboración de perfiles debe tener un resultado o acción resultante (es decir, no se entendería como realización de perfiles aquella recopilación de datos de un usuario que no produjera un resultado concreto. En otras palabras, si se recogen muchos datos, pero no hay forma de darles un contexto o compararlos adecuadamente, no constituiría una elaboración de perfiles). Cabe destacar que, en relación con esta obligación de información a la que se refieren los citados considerandos, la exigencia es la de ser «previa», lo que nos lleva de nuevo a la reflexión sobre cómo la industria podrá aplicar en la práctica una exigencia como la que aquí se prevé, especialmente después del gran número de críticas que, unánimemente, se han vertido a la solución que en su día consensuaron la Agencia Española de Protección de Datos y la industria

(8)Así, por ejemplo –como señaló la AEPD, en su informe 78/2005–, una compañía telefónica que quiera saber las horas de conexión de un determinado usuario tendrá que explicar el objetivo concreto que se persigue con esa información para, por ejemplo, analizar si puede haber otra tarifa para la zona en la que se encuentre el usuario.

publicitaria española en relación con el diseño de la cláusula informativa para las *cookies*.

- **Considerandos 47 y 70 del RGPD / Artículo 21 del RGPD.** Si los datos personales son tratados con fines de *mercadotecnia directa*, el interesado debe tener derecho a oponerse a dicho tratamiento y a ser informado de tal derecho[9]. De nuevo, en este caso, el reglamento deja libertad a los anunciantes para diseñar vías aceptables de información previa a los usuarios y opciones válidas para el ejercicio efectivo de sus derechos.

(9)Sobre el sistema de *opt-in* véase el *Informe del Gabinete Jurídico de la AEPD*, en el consentimiento para instalar *cookies* 0011/2014.

- **Considerando 71 del RGPD / Artículos 22 y 47 del RGPD.** El interesado debe tener derecho a no ser objeto de una decisión que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar[10].

(10)El RGPD señala, como ejemplos de tales decisiones, la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana.

No obstante lo anterior, se permite la elaboración de perfiles (excepciones del considerando 71 del RGPD) si lo autoriza el derecho de la UE o el de alguno de sus Estados miembros. Esta excepción concreta abre la posibilidad, y así lo contempla expresamente el citado considerando, de que se autorice la elaboración de perfiles de usuarios con la finalidad, por ejemplo, de prevenir delitos fiscales y económicos. Asimismo, la opción los perfiles consentidos también podría resultar aplicable en aquellos casos en los que fuera necesario prestar el servicio contratado por el usuario o cuando se dispusiere de su consentimiento expreso.

Sea como fuere, y aunque la elaboración de perfiles se debiera a alguna de las circunstancias mencionadas, el sujeto sobre el que se realizó la realización de perfiles debe obtener una explicación del porqué de tal perfil y de la decisión que la organización hubiere tomado tras el análisis de los datos, dando posibilidad al titular de los mismos a expresar su punto de vista (e impugnar, en su caso) la decisión que eventualmente se haya tomado en relación con sus datos personales, comunicación que deberá materializarse siempre frente a una persona física real, no satisfaciéndose adecuadamente tal derecho si la respuesta se deriva de una acción mecanizada, como así se señala en el artículo 22.3 del RGPD:

> «En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión.»

La posibilidad de creación de perfiles se completa con lo dispuesto en los artículos 13.2.f), 14.2.g) y 15.1.h del RGPD, que señalan (las negritas son nuestras):

> «13.1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: […] 13.2.f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, 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.»

> «15.1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información: […] h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, 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.»

Por tanto, a las cuestiones anteriores habría que añadir, y así se menciona en el considerando 71:

- Información sobre la lógica aplicada. Es decir, explicar el mecanismo de funcionamiento del algoritmo subyacente que opera en la toma de decisiones automatizadas, desde el punto de vista y los intereses del usuario final. No se trata, por tanto, de conocer los fundamentos matemáticos o informáticos del algoritmo en cuestión (que podrían estar protegidos por la legislación en materia de propiedad intelectual o industrial), sino, por el contrario, saber bajo qué criterios opera el algoritmo (Pascuale III, 2017).

- No obstante lo anterior, cierto sector de la doctrina entiende que es improbable el ejercicio práctico y eficaz de un «derecho a la explicación» según el RGPD (véase, por ejemplo, Edwards y Veale, 2017) que, en el mejor de los casos, puede constituir una «distracción» de los objetivos fundamentales del RGPD y, en el peor, una falacia más en torno a la transparencia.

- Importancia del tratamiento. Se debe hacer ver al usuario la importancia de esa elaboración de perfiles desde el punto de vista de los intereses del usuario, no desde la perspectiva del responsable del tratamiento.

La potencial peligrosidad del *profiling* se pone de manifiesto también en el considerando 91 del RGPD (y en los correlativos artículos 35 y siguientes), cuando prescribe la obligación de llevar a cabo una *evaluación del impacto* si existe una elaboración de perfiles de dichos datos. En concreto, señala:

> «La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basadas en la elaboración de perfiles de dichos datos, o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas.»

Llegado este punto, merece la pena detenernos un instante en la exigencia o no de «automatismo» en la realización de perfiles y en sus ulteriores consecuencias.

Referencias bibliográficas

Frank A. Pascuale III (2017). «Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society». *Ohio State Law Journal* (vol. 78).

Lilian Edwards, Michael Veale (2017). «Slave to the Algorithm? Why a "Right to an Explanation" Is Probably not the Remedy You Are looking For» (3 de julio de 2017).

Así, recordando el artículo 22.1 del RGPD antes expuesto, señalábamos que ningún interesado debía verse obligado a ser objeto de una decisión basada únicamente en el tratamiento automatizado que pudiera afectarle.

En consecuencia, y dando por sentada la existencia de una base legal para el tratamiento, el precepto exige que la decisión final, a fin de que no sea recurrible por el usuario, no debe sustentarse **exclusivamente** en un tratamiento automatizado, sino que, complementariamente, una persona debe participar en tal decisión.

Por otro lado, la decisión a la que alude el art. 22.1 exige que produzca efectos jurídicos (o despliegue efectos similares) sobre el interesado. Como es lógico suponer, hay que interpretar esta idea de forma amplia, beneficiando siempre al titular de los datos. Sirva como ejemplo el que recoge el considerando 71, cuando menciona un supuesto de denegación automática *online* de una solicitud de crédito o la práctica de contratación electrónica sin intervención humana (hecho este que en la actualidad parece comenzar a generalizarse con la utilización de *chatbots*).

Como hemos adelantado, el RGPD, en el art. 22 y en el considerando 71, recoge ciertas excepciones en las que deben permitirse las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles. A saber:

- Si lo autoriza expresamente el derecho de la Unión o el de los Estados miembros aplicable al responsable del tratamiento[11].
- Si es necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento.
- Si el interesado ha dado su consentimiento explícito.

[11] Incluyendo los tratamientos realizados con fines de control y prevención del fraude y la evasión fiscal, realizados de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento.

La existencia del derecho de la Unión o de los Estados miembros, habilitante (o, en su caso, inhabilitante) para los tratamientos, está recogida en los arts. 6.3 (letras a y b), 9.2 (letras a, b, g, h, i y j), 9.3 y 10. Y, sobre todo, en aquellos contenidos del artículo 22.3 del RGPD que señalan que:

> «En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.»

Estos derechos de los interesados, relacionados con el *big data*, el *profiling* y su capacidad para oponerse a los tratamientos, deben extenderse también a las transferencias internacionales de datos y a las eventuales normas corporativas vinculantes autorizadas que pudieran invocarse, reglas corporativas que en todo caso deberán incorporar todos los principios esenciales y derechos

aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal, tal y como señala el considerando 110 del RGPD y según recoge el art. 47 de dicho cuerpo legal.

Aunque, como señala el artículo 22.4 del RGPD, las decisiones derivadas de una realización de perfiles previa no podrán sustentarse en categorías especiales de datos personales (por ejemplo, información racial, étnica o religiosa), se permite realizar este tipo de práctica siempre y cuando concurra alguno de los siguientes supuestos:

- La persona afectada haya dado su consentimiento explícito al tratamiento de dichos datos personales para uno o más fines especificados, excepto cuando la ley de la Unión o la de un Estado miembro lo prohíban. Los usuarios deben tener la opción real de negarse a la realización de perfiles.

- El tratamiento sea necesario por razones de interés público, esencial sobre la base de la legislación de la Unión o de los Estados miembros.

- No obstante, aun permitiendo el tratamiento de estos datos, el artículo 22.4 del RGPD (y, en el mismo sentido, el considerando 84) exige a los responsables y encargados del tratamiento que garanticen el establecimiento de «medidas adecuadas para salvaguardar los derechos y libertades de la persona afectada y sus legítimos intereses». La Propuesta de Reglamento sobre Privacidad y Comunicaciones Electrónicas (Reglamento ePrivacy en adelante) complementa esta idea con la necesidad de proteger las comunicaciones y transmisiones «máquina a máquina» (como, por ejemplo, la identificación mediante etiquetas de radiofrecuencia, los contadores inteligentes, las señales de geolocalización, etc.). Así, en su artículo 8 señala:

  «La recopilación de esta información quedará supeditada a la aplicación de medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado en relación con los riesgos, según lo establecido en el artículo 32 del Reglamento (UE) 2016/679.»

Dentro de los perfiles permitidos, el considerando 71 del RGPD obliga al responsable del tratamiento a utilizar, en todo caso, procedimientos matemáticos o estadísticos adecuados y a aplicar medidas técnicas y organizativas para corregir inexactitudes y evitar errores, minimizando así el riesgo de «efectos discriminatorios contra personas físicas sobre la base de un origen racial o étnico, las ideas políticas, la religión o las creencias, la afiliación sindical, la salud o la genética, o la orientación sexual, o que den lugar a medidas que produzcan tal efecto».

Finalmente, otro aspecto que merece una especial atención es el relativo al derecho que tiene el afectado por el *profiling* a oponerse al tratamiento en cualquier caso y en todo momento, incluso cuando la elaboración de perfiles sea perfectamente legal.

Así, de conformidad con lo dispuesto en el artículo 21 del RGPD, y aun habiendo estado autorizado con arreglo al artículo 6, el tratamiento de datos deberá cesar en caso de objeción de la persona afectada a la elaboración de perfiles, a menos que el responsable del tratamiento demuestre «motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.» De nuevo, el reglamento hace prevalecer el derecho del usuario (como parte más débil de la ecuación) frente a los intereses de la industria, salvo que existan motivos debidamente justificados, como podrían ser los casos de interés legítimo a los que se refieren los considerandos 47 y 70. En el caso de los menores de edad, el interés de estos prevalece con más fuerza respecto del interés legítimo del responsable del tratamiento (art. 6.1.f) RGPD).

Este derecho de oposición al tratamiento se aplicará, sin mayores condicionantes, cuando el tratamiento sea con fines de mercadotecnia directa.

En la práctica, lo que el artículo 21 pretende es que este derecho sea específicamente citado, de manera que el usuario tenga conocimiento de la posibilidad de ejercicio autónomo de este derecho de oposición, lo que supone una novedad respecto del régimen actual de la LOPD. De cara a su ejecución, dicho artículo obliga a que, a más tardar en el momento de la primera comunicación con el interesado, este derecho de oposición desarrollado en los apartados 1 y 2 se mencione explícitamente al interesado y se presente claramente y al margen de cualquier otra información. De este modo, en el caso del desarrollo de actividades de *profiling*, el responsable de tales actividades deberá desarrollar un procedimiento en virtud del cual el usuario afectado pueda oponerse al tratamiento de sus datos de manera autónoma y sin que la presentación de tal vía se pueda confundir con otros procesos de ejercicio de derechos puestos a su disposición.

2. Publicidad comportamental *online*

2.1. ¿Qué es la publicidad comportamental *online*?

Independientemente de que más adelante ofrezcamos las definiciones que distintos autores han formulado, diremos ahora que la publicidad comportamental *online* (PCO) (*online behavioral advertising*, OBA) comprende un conjunto de actividades tendentes a recabar y tratar los datos derivados de las transacciones o del comportamiento *online* de los usuarios al objeto de personalizar y orientar dicha publicidad. Como es lógico suponer, tales datos pueden ser de tipología y procedencia muy variadas, contemplando, entre otros muchos, referencias a los sitios web visitados, los artículos leídos, los vídeos vistos, así como todo lo que se indague usando un motor de búsqueda.

> Un ejemplo de PCO sería cuando una red de publicidad (una empresa que, por lo general, suministra publicidad a miles de sitios web) examina las visitas de un consumidor a tal sitio web. Si se observa que un determinado consumidor visita varios sitios web sobre guitarras, la red asume que el consumidor está interesado en ese producto. En base a ello, la red está en condiciones de mostrar anuncios de guitarras solo a personas (presumiblemente interesadas) en ellas. Por este motivo, cuando dos personas visitan el mismo sitio web simultáneamente, uno puede ver los anuncios de guitarras mientras que el otro, que había visitado sitios web sobre plumas, verá anuncios de plumas.

No es de extrañar, en consecuencia, que los anunciantes consideren la PCO como una nueva y efectiva forma de llegar a su público objetivo, como lo demuestran las tasas de crecimiento anual de los ingresos por PCO, tanto en los Estados Unidos como en el resto del mundo (véase eMarketer, 2010, y también Chen y Stallaert, 2014).

Referencias bibliográficas

eMarketer (16 de febrero de 2010). *How Should Marketers Address Concerns about Ad Targeting?* [en línea] <https://www.emarketer.com/Article/How-Should-Marketers-Address-Concerns-About-Ad-Targeting/1007514>

Jianqing Chen, **Jan Stallaert** (2014). «An Economic Analysis of Online Advertising Using Behavioral Targeting». *MIS Quarterly* (vol. 38, n.º 2, págs. 429–449).

2.2. Los riesgos de la PCO

No obstante, al tiempo que la industria mantiene la convicción de que la PCO es capaz de crear una publicidad más eficiente y, en consecuencia, provocar un incremento de los ingresos (Howard, 2010), el desarrollo de la PCO se muestra ante el consumidor como un riesgo que puede afectar a su privacidad por lo que tiene de recopilación, uso y compartición de datos personales.

Referencia bibliográfica

Howard Beales (2010). *The Value of Behavioral Targeting* [en línea] <http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf>

Es debido a esta preocupación entre los consumidores por lo que la PCO viene siendo sistemáticamente examinada por organismos reguladores tales como la Comisión Federal de Comercio de los Estados Unidos (FTC 2012)[12], las autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29[13]) y distintas organizaciones de consumidores. En respuesta a tales inquietudes, pero conscientes de esta problemática, ciertas asociaciones de la industria, como por ejemplo la Digital Advertising Alliance, en EE. UU., y la European Interactive Digital Advertising Alliance, en Europa, han establecido programas de autorregulación dirigidos a proteger la privacidad de los consumidores y a analizar cómo deben ser informados sobre la recopilación y el uso de sus datos.

Como decimos, hay muchas definiciones de PCO, que en el entorno anglosajón también suele denominarse *online profiling* ('perfil online') y *behavioral targeting* ('segmentación por comportamiento')[14]. He aquí algunas de ellas:

> «Determinación de la publicidad basada en un comportamiento de navegación previo.» (Smit, Van Noort y Voorveld, 2014)

> «Un método de personalización de publicidad dirigida por la tecnología que permite a los anunciantes entregar mensajes publicitarios de gran importancia para los individuos.» (Ham y Nelson, 2016)

> «La recolección de datos sobre las actividades en línea de un individuo para su uso en la selección de qué anuncio mostrar en cada momento.» (McDonald y Cranor, 2010)

2.3. PCO y *cookies*

Desde el punto de vista tecnológico, el mecanismo que las empresas de publicidad utilizan con más frecuencia para recabar los datos del comportamiento de navegación de los consumidores son las denominadas *cookies* (en sus distintas variedades de rastreo, *flash cookies*, etc.). Se ha acreditado (Altaweel, Good y Hoofnagle, 2015) que los 100 sitios web más populares recaban más de 6.000 *cookies*, de las cuales el 83% son de terceros. Estos elementos permiten a las empresas recopilar información muy útil de millones de consumidores y, en muchas ocasiones, para usarla posteriormente con fines de PCO (según se afirma en Boerman, Kruikemeier y Zuiderveen, 2017, Facebook tiene perfiles individuales de 1,65 millones de personas y AddThis tiene perfiles de 1,9 millones de personas).

(12) Federal Trade Commission (2012), *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, marzo,* <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

(13) Documento de trabajo 171. *Opinion 2/2010 on Online Behavioural Advertising*. Article 29 Data Protection Working Party (2010 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf>

(14) Véase: Steven C. Bennett, (2011). «Regulating Online Behavioral Advertising». *John Marshall Law Review* (núm. 44, 899–62).

Referencias bibliográficas

Edith G. Smit, Guda Van Noort, Hilde A. Voorveld (2014). «Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns, and Online Coping Behaviour in Europe». *Computers in Human Behavior* (n.º 32, págs. 15–22).

Chang-Dae Ham, Michelle R. Nelson (2016). «The Role of Persuasion Knowledge, Assessment of Benefit and Harm, and Third-person Perception in Coping with Online Behavioral Advertising». *Computers in Human Behavior* (n.º 62, págs. 689–702).

Aleecia M. McDonald, Lorrie F. Cranor (2010). «Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising». *TPRC* [en línea] <http://aleecia.com/authors-drafts/tprc-behav-AV.pdf>

En relación con la PCO, la *Guía sobre las normas de uso de las cookies* de la AEPD establece diferentes clasificaciones de las mismas en función de su finalidad. Entre otras, distingue las siguientes:

- **Cookies publicitarias**. Se trata de aquellas que permiten la gestión de los espacios publicitarios que el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado, en base a criterios como el contenido editado o la frecuencia con la que se muestran los anuncios.

- **Cookies de publicidad comportamental**. Son las que almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación.

En el despliegue y la utilización de estas *cookies* intervienen los siguientes actores[15]:

Tabla 1

Usuario Es el destinatario, persona física, que accede al servicio prestado por un editor.	**Editor** Entidad prestadora de servicios de la sociedad de la información titular de una página web a los que puede acceder un usuario y para cuya prestación se utilizan *cookies*.
Anunciante Entidades cuyos productos, servicios o imagen se anuncian a través de los espacios publicitarios de los que disponen los editores en sus páginas o en otras aplicaciones desde las que prestan los servicios a los usuarios.	**Agencias de publicidad / de medios** Entidades que se encargan del diseño y la ejecución de publicidad, así como de la creación, preparación o programación de las campañas publicitarias de los anunciantes.
Redes publicitarias Entidades que, actuando en nombre de uno o varios editores, ofrecen la posibilidad de obtener espacios publicitarios o algún tipo de resultado concreto a través de la gestión y el tratamiento de los datos obtenidos de la utilización de las *cookies* descargadas o almacenadas en los equipos terminales de los usuarios.	**Empresas de análisis y medición** Entidades que miden y/o analizan el comportamiento de la navegación de los usuarios en la página web de un editor, con la finalidad de mejorar el servicio que presta el editor.

2.4. Los datos usados por la PCO

Los datos utilizados para desarrollar la PCO no son siempre los mismos, sino que dependen del nivel de personalización (individualización) perseguido, el cual se sustenta en:

- Los **tipos de datos** que se utilizan para orientar el anuncio (por ejemplo, los datos de navegación o el historial de búsqueda).

- El **volumen de información** que se utiliza (por ejemplo, aquellos datos que se obtienen de una sola búsqueda o de la combinación de una multiplicidad de datos de navegación e historiales de búsqueda).

Referencias bibliográficas

Ibrahim Altaweel, Nathaniel Good, Chris J. Hoofnagle (2015). «Web Privacy Census». *Technology Science* [en línea] <http://techscience.org/a/2015121502>.

Sophie C. Boerman, Sanne Kruikemeier, Frederik J. Zuiderveen Borgesius (2017). «Online Behavioral Advertising: A Literature Review and Research Agenda». *Journal of Advertising*. [en línea] <http://dx.doi.org/10.1080/00913367.2017.1339368>.

(15)AEPD. *Guía sobre las normas de uso de las cookies. Op. cit.*

Los datos más frecuentemente utilizados para conformar los niveles de personalización más usuales suelen ser: edad, sexo y ubicación (Aguirre y otros, 2015); nivel de educación (Tucker, 2014); intereses (Aguirre, *op. cit.* y Tucker, *op. cit.*); comportamiento de compras *online* (Bleier y Eisenbeiss, 2015); y el historial de búsquedas (Van Doorn y Hoekstra, 2013).

Referencias bibliográficas

Elizabeth Aguirre, Dominik Mahr, Dhruv Grewal, Ko de Ruyter, Martin Wetzels (2015). «Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-building Strategies on Online Advertisement Effectiveness». *Journal of Retailing* (vol. 91, n.º 1, págs. 34–49).

Catherine E. Tucker (2014). «Social Networks, Personalized Advertising, and Privacy Controls». *Journal of Marketing Research* (vol. 51, n.º 5, págs. 546–562).

Alexander Bleier, Maik Eisenbeiss (2015). «The Importance of Trust for Personalized Online Advertising». *Journal of Retailing* (vol. 91, n.º 3, págs. 390–409).

Jenny Van Doorn, Janny C. Hoekstra (2013). «Customization of Online Advertising: The Role of Intrusiveness». *Marketing Letters* (vol. 24, n.º 4, págs. 339–351).

A pesar de las potenciales ventajas que pueda ofrecer una tecnología publicitaria como la descrita, los hallazgos obtenidos de las investigaciones referidas señalan que el nivel de personalización influye claramente en factores relacionados con el consumo tales como la sensación de intrusión o de vulnerabilidad y la utilidad percibida del anuncio[16].

[16]No entramos ahora a valorar las respuestas negativas a niveles más altos de personalización que, según los estudios citados, corresponden a la teoría de la elección, la teoría de la propiedad psicológica y la teoría de la reactancia psicológica.

2.5. La aproximación normativa europea a la PCO

La plataforma REFIT (formada por la Comisión Europea, las autoridades nacionales y diversas partes interesadas en mejorar la legislación actual de la UE), cuya función es apoyar el proceso de simplificación de la legislación de la UE y reducir la carga normativa, publicó en 2016 ciertas recomendaciones con el fin de asegurar la protección de los datos personales en relación con la publicidad comportamental, que se resumen a continuación:

- La Comisión, los Estados miembros y las autoridades de protección de datos deben garantizar que la directiva sobre la privacidad electrónica, objeto de revisión (y que fue adoptada en 2002 y modificada en 2009), esté en consonancia y no se solape con el Reglamento General de Protección de Datos adoptado en 2016. La Comisión y los Estados miembros deben procurar una mayor armonización en la aplicación de la directiva (y la Propuesta de Reglamento que en su caso llegue a derogarla), incluidas las disposiciones sobre *cookies* y los mecanismos de aplicación.

- El Parlamento Europeo y los Estados miembros, incluidas las autoridades nacionales de protección de datos, deberían promover un enfoque de «privacidad por diseño». Las reglas relacionadas con las *cookies* y las tecnologías de seguimiento, así como las reglas sobre las comunicaciones no solicitadas, deben ser revisadas para asegurar que sean adecuadas en el futuro.

- Bajo determinadas condiciones, podrían preverse excepciones adicionales a la regla del «consentimiento» para las *cookies* y técnicas similares. La información proporcionada a los consumidores en relación con el requisito del «consentimiento para aceptar las *cookies*» debe tener sentido, ser completa y de fácil comprensión.

- La reforma de la legislación no debe abrir ninguna puerta trasera dirigida al seguimiento de los usuarios y cualquier excepción a la regla del consentimiento solo debe afectar a las *cookies* que no supongan ningún riesgo para la privacidad.

También el RGPD muestra su preocupación por el desarrollo de este tipo de tecnología. Así, en su considerando 30 hace la única mención al término «*cookies*» que aparece en dicha norma, para referirse a este supuesto de la siguiente manera:

> «Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de "*cookies*" u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.»

Por su parte, también la Propuesta de Reglamento e-Privacy[17], consciente de esta problemática, plantea regular estas (casi) nuevas técnicas que permitirían rastrear los comportamientos en línea de los usuarios finales y, como consecuencia, posibilitar la PCO. Así pues, en su considerando 6 afirma que:

> «Aunque los principios y las principales disposiciones de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sigan siendo por lo general válidos, dicha directiva no se ha adaptado del todo al ritmo de la evolución de la tecnología y del mercado, debido a lo cual se ha deparado una protección incoherente e insuficientemente eficaz de la privacidad y la confidencialidad en relación con las comunicaciones electrónicas. Por lo tanto, procede derogar la Directiva 2002/58/CE y sustituirla por el presente reglamento.»

(17)Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). Usualmente denominado Reglamento e-Privacy <http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017PC0010&from=IT>.

Esta propuesta normativa, además, establece la necesidad de autorizar a los Estados miembros para crear disposiciones nacionales que garanticen la aplicación e interpretación efectiva de la norma, así como la necesidad de delegar en la Comisión (considerando 41 y artículo 8.3) el poder de adoptar actos conducentes al desarrollo de iconos normalizados que ofrezcan un panorama general visible e inteligible de la recogida de la información emitida por los equipos terminales, su finalidad, las personas responsables y cualquier medida que el usuario final del equipo terminal puede adoptar para reducir al mínimo dicha recopilación. Esta norma parece que persigue normalizar el desarrollo del icono informativo desarrollado por la industria a los efectos de identificar qué publicidad de la que se muestra a un usuario de internet está basada en el análisis del comportamiento deducido tras el análisis de su historial de navegación a través de la tecnología de *tracking cookies*.

2.6. Información y consentimiento del usuario en la LSSICE y en la Propuesta de Reglamento e-Privacy

Con carácter previo, hay que advertir que el RGPD menciona, en su considerando 24, que:

> «[...] para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.»

Seguimiento en internet

Como se señala en el artículo 4.4 del RGPD, la definición de elaboración de perfiles es la siguiente: «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, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de dicha persona física.»

A fecha de hoy, en el apartado segundo del artículo 22.2 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), se señala (las negritas son nuestras):

> «Los prestadores de servicios podrán utilizar **dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios**, a condición de que los mismos hayan dado su **consentimiento** después de que se les **haya facilitado información clara y completa sobre su utilización**, en particular, sobre los **fines del tratamiento** de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.»

Y añade que:

> «Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el **uso de los parámetros adecuados del navegador** o de otras aplicaciones.
>
> Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.»

Este precepto nacional parece dejar claras dos cuestiones:

- En primer lugar (antes del RGPD), se acepta (con condiciones) el uso de los dispositivos referidos en los terminales como mecanismo para recabar el comportamiento del usuario.

- En segundo lugar (con la entrada en vigor del RGPD), se exige que, con anterioridad a su consentimiento, la información que se suministre al usuario debe ser tan completa y clara como fuere necesario para que tal usuario conozca fielmente la finalidad perseguida por dichos «*dispositivos de almacenamiento y recuperación de datos*» (*cookies*, en definitiva) y el uso que se dará a la información recabada.

A primera vista, más limitativo parece el redactado de la Propuesta de Reglamento e-Privacy, cuyo artículo 8.1 (las negritas son nuestras) señala:

«1. El uso de las **capacidades de tratamiento y almacenamiento de los equipos terminales** y la **recopilación de información del equipo terminal** de los usuarios finales, incluida la relativa a su soporte físico y lógico, excepto por parte del usuario final, **estarán prohibidos**, **salvo** por los motivos siguientes:

a) cuando sean **necesarios con el fin exclusivo de efectuar la transmisión** de una comunicación electrónica a través de una red de comunicaciones electrónicas, o

b) cuando el usuario final haya dado su **consentimiento**, o

c) cuando sean necesarios para la **prestación de un servicio de la sociedad de la información solicitado por el usuario final**, o

d) cuando sean **necesarios para medir la audiencia en la web**, siempre que esa medición corra a cargo del proveedor del servicio de la sociedad de la información solicitado por el usuario final.»

Como puede observarse, la redacción dada al precepto arranca prohibiendo el uso de aquellos dispositivos para, acto seguido, posibilitar su uso bajo ciertos supuestos.

2.7. El consentimiento como base legitimadora del tratamiento

Como hemos visto, el art. 22.2 de la LSSICE exige el consentimiento del usuario para la recogida de datos (y su ulterior tratamiento) a través de *cookies*.

Por su parte, la *Guía sobre las normas de uso de las cookies* de la AEPD señala que tal consentimiento:

«podrá obtenerse mediante fórmulas expresas, tales como haciendo clic en un apartado que indique "consiento", "acepto", u otros términos similares; o infiriendo el consentimiento de una determinada acción realizada por el usuario, en un contexto en que a este se le haya facilitado información clara y accesible sobre las finalidades de las *cookies* y de si van a ser utilizadas por el mismo editor y/o por terceros, de forma que quepa entender que el usuario acepta que se instalen *cookies*.»

Con la aprobación del RGPD, en el caso en que haya tratamiento de datos de carácter personal, se aplicarán las normas sobre el consentimiento que en él se establezcan. No obstante, la tónica general de la industria, con tal de evitar la aplicación de la LOPD (que está siendo objeto de reforma), ha sido la de no tratar datos personales o anonimizarlos. De este modo, se evitaba cumplir una gran cantidad de exigentes requisitos técnicos y organizativos que resultaban prescindibles para el desarrollo del negocio. A la vista de la nueva regulación, parece que dicha tendencia se seguirá manteniendo, incluso con mayor intensidad, teniendo en cuenta el nuevo régimen sancionador y el mayor control que parece implementar el RGPD.

La Propuesta de Reglamento e-Privacy sigue el mismo principio del consentimiento habilitante[18]. Para obtener el consentimiento de los usuarios finales según se define en el RGPD, los navegadores deben solicitar al usuario final del equipo terminal un acto afirmativo claro que manifieste su voluntad libre, específica, informada e inequívoca de aceptar el almacenamiento de las *cookies* en el equipo y el ulterior acceso a las mismas. Dicho acto, como se especifica en la Propuesta de Reglamento e-Privacy, puede considerarse un acto afirmativo

(18)Considerando 24.

si se solicita a los usuarios finales que seleccionen la opción «aceptar *cookies* de terceros» para confirmar su acuerdo y se les ofrece la información necesaria para poder elegir.

Llegados a este punto, es imprescindible remarcar la necesaria implicación de los fabricantes con el fin de que hagan saber a los usuarios finales las posibilidades que tienen para elegir la configuración de privacidad de sus navegadores[19]. Obviamente, la información suministrada debe ser neutra, sin animar a los usuarios a seleccionar una configuración de menor privacidad. Además, tal información deberá contemplar los riesgos que puede entrañar autorizar el almacenamiento de *cookies* de terceros en el ordenador, incluyendo la conservación a largo plazo de registros de los historiales de navegación y el uso de los mismos para la remisión de publicidad personalizada[20].

(19)Propuesta de Reglamento e-Privacy, art. 10.

(20)Por este motivo, resulta conveniente que los navegadores propongan a los usuarios procedimientos sencillos para modificar en cualquier momento la configuración de privacidad, que les permitan excluir o aceptar determinados sitios web o especificar en qué sitios web aceptan siempre o no aceptan nunca *cookies* (de terceros).

2.8. Mecanismos de obtención del consentimiento

La precitada *Guía sobre las normas de uso de las cookies* de la AEPD señala los mecanismos que resultarían jurídicamente admisibles para obtener el consentimiento. De forma resumida:

- A través de la aceptación de los «términos y condiciones de uso de la página web» o de su «política de privacidad» al solicitar el alta en un servicio.

- Durante el proceso de configuración del funcionamiento de la página web o aplicación (*settings-led consent*).

- En el momento en que se solicite una nueva función ofrecida en la página web o aplicación (*feature-led consent*).

- Antes del momento en que se vaya a descargar un servicio o una aplicación ofrecidos en la página web.

- A través del formato de información por capas, donde la primera de ellas debe incluir la petición del consentimiento.

Finalmente –según se establece en la guía de la AEPD–, podría entenderse que el usuario ha dado su consentimiento para la instalación de las *cookies* si, pese a no haberlo hecho de forma expresa, continuara utilizando la página web. Además, deben darse otros requisitos, como que se le haya informado claramente en este sentido y que se ofrezca en todo momento, a través de las formas señaladas en dicha guía y de modo permanente, un aviso que facilite información sobre la utilización de las *cookies* y la posibilidad de desinstalarlas. En base a lo dicho, se entenderá que se ha prestado el consentimiento:

- Si el usuario ha utilizado la barra de desplazamiento, siempre y cuando la información sobre las *cookies* sea visible, sin hacer uso de esta.

- Si el usuario ha clicado sobre cualquier enlace contenido en la página.

- A través de la configuración del navegador.

La importancia de la protección efectiva a los equipos terminales de los usuarios también está presente en la Propuesta de Reglamento e-Privacy que, en relación con el principio de proporcionalidad[21], pone de manifiesto la ineficacia de la todavía vigente Directiva sobre privacidad y comunicaciones electrónicas[22], que no ha resultado eficaz para capacitar a los usuarios finales en este ámbito. La Propuesta de Reglamento e-Privacy insiste en que es necesario aplicar este principio de proporcionalidad (entre las garantías perseguidas y las medidas a adoptar) centralizando el consentimiento en los programas informáticos y facilitando a los usuarios información sobre las opciones de privacidad que ofrecen[23].

Por otro lado, es opinión del REFIT que la todavía vigente Directiva de privacidad, en lo relativo a la eficacia y eficiencia perseguidas, no ha alcanzado plenamente sus objetivos, puesto que los usuarios finales podrían dar su consentimiento para la instalación de *cookies* de rastreo sin comprender lo que ello significa y, en el peor de los casos, sin su consentimiento.

Para hacer frente a todo ello, de entre las opciones manejadas en los trabajos preparatorios de la Propuesta de Reglamento e-Privacy, se entendió como más oportuna aquella que suponía un «refuerzo moderado de la privacidad/confidencialidad y simplificación»[24]. Esta opción se caracteriza por:

- Centralizar el consentimiento de los usuarios en los programas o en las aplicaciones, tales como los navegadores de internet.

- Animar a los usuarios a elegir su configuración de privacidad.

- Ampliar las excepciones a la norma del consentimiento del uso de *cookies* (en cuya virtud es posible que una porción de empresas elimine los mensajes y anuncios de *cookies*).

- Incrementar la dificultad para obtener el consentimiento en actividades de PCO, en aquellos usuarios que opten por no aceptar *cookies* de terceros en la configuración de los navegadores.

(21)Enunciado en el art. 5 del Tratado de la UE.

(22)Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

(23)La Propuesta de Reglamento e-Privacy, al objeto de abordar necesidades locales, posibilita que los Estados miembros implanten excepciones nacionales para determinados fines legítimos.

(24)Epígrafe 3.4. Propuesta de Reglamento e-Privacy.

Finalmente, y de cara a armonizar los preceptos de ambas normas (RGPD y e-Privacy), la Propuesta de Reglamento e-Privacy[25] regula el consentimiento del usuario final, independientemente de si se trata de una persona física o jurídica, con el mismo significado y sujeto a las mismas condiciones que el consentimiento del interesado a tenor de lo dispuesto en el RGPD.

[25]Considerando 18 y artículo 9.

2.9. Excepciones al consentimiento

La Propuesta de Reglamento e-Privacy[26] recoge las excepciones a la obligación de obtener el consentimiento para hacer uso de las capacidades de tratamiento y almacenamiento de equipos terminales o acceder a la información almacenada en ellos, limitándolas a aquellas situaciones que no supongan intromisión (o lo hagan de manera limitada) a la vida privada[27]. Por ejemplo:

[26]considerando 21 y artículo 8.

[27]Señala el e-Privacy, a modo de ejemplo, que no debería solicitarse consentimiento para autorizar el acceso o almacenamiento técnico que sean estrictamente necesarios y proporcionados al fin legítimo de permitir el uso de un servicio específico expresamente solicitado por el usuario final.

- No debe solicitarse el consentimiento para autorizar el acceso o almacenamiento técnico que sean estrictamente necesarios y proporcionados para el fin legítimo de permitir el uso de un servicio específico expresamente solicitado por el usuario final[28].

[28]Lo que puede incluir el almacenamiento de *cookies* mientras dure una sesión única determinada en un sitio web, a fin de conservar las entradas del usuario final cuando este rellena formularios en línea de varias páginas

- No debe solicitarse el consentimiento cuando las *cookies* se utilicen para medir el tráfico en un sitio web.

- No debe considerase como acceso a un dispositivo o utilización de las capacidades de tratamiento la comprobación de la configuración que realice un proveedor de la sociedad de la información para prestar el servicio de acuerdo con los parámetros del usuario final, así como tampoco el mero registro por parte del proveedor del hecho de que el dispositivo del usuario final no puede recibir el contenido que ha solicitado.

2.10. Cambios en el uso de las *cookies*

Como señala la *Guía sobre las normas de uso de las cookies*, se indica que el consentimiento puede fundamentarse en las circunstancias concretas que concurren en el acceso por parte de un equipo terminal en particular a una determinada página web. Si el consentimiento ha sido originariamente obtenido de forma válida, no es necesario obtenerlo de nuevo cada vez que un usuario visite la página web en cuestión. No obstante, si las características o los fines de uso de las *cookies* cambian después de haber obtenido el consentimiento, será necesario informar a los usuarios acerca de esos cambios y permitirles tomar una nueva decisión acerca de tales actividades.

2.11. Revocación del consentimiento para el uso de *cookies*

El derecho a la revocación del consentimiento en cualquier momento, que se contiene en el apartado 1 del art. 22 de la LSSICE, cabe extenderlo también al consentimiento expresado para el almacenamiento de *cookies* en el equipo terminal del usuario. Por este motivo, el editor deberá asegurarse de que, en su política de privacidad, facilita información a los usuarios sobre cómo se puede revocar el consentimiento y de qué forma se pueden eliminar las *cookies*. Para ello, es necesario que, como se afirma en el apartado VII de la *Guía sobre las normas de uso de las cookies* de la AEPD, «Retirada del consentimiento para el uso de las *cookies*», se informe al usuario sobre las consecuencias derivadas de la retirada de dicho consentimiento, como, por ejemplo, del impacto que ello puede tener en las funcionalidades de la página web en cuestión.

2.12. Posibilidad de denegación de acceso al servicio en caso de rechazo a las *cookies*

Como se ha dicho –y así recuerda la precitada guía de la AEPD–, podrán existir supuestos en los que la no aceptación de la instalación de *cookies* impida la utilización total o parcial del servicio, siempre que se informe adecuadamente al usuario a este respecto:

> «No obstante, no podrá denegarse el acceso al servicio en caso de rechazo a las *cookies* en aquellos supuestos en que tal denegación impida el ejercicio de un derecho legalmente reconocido al usuario, por ser el acceso a dicha página web el único medio facilitado al usuario para ejercitar tal derecho.»

Ejemplo

Por ejemplo, la baja en un servicio telefónico, de acceso a internet o de otro tipo.

2.13. Muros de *cookies* (*tracking walls*) y otros sistemas del tipo «lo-tomas-o-lo-dejas»

El Grupo de Trabajo del Artículo 29, en su documento de trabajo número 247, señala expresamente que muchos sitios de internet solo dan a los usuarios las opciones de aceptar las condiciones que unilateralmente impone el sitio en relación con el uso de *cookies* o, en caso de no aceptar, impedir totalmente su funcionalidad. Esas barreras de acceso, conocidas como *tracking walls* o «muros de *cookies*», provocan que muchos usuarios se vean impelidos a permitir el acceso a sus datos, aunque no quieran, si finalmente necesitan utilizar el servicio web de que se trate.

El Grupo de Trabajo del Artículo 29 ha sido consciente de esta realidad y, en tal sentido, ha mostrado su preocupación[29] al señalar, en relación con los *tracking walls*, que el reglamento propuesto disminuiría el nivel de protección que se disfrutaba en el marco del RGPD y recomienda una prohibición explícita del uso de estos procedimientos que obligan a los usuarios a consentir la recopilación de datos si desean tener acceso al servicio.

(29)Véase: Article 29 Data Protection Working Party *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*. Adoptada el 4 de abril de 2017.

Tal como ya se ha señalado en anteriores opiniones del GT29 en relación con la Directiva sobre privacidad electrónica[30], estos planteamientos de «lo-tomas-o-lo-dejas» rara vez son legítimos[31]. Cuando el uso de la capacidad de procesamiento y almacenamiento de los equipos terminales o la recogida de información de tales equipos permita el seguimiento de las actividades del usuario a través del tiempo, o a través de distintos servicios (por ejemplo, en diferentes sitios web o aplicaciones), tales actividades de procesamiento pueden suponer un serio riesgo para la privacidad de sus usuarios. Así pues, dada la importancia fundamental de internet para instrumentalizar el derecho fundamental a la libertad de expresión, incluido el derecho de acceso a la información, la capacidad de los particulares para acceder a los contenidos *online* no debe depender de la aceptación del *tracking* de sus actividades en dispositivos y sitios web o aplicaciones. En consecuencia, la futura normativa sobre privacidad electrónica debería especificar que el acceso a contenidos en sitios web y aplicaciones no puede condicionarse a la aceptación de dichas actividades de procesamiento intrusivo, independientemente de la tecnología de seguimiento aplicada (*cookies*, huella digital del dispositivo, inyección de identificadores únicos) o cualesquiera otras técnicas de monitorización.

(30)Véase, por ejemplo, el documento de trabajo 240 (*ePrivacy review*), pág. 16; el documento de trabajo 208 (*consent exemption*), pág. 5.

(31)Esta posición se entiende sin perjuicio de lo dispuesto en el artículo 7.4 del RGPD, que también puede impedir «tomarlo o dejarlo» en otras situaciones, cuando sea apropiado.

Por tanto, no parece descabellado pensar, por ejemplo, que los sitios web financiados por el Estado, los sitios relacionados con la salud u otras informaciones sensibles y los sitios con una posición de monopolio no deben poder instalar muros de seguimiento, circunstancias que deberán ser presumiblemente matizadas por las normas que cada Estado miembro decida adoptar al efecto.

2.14. Resumen sumario de conceptos y normativa en la que se basan

Tabla 2

	Grupo de Trabajo 29*	LSSICE, art. 22	LOPD	Propuesta Reglamento e-Privacy	RGPD
¿Cómo debe ser la política de privacidad de la página web?			Adecuar el mensaje al tipo de usuario medio al que se dirige esa página web. *Guía sobre las normas de uso de las cookies*, AEPD.	Clarificación y simplificación de la norma relativa al consentimiento para el uso de *cookies* y otros identificadores (secciones 3.1 y 3.4).	«Toda información debe ser **concisa, fácilmente accesible, fácil de entender, y que se utilice un lenguaje claro y sencillo**» (considerando 58).

* Dictámenes previos a la publicación del RGPD.

	Grupo de Trabajo 29*	LSSICE, art. 22	LOPD	Propuesta Reglamento e-Privacy	RGPD
¿Qué debe incluir la política de *cookies*?	**Dictamen 4/2012** No especifica nada. Solo menciona que la «Información [debe ser] presentada de manera clara y comprensible».		Si los usuarios de la plataforma tienen niveles elevados de conocimientos técnicos, no es preciso poner qué son las *cookies*. Sí debe indicarse la finalidad de estas. *Guía sobre las normas de uso de las cookies*, AEPD.		No hace referencia expresa a las *cookies*, pero sí recalca que debe incluirse toda la información posible cuando se dé la información al interesado. Según el considerando 58, «El principio de transparencia exige que **toda información** dirigida al público o al interesado sea concisa, fácilmente accesible y **fácil de entender**, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. **Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo**,[…]».
División de la información de las *cookies por capas*			Indicar el tipo de *cookies* que se utiliza y la finalidad de estas (en la primera capa). Indicar las características más técnicas en la segunda capa. *Guía sobre las normas de uso de las cookies*, AEPD.		El RGPD no indica nada acerca de dividir la información por capas. Por lo tanto, aunque la finalidad se debe mostrar en la primera, el reglamento permite que, si se quiere saber más sobre qué tipos de *cookies* están instaladas, se acceda a una segunda capa donde se muestre.
¿Qué garantías deben establecerse de cara a la protección de los menores?	No hace especial referencia a los menores.	No hace especial referencia a los menores. Solo se menciona que se restringirá la prestación de aquellos servicios que supongan un daño o un peligro para la protección de los menores.	No hace especial referencia a los menores, apenas una línea en la guía de *cookies*: «Asimismo, es conveniente recordar la necesidad de adoptar cautelas adicionales en este ámbito en relación con los menores de edad.»		Si la página va destinada a menores, adecuar el mensaje a ellos y poner imágenes o referencias visuales de más sencilla comprensión (considerando 58, artículo 12.1 RGPD).

* Dictámenes previos a la publicación del RGPD.

	Grupo de Trabajo 29*	LSSICE, art. 22	LOPD	Propuesta Reglamento e-Privacy	RGPD
¿Cómo debe mostrarse el aviso de *cookies*?			Se tiene que ver. Se señala que debe tenerse en cuenta el diseño y la mecánica de la página web para adaptarlos de la mejor forma posible a este requisito. Se propone como solución: **a)** Incrementar el tamaño del enlace. **b)** Poner el anuncio en zonas visibles. *Guía sobre las normas de uso de las cookies*, AEPD.		El usuario debe poder ver la información sin ningún tipo de duda. Por ejemplo, poner el anuncio en la mitad de la pantalla y oscurecer el resto del portal puede ser una buena opción (el autor propone la idea de oscurecer la pantalla ya que, de este modo, se considera que no se puede «esquivar» el anuncio, como sucede, por ejemplo, en los anuncios de *cookies* que aparecen en la zona superior de la pantalla). Debe tenerse en cuenta el considerando (39): «Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales […].»
¿Cómo debe mostrarse la política de *cookies*?			Poner la «política de *cookies*» de forma destacada y separada (mediante un hiperenlace distinto, por ejemplo) del resto de la información sobre términos y condiciones de uso o sobre la política de privacidad. *Guía sobre las normas de uso de las cookies*, AEPD.		El RGPD no menciona nada al respecto.

* Dictámenes previos a la publicación del RGPD.

	Grupo de Trabajo 29*	LSSICE, art. 22	LOPD	Propuesta Reglamento e-Privacy	RGPD
¿Qué debe incluir la «política de privacidad»?	**Dictamen 15/2011** • Indicar el responsable del tratamiento. • Qué tipo de datos personales están siendo recogidos y la finalidad. • Si los datos se comunicarán a terceros.				• Indicar el responsable del tratamiento. • Los fines del tratamiento y la base jurídica. • Datos de contacto del DPO (artículo 13). • El tipo de datos personales que se recogen. • Si los datos se comunicarán a terceros.
El tiempo del consentimiento de las *cookies y la información al usuario*	**Dictamen 2/2010** Aunque se establece que el consentimiento no debe ser «para siempre», no señala mayores exigencias o características de ese tiempo. En la política de *cookies* no debe mostrarse ese tiempo.			No hay que indicar al usuario el tiempo de almacenamiento de las *cookies*, **pero solo se podrán instalar** de forma estrictamente necesaria y proporcionada al servicio (considerando 19).	Aunque se establece que el consentimiento no debe ser «para siempre» y no señala mayores exigencias o características de ese tiempo, sí se indica que debe ser el mínimo posible. En el aviso de *cookies* que el usuario ve, debe indicarse que los datos personales no se conservan más tiempo del necesario. Véanse los arts. 13.2.a), 14.2.a) y el considerando 39 del RGPD.
					• Indicar el riesgo que puede suponer para el usuario proporcionar esos datos (considerando 39 RGPD). • Indicar (de forma clara) cómo ejercer los derechos (art. 13.2.b).
Debe indicarse si se va proceder a una elaboración de perfiles				Señala que la tecnología nunca podrá proceder a la elaboración de perfiles de usuarios sin el consentimiento previo del titular de los derechos (considerando 15).	Dentro de las finalidades, debe indicarse si con los datos proporcionados se van a realizar perfiles y sus consecuencias (arts. 13.2.f y 14.2.g y considerando 60 RGPD).

* Dictámenes previos a la publicación del RGPD.

	Grupo de Trabajo 29*	LSSICE, art. 22	LOPD	Propuesta Reglamento e-Privacy	RGPD
Información que hay que suministrar para ejercer los derechos ARCO respecto de las *cookies*	**Dictamen 15/2011** No se hace referencia expresa a las *cookies*, pero en el momento de recabar datos de carácter personal de un usuario hay que indicar cómo revocar el consentimiento y solicitar la eliminación de esos datos.			Los métodos empleados para suministrar información y obtener el consentimiento del usuario final deben ser lo más sencillos posibles (considerando 22). Se deja la posibilidad de que esa autorización la pueda hacer el usuario con la configuración de su navegador.	No habla específicamente de las *cookies*, pero en el momento de recabar datos de carácter personal de un usuario hay que indicar cómo revocar el consentimiento y solicitar la supresión de los datos. Se incluye que debe indicarse con la mayor claridad y sencillez posible (artículo 13.2.b RGPD).
Extensión del consentimiento			Indicar si el consentimiento se presta solo para la página web en la que se está solicitando o si se facilita también para otras páginas web del mismo editor. *Guía sobre las normas de uso de las cookies*, AEPD.	El consentimiento se puede otorgar mediante la configuración del navegador del usuario. Según el punto 3.4: «…con esta opción se centraliza el consentimiento en programas o aplicaciones tales como los navegadores de internet, se incita a los usuarios a elegir su configuración de privacidad…».	No habla expresamente de *cookies*, pero debería indicarse si el consentimiento se presta solo para la página web en la que se está solicitando o si se facilita también para otras páginas web del mismo editor. Con arreglo al considerando 58, «...comprender si se están recogiendo, por quién y con qué finalidad…», se puede apreciar que saber la finalidad exacta engloba saber qué webs están recabando datos de carácter personal del usuario.

* Dictámenes previos a la publicación del RGPD.

3. Las aplicaciones móviles

3.1. Realidad y riesgos en las aplicaciones móviles

Se ha señalado que cada usuario descarga una media de 37 aplicaciones móviles (*apps*), tanto para iOS como para Android[32]. Muchas de tales aplicaciones solicitan del usuario su consentimiento para acceder a muchos más datos de los que realmente necesitan para desarrollar su función. Algunos de los datos que suponen un mayor riesgo para los intereses de los usuarios son:

(32)GT29 - *Opinion 02/2013 on apps on smart devices.* Adoptada el 27 de febrero de 2013 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>.

- Ubicación.
- Contactos.
- Identificadores de los dispositivos (tales como el **IMEI**, **IMSI**, **UDID** y el número de teléfono móvil).
- Identidad del interesado.
- Identidad del teléfono (es decir, el «nombre del teléfono[33]»).
- Tarjeta de crédito y datos de pago.
- Registros de llamadas telefónicas, SMS o mensajería instantánea.
- Historial de navegación.
- Correo electrónico.
- Credenciales de autenticación de servicios de la sociedad de la información.
- Fotos y vídeos.
- Biometría (p. ej., reconocimiento facial y plantillas de huellas dactilares).

(33)Cosa que sucede cuando el usuario etiqueta a su terminal con una denominación concreta «iPhone de Carlos»).

IMEI, IMSI y UDID

El IMEI (del inglés *international mobile station equipment identity*, 'identidad internacional de equipo móvil') es un código USSD pregrabado en los teléfonos móviles GSM que identifica al aparato de forma exclusiva en todo el mundo y es transmitido por el aparato a la red al conectarse a esta.

IMSI (del inglés *international mobile subscriber identity*, 'identidad internacional del abonado a un móvil') es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

UDID es el número de identificación de cada iPhone por el que, cuando se solicita, se garantiza que la información que va a recibirse solo puede ser usada en ese iPhone.

Los fabricantes de *apps* que desconozcan (o no tengan en cuenta) los requisitos de protección de datos pueden crear riesgos significativos para la privacidad de los usuarios. Los principales riesgos son la falta de transparencia y de concienciación en relación con los tipos de procesamiento de datos que una *app* puede realizar y la ausencia del necesario consentimiento por parte de los usuarios finales con anterioridad a tal tratamiento. Unas deficientes medidas de seguridad, la tendencia a la maximización de los datos[34] y la elasticidad de los propósitos para los que se recopilan datos personales contribuyen a incrementar los riesgos.

[34]Como concepto contrario a la «minimización de los datos» señalada en el RGPD.

En septiembre de 2014, la Agencia Española de Protección de Datos (junto con las autoridades de protección de datos de Alemania, Canadá, Francia, Italia y el Reino Unido) participó en el análisis coordinado para examinar las condiciones de privacidad de más de 1.200 aplicaciones móviles, entre las más populares. Dicho análisis, organizado por la Red Global de Control de la Privacidad (GPEN, por sus siglas en inglés), contemplaba el examen de *apps* de dispositivos Apple y Android, tanto gratuitas como de pago, públicas y comerciales, pertenecientes a categorías como el ocio, la salud, el ejercicio físico o la realización de transacciones bancarias. Dicho análisis era consecuencia de la popularidad y el alcance transnacional que han alcanzado las *apps* y los riesgos que puede implicar una utilización inadecuada de los datos personales de sus usuarios.

Red Global de Control de la Privacidad (GPEN)

La GPEN, creada para fomentar la cooperación transfronteriza entre autoridades, está compuesta por entidades nacionales y regionales de todo el mundo, entre las que se encuentran las principales autoridades europeas de protección de datos, el Supervisor Europeo de Protección de Datos y la Comisión Federal de Comercio (FTC, por sus siglas en inglés).

El análisis se centró en conocer:

- Los tipos de permisos solicitados por las aplicaciones.
- Si estos permisos eran excesivos en relación con el servicio prestado por la *app*.
- La manera en que se explicaba a los usuarios para qué se solicitaba su información personal y qué uso se planeaba dar a la misma.

Los resultados del análisis fueron, esencialmente, los siguientes:

- El 75% de las *apps* examinadas solicitaron uno o más permisos al usuario, siendo los más comunes la ubicación, la identificación del dispositivo, el acceso a otras cuentas, a la cámara y a los contactos.

- En el 59% de las *apps*, a los participantes no les resultó fácil encontrar las informaciones relativas a la privacidad antes de proceder a su instalación[35].

[35]Pudo constatarse que muchas aplicaciones ofrecían poca información sobre la finalidad de la obtención de los datos y remitían, en algún caso, a otras páginas web con políticas de protección de datos que no se adaptaban a la aplicación en cuestión o conducían a páginas en las que se solicitaba que el usuario iniciase una sesión.

- El 31% de las aplicaciones analizadas solicitaban permisos excesivos en relación a las funciones que presta la *app*.

- El 43% de las *apps* no habían adaptado sus políticas de protección de datos para ser leídas en pequeña pantalla.

- Solo un 15% de las *apps* suministraban información clara en relación con la forma, los fines y la divulgación de los datos personales recabados. (El 31% ofrecía información parcial, el 24% información inadecuada, y el 30% no ofreció información alguna sobre privacidad, aparte de los permisos.)

- Las aplicaciones que gozan de gran popularidad en el mercado se encontraban entre las que obtuvieron las mejores puntuaciones.

De todo lo anterior se deducen las siguientes claras amenazas para los usuarios de aplicaciones móviles:

1) Exceso de información personal solicitada por la *app*.

2) Escasa, nula o inadecuada información sobre la finalidad de los datos recabados y sus ulteriores tratamientos.

3) Escasa o nula protección tecnológica (y legal) de los datos recabados.

En cuanto a las *apps*, el Grupo de Trabajo del Artículo 29 ha señalado como más significativos los siguientes riesgos[36]:

[36]GT29 – Opinión 2/2013 citada.

- **Falta de transparencia**. Los desarrolladores de aplicaciones están limitados por las características de los sistemas operativos y las tiendas de aplicaciones para garantizar que el usuario final disponga de información completa en un momento relevante[37].

(37)Sin embargo, no todos los desarrolladores de aplicaciones aprovechan estas características, ya que muchas aplicaciones no tienen una política de privacidad o no informan de manera significativa a sus potenciales usuarios sobre el tipo de datos personales que la aplicación puede procesar y para qué.

- **Falta de consentimiento libre e informado**. Una vez que se descarga la aplicación, a menudo el consentimiento se reduce a una casilla de verificación que indica que el usuario final acepta los términos y las condiciones.

- **Deficientes medidas de seguridad.** Ello puede conducir al procesamiento no autorizado de datos personales (sensibles) cuando es la propia aplicación la que filtra datos personales al exterior.

- **Desconocimiento (accidental o deliberado) del principio de limitación del propósito.** Esto exige que los datos personales solo puedan ser recopilados y tratados con fines específicos y legítimos. Por desgracia, vemos con frecuencia cómo los datos personales recopilados por las *apps* se distribuyen a un número indeterminado de terceros por motivos indefinidos o etéreos tales como «investigación de mercado».

3.2. Actores implicados y sus responsabilidades

En lo que concierne al uso seguro de las aplicaciones móviles y a su privacidad, los actores implicados más significativos son:

1) Los **fabricantes de las *apps***, cuya responsabilidad alcanza a garantizar un desarrollo seguro de las aplicaciones, también desde el diseño.

En muchos casos, los fabricantes de *apps* móviles adoptarán la posición jurídica de responsables del tratamiento, toda vez que son ellos los que vienen a determinar los fines y medios del tratamiento, tal y como señala el art. 4.7 del RGPD.

La responsabilidad del fabricante de la *app* será considerablemente menor si no se procesan datos personales o si el fabricante ha adoptado las medidas técnicas y organizativas apropiadas para garantizar que los datos se anonimizan irreversiblemente antes de salir del dispositivo.

Sea como fuere, si el fabricante de la *app* tiene acceso a la información almacenada en el dispositivo, también debe aplicársele lo dispuesto en materia de consentimiento informado en el RGPD y lo que prevea la Propuesta de Reglamento e-Privacy.

2) Los **fabricantes de los dispositivos y de los sistemas operativos** sobre los que se ejecutarán las *apps*, cuya responsabilidad alcanza a permitir el acceso de las *apps* a las características de seguridad del dispositivo y del sistema operativo (SO).

Los fabricantes de los dispositivos y de los SO también deben ser considerados como responsables del tratamiento en el caso del tratamiento de cualquier dato personal que realicen para sus propios fines conjuntos, para cualquier dato personal que se procese para sus propios fines (por ejemplo, los datos de registro del usuario), para datos generados automáticamente por el dispositivo o para datos personales procesados por el sistema operativo o por el fabricante del dispositivo como resultado de la instalación o el uso de aplicaciones.

> Las aplicaciones que requieren acceso a la geolocalización deben utilizar los servicios de ubicación del SO. En dicho caso, este puede recopilar datos personales para proporcionar la información de geolocalización a las aplicaciones y también puede utilizar los datos para mejorar sus propios servicios de localización. Para este último propósito, el fabricante del SO debería ser considerado responsable del tratamiento.

Por otro lado, los fabricantes del SO y del dispositivo también son responsables de la interfaz de programación de aplicaciones (API, por sus siglas en inglés) que permite el procesamiento de datos personales por parte de las aplicaciones operativas en el dispositivo inteligente.

3) Los **distribuidores** (por ejemplo, las tiendas oficiales como Google Play o App Store, entre otras), cuya responsabilidad alcanza a garantizar que las aplicaciones dispuestas para su descarga respetan la privacidad de sus usuarios.

Actualmente, la mayoría de las aplicaciones que se ejecutan en dispositivos móviles (móviles inteligentes o tabletas) se descargan desde tiendas (oficiales y no oficiales) de aplicaciones. Aunque tales distribuidores puedan realizar controles (limitados) respecto de las aplicaciones de terceros que albergan, no puede obviarse el riesgo adicional para los usuarios finales. Por tanto, asumiendo que no todas las aplicaciones habrán pasado por los adecuados controles de seguridad, los usuarios finales (y las organizaciones a las que pertenecen, si se trata de dispositivos corporativos o se permite su uso) deberán tratar tales aplicaciones como no-confiables por defecto y adoptar para ellas las medidas de seguridad que se estimen convenientes.

Frecuentemente, las tiendas de aplicaciones procesan pagos para la descarga de *apps* que requieren el registro del usuario (nombre, dirección y datos financieros, por lo general). Estos datos pueden combinarse con otros sobre el comportamiento de compra, el uso y con aquellos leídos o generados por el dispositivo. Para el tratamiento de tales datos personales, dichos distribuidores deberán ser considerados igualmente como responsables del tratamiento.

4) Los propios **usuarios**, cuya responsabilidad reside en hacer un uso seguro de las aplicaciones descargadas, devienen actores al informarse sobre sus peculiaridades, también en materia de seguridad y protección de la información, y adoptarán la posición jurídica de «interesado» según se señala en el RGPD.

5) Terceras partes. Se trata, por ejemplo, de organizaciones que suministren métricas para propietarios de *apps* y anunciantes a través del uso de rastreadores incorporados por el desarrollador de aplicaciones dentro de estas. Uno de sus servicios es informar a los desarrolladores de aplicaciones acerca de qué otras aplicaciones utiliza un usuario a través de la recopilación de un identificador único. La compañía define los medios (es decir, los rastreadores) y los propósitos de sus herramientas antes de ofrecerlos a desarrolladores de aplicaciones, anunciantes y otros y, por lo tanto, actúa como responsable del tratamiento.

Finalmente, cabe señalar que las aplicaciones móviles juegan un papel significativo no solo en el desenvolvimiento personal de los ciudadanos, sino también como parte de los sistemas de información de las organizaciones (públicas o privadas). Así, en el contexto de las organizaciones, conviene recordar la posibilidad de acceso a los dispositivos móviles por parte de actores maliciosos que, habitualmente, persiguen un doble objetivo, acceder a los datos contenidos en el propio dispositivo y/o, a través de estos, acceder a la información corporativa. Todas las organizaciones, en base a esta realidad, deberán adoptar las medidas de seguridad pertinentes.

Algunas de las amenazas más frecuentes son[38]:

- Acceso físico no autorizado al dispositivo móvil.
- Acceso no autorizado a la información almacenada.
- Acceso no autorizado y manipulación de la información transmitida.
- Presencia de código dañino en las aplicaciones móviles.
- Uso de aplicaciones o servicios no aceptados por la organización.
- Uso inadecuado cuando el dispositivo se comparte para uso personal y profesional.
- Reutilización o reciclado de dispositivos móviles.
- Utilización de BYOD (*bring your own device*) en el seno de la organización.

(38)Como señala la Guía CCN-STIC 827 *Gestión y uso de dispositivos móviles*. Descargable desde <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html>.

3.3. Protección desde el diseño y medidas de seguridad

Sin repetir lo que se ha señalado hasta este momento y sin tener en cuenta la aplicación de otras normativas para sectores específicos[39], el RGPD contiene dos preceptos que consideramos relevantes para la protección de los datos tratados por las aplicaciones móviles, a saber:

El artículo 25 introduce el principio de *protección de datos desde el diseño*, obligando a los responsables y encargados del tratamiento a considerar la privacidad durante todo el ciclo de desarrollo de nuevos sistemas o procesos que usen datos personales.

Este principio es, en este contexto, exigible a los fabricantes de las *apps*.

3.4. Las medidas de seguridad

El artículo 32 del RGPD señala que los responsables y encargados del tratamiento deben aplicar medidas técnicas y organizativas adecuadas para garantizar la integridad de los sistemas y los procesos. Estas medidas deben contrarrestar los riesgos asociados al tratamiento de datos, tales como la destrucción accidental o deliberada, la pérdida, la modificación y la divulgación o el acceso no autorizado a datos personales, transmitidos o almacenados. Como hemos mencionado anteriormente, todas las organizaciones que tratan datos personales, responsables y encargados del tratamiento –a las que ahora se suman los fabricantes de *apps* móviles– deben desarrollar el correspondiente análisis de riesgos[40] y, en función del volumen de datos tratados, una evaluación de impacto[41].

Así pues, los fabricantes de *apps* deben poder demostrar que los principios y las medidas de seguridad, señalados respectivamente en los artículos 25 y 32, están adecuadamente contemplados e implantados y que se supervisa el cumplimiento del RGPD.

Visto lo anterior, es importante saber qué medidas pueden tomarse para garantizar la confidencialidad de los datos procesados por las *apps* en el contexto del RGPD.

(39) Por ejemplo, lo que dispone el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica, en relación con el desarrollo seguro de aplicaciones, y cuyo ámbito subjetivo de aplicación lo constituyen las entidades del sector público.

(40) considerando 83.

(41) considerandos 90 y 91 y art. 36.

Una de las vulnerabilidades más importantes de las *apps* es que pueden ser objeto de ingeniería inversa, lo que comportaría conocer su estructura y permitir el acceso no autorizado de terceros a la información almacenada en el dispositivo (contactos, registros, claves de cifrado, claves API, credenciales del usuario, etc.).

Ingeniería inversa

La ingeniería inversa es un proceso llevado a cabo con el objetivo de obtener información o un diseño a partir de un producto, con el fin de determinar cuáles son sus componentes, de qué manera interactúan entre sí y cuál fue el proceso de fabricación. (Fuente: Wikipedia).

Al objeto de contrarrestar la ingeniería inversa y asegurar los datos de los usuarios, las aplicaciones deben estar protegidas mediante la utilización de un doble enfoque:

- El código fuente de las aplicaciones móviles debe protegerse utilizando métodos de ofuscación y técnicas de cifrado. El fortalecimiento del código fuente garantiza que las aplicaciones móviles permanezcan ilegibles para los *hackers* que logren descompilarlos o desmontarlos.

- Los mecanismos de autoprotección de aplicaciones en tiempo de ejecución (RASP)[42] deben integrarse en las aplicaciones móviles para protegerlas del análisis dinámico y de los ataques *online* mediante la supervisión de la integridad del dispositivo en el que se ejecutan.

(42)*Runtime application self-protection*, 'autoprotección de aplicaciones de tiempo de ejecución', es una tecnología de seguridad que se crea o se vincula a una aplicación o a un entorno de ejecución de aplicaciones que es capaz de controlar la ejecución de estas con el fin de detectar y prevenir ataques en tiempo real.

RASP

Runtime application self-protection (RASP, 'autoprotección de aplicaciones de tiempo de ejecución') es una tecnología de seguridad que se crea o se vincula a una aplicación o a un entorno de ejecución de aplicaciones que es capaz de controlar la ejecución de aplicaciones con el fin de detectar y prevenir ataques en tiempo real.

(43)*Secure sockets layer* (SSL, 'capa de conexiones seguras') es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de internet. Recientemente, ha sido sustituido por TLS *transport layer security*, basado en SSL y totalmente compatible.

Además de lo anterior, deben adoptarse medidas para garantizar la confidencialidad de los datos en sí mismos, a saber:

- La utilización de SSL/TSL[43] asegura que las aplicaciones móviles se comunican con el servidor deseado, al tiempo que se protegen los datos en tránsito de ser interceptados por un ataque de *man-in-the-middle*.

- La criptografía *white-box*[44] es una solución recomendada para aplicaciones móviles que utiliza una clave de cifrado. La tecnología asegura que la clave no pueda ser desvinculada de la aplicación ni utilizada para descifrar datos almacenados o transmitidos.

(44)La criptografía *white-box* utiliza técnicas que permiten realizar un cifrado para que un atacante no pueda acceder a la clave, incluso aunque sea capaz de observar libremente la ejecución del código dinámico y conocer los detalles de los algoritmos utilizados.

SSL

SSL (*secure sockets layer*, 'capa de conexiones seguras') es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de internet. Recientemente, ha sido sustituido por TLS (*transport layer security*), basado en SSL y totalmente compatible.

White-box

La criptografía *white-box* utiliza técnicas que permiten realizar un cifrado para que un atacante no pueda acceder a la clave, incluso aunque sea capaz de observar libremente la ejecución del código dinámico y conocer los detalles de los algoritmos utilizados.

3.5. Obligaciones, recomendaciones y buenas prácticas

El Supervisor Europeo de Protección de Datos (SEPD), consciente de la problemática y los riesgos del uso de las aplicaciones móviles, y a la vista de lo dispuesto en el RGPD (y en otras normas), recogió en sus *Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions*[45] algunos principios que deberían observarse en el tratamiento de datos personales a través de aplicaciones móviles. Estos principios, originariamente dirigidos a las instituciones de la UE, son igualmente aplicables a cualquier organización e, incluso, a los propios ciudadanos. Por su interés, se incluye una recopilación/adaptación sumaria de los más significativos para nuestro propósito.

(45)Véase: EDPS. *Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions* <https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf>.

1) Analizar si la aplicación móvil procesa datos personales y cuáles. Los principios generales, las obligaciones y las recomendaciones que figuran en las Directrices del SEPD relativas a la protección de datos personales en la gestión de TI y la gestión de las instituciones de la UE[46] se aplican también al desarrollo y funcionamiento de las aplicaciones móviles.

(46)Véase: EDPS. *Guidelines on the protection of personal data processed through web services provided by EU institutions* <https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_web_services_en.pdf>.

2) La aplicación móvil debe recopilar solo aquellos datos que sean estrictamente necesarios para desarrollar sus funcionalidades legales, tal y como han sido comunicadas a los usuarios. Lo que la aplicación móvil debe hacer con los datos personales del usuario se tiene que comunicar claramente a este antes de la instalación de la aplicación móvil y no debe realizar ningún tratamiento para otros fines incompatibles. La guía del GT29 sobre el consentimiento muestra un ejemplo muy claro, en el que una *app* de edición fotográfica no podrá solicitar acceder al GPS del celular al no ser necesario para la finalidad del programa.

3) Informar adecuadamente al usuario y obtener su consentimiento antes de instalar cualquier aplicación en su dispositivo móvil. Todos los requisitos del consentimiento válido se aplican a las aplicaciones móviles. Los usuarios deben tener la opción de revocar su decisión en cualquier momento. El consentimiento debe recogerse antes de que se realice cualquier lectura o almacenamiento de información desde o hacia el dispositivo móvil. Un elemento esencial del consentimiento es la información proporcionada al usuario.

El tipo y la exactitud de la información proporcionada deben ser tales que permitan a los usuarios evitar la fatiga de información, mantener el control de los datos en su dispositivo móvil para proteger su propia privacidad. En particular, el consentimiento debe ser:

- **Específico.** La información proporcionada al usuario debe enfatizar el tipo de datos procesados y su propósito. Este aspecto debe de entenderse

de manera muy estricta. No valen generalidades. Si no se especifica para que se va usar un determinado dato solicitado por una *app*, esta no tendrá una finalidad clara y, por lo tanto, su creador/desarrollador estaría incumpliendo este apartado.

- **Manifestado mediante una acción expresa activa.** El procedimiento y las herramientas utilizadas para obtener el consentimiento deben permitir a los usuarios expresar sus deseos, sin margen de duda sobre su decisión. La guía del grupo de trabajo del GT29 sobre el consentimiento, señala que los movimientos físicos pueden calificarse como una clara acción afirmativa, como girar el teléfono inteligente, deslizar una barra de izquierda a derecha, etc. Sin embargo, el deslizamiento de una barra de arriba abajo, no se considerará como una clara acción afirmativa. Esto se debe a que el sujeto puede estar desplazándose a través de grandes cantidades de texto y dicha acción no es lo suficientemente inequívoca al poder pasarse por alto los avisos en Materia de Protección de Datos correspondientes.

- **Libremente prestado.** Los usuarios deben tener la oportunidad de hacer una elección real (p. ej., sin ser sometidos a presiones o sin que se presente con un enfoque de «lo-tomas-o-lo-dejas»). Si el usuario final se ve obligado a facilitar el acceso a Datos de Carácter Personal que no son estrictamente necesarios para ejecutar las funciones de la *app* para que esta funcione, se entiende que no ha prestado su consentimiento de forma libre.

Las aplicaciones móviles deben proporcionar a los usuarios:

- **Opciones reales para el tratamiento de datos personales.** La aplicación móvil debe solicitar el consentimiento granular para cada categoría de datos personales que procesa y para cada uso. Si el sistema operativo no permite una elección granular, la propia aplicación móvil debería implementarla. En este caso, la aplicación móvil debe informar claramente al usuario –antes de la instalación– de que, a pesar de la configuración del sistema operativo, el usuario tendrá la oportunidad de elegir a qué categoría de datos personales presta su consentimiento a través de las funcionalidades adecuadas proporcionadas directamente por la aplicación móvil.

- **Funcionalidades para revocar el consentimiento.** La aplicación móvil debe contar con funcionalidades para revocar el consentimiento de los usuarios para cada categoría de datos personales tratados y para cada uso. La *app* también debe proporcionar funcionalidades para eliminar los datos personales de los usuarios cuando se desee.

1) Proporcionar información adecuada a los usuarios para que puedan tomar decisiones informadas. El tamaño de la pantalla del dispositivo móvil y la interacción que los usuarios de *apps* móviles esperan tener con su dispositivo no deben impedir que tales usuarios reciban la información preceptiva. Por lo tanto, la aplicación móvil debería incluir:

- Una notificación por capas en la que la notificación inicial al usuario contenga la información esencial, de forma que cualquier información adicional esté disponible progresivamente a través de enlaces subsiguientes. La información debe ser fácilmente accesible y visible. Según la Guía de Transparencia del WP29, una vez que se instala la aplicación, la información sobre Protección de Datos nunca debe ser más que «dos golpes de distancia».

- Información contextual en tiempo real a través de iconos e imágenes para mostrar cuándo se tratan determinadas categorías de datos personales (por ejemplo, ubicación o datos biométricos) o si se están implementando ciertas medidas (por ejemplo, medidas de seguridad como el uso del cifrado). El vídeo y el audio también pueden utilizarse para informar y sensibilizar a los usuarios. No se podrá poner esa información junto con dibujos, gráficos, colores, símbolos, etc. que provoquen que el texto o enlace sea menos visible o difícil de encontrar en la página web.

2) Evaluar el impacto de la protección de datos cuando se descarga una *app* de una tienda de *apps*. Las aplicaciones móviles suelen distribuirse a través de tiendas de aplicaciones móviles que, a menudo, son propiedad de los mismos operadores que proporcionan los sistemas operativos y los propios dispositivos móviles. Debe tenerse en cuenta que estas tiendas de *apps*, en su condición de servicios de terceros, son responsables del tratamiento de los datos personales que tratan y, como hemos señalado, están sujetos a todas las obligaciones pertinentes.

3) Evaluar las características de procesamiento de datos de un componente de terceros o de un servicio de terceros antes de integrarlo en una aplicación móvil. Cuando se utilicen componentes o servicios de terceros en las aplicaciones móviles, debe evaluarse la forma en que estas herramientas recopilan y procesan datos personales, incluidas las transferencias de aplicaciones móviles a servidores gestionados por terceros. Los componentes de terceros incluyen *kits* de desarrollo de software (SDK, por sus siglas en inglés), marcos de programación y bibliotecas, ya sea para facilitar el desarrollo de las *apps* o para propósitos específicos, tales como mostrar fotos o mapas o comunicarse a través de redes sociales. Los servicios de terceros pueden recibir datos de la aplicación móvil y procesarlos (p. ej., para analizar el uso de la aplicación móvil) o pueden alojar contenido específico para la aplicación móvil en servido-

res centrales. Si se utilizan servidores terceros de fuera de la UE y del EEE, es imprescindible tener en cuenta las normas aplicables a las transferencias de datos a terceros países.

4) Aplicar la gestión apropiada del riesgo de seguridad de la información al desarrollo, la distribución y la operación de aplicaciones móviles. A través de un proceso de gestión de riesgos de seguridad de la información, deben identificarse los riesgos relevantes para los datos personales tratados por las aplicaciones móviles y tomar las medidas organizativas y técnicas apropiadas para proteger tales datos.

5) Adoptar procedimientos internos para el tratamiento de las brechas de seguridad, en particular, la notificación de los incidentes. Una brecha de datos en una aplicación móvil corporativa debe comunicarse internamente de acuerdo con la política de la organización, la gestión de la seguridad y la violación de datos. El DPD debe evaluar y documentar el incumplimiento y las medidas adoptadas en respuesta a futuras evaluaciones y verificaciones y considerar si es exigible informar a la autoridad competente e, incluso, a los propios usuarios.

6) Si se trata de una corporación, la organización debería **contar con políticas y procesos de desarrollo seguro para aplicaciones móviles**, incluidos los procedimientos de pruebas operativas y de seguridad. Seguridad desde el diseño. Un enfoque integrado de pruebas de seguridad desempeña un papel esencial en la fase de desarrollo (con análisis de código estático de seguridad y enfoques dinámicos como las pruebas de penetración).

7) Adoptar e implementar un proceso de gestión de vulnerabilidades apropiado para el desarrollo y la distribución de aplicaciones móviles. La organización debe mantener procedimientos para la gestión de las vulnerabilidades de las aplicaciones móviles instaladas en los dispositivos. La necesidad de actualizar las aplicaciones con los últimos parches de seguridad es una exigencia para las organizaciones y también para los usuarios individuales.

3.6. Tratamientos de datos de menores de edad

Cada vez es más frecuente que las *apps* móviles traten datos personales de menores de edad, toda vez que este colectivo es consumidor habitual de contenidos y aplicaciones para dispositivos móviles.

El RGPD contempla precisiones especiales más rigurosas para este tipo de tratamientos, como corresponde a las características de estos usuarios. Así, en relación con la fabricación, la distribución y el uso de aplicaciones móviles que tengan como destinatarios a los menores[47] debe tenerse en cuenta:

[47] Niños, en la terminología del RGPD.

1) Respecto de las condiciones aplicables al consentimiento del menor, en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un menor se considerará lícito cuando este tenga, como mínimo, 16 años. Si es menor de dicha edad, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. (Art. 8.1[48]).

(48)Señala el art. 8.3 RGPD que el apartado 1 del artículo 8 no afectará a las disposiciones generales del derecho contractual de los Estados miembros, como las normas relativas a la validez, la formación o los efectos de los contratos en relación con un niño.

El art. 8.1 *infine* del RGPD señala que los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años, edad que se ha tomado también como límite inferior en la versión pública, a la fecha de la redacción de estos módulos, del Proyecto de Ley Orgánica de Protección de Datos (art. 7 PLOPD).

2) En este sentido, el responsable del tratamiento hará esfuerzos razonables para verificar en los casos señalados en el art. 8.1 RGPD, que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el menor, teniendo en cuenta la tecnología disponible (artículo 8.2 del RGPD).

Una plataforma *online* deberá asegurarse de que los clientes menores de edad solo se suscriban a sus servicios con el consentimiento de sus padres o tutores, si son menores de 16 años. El responsable del tratamiento deberá seguir estos pasos:

1) Solicitar al usuario que indique si es menor o mayor de 13 años (en caso de España)

Si el usuario declara que está por debajo de la edad de consentimiento digital:

2) Se informará al niño que el padre/madre o bien el tutor necesita consentir o autorizar el tratamiento antes de que se le pueda dar el servicio. Se solicita al usuario que divulgue la dirección de correo electrónico del padre o madre o del tutor.

3) Se pondrá en contacto con el padre o tutor para obtener su consentimiento por correo electrónico para su tratamiento y tomará las medidas razonables para confirmar que el adulto tiene la autorización parental.

4) En caso de reclamaciones, la plataforma tomará cualesquiera otras medidas adicionales para verificar la edad del suscriptor.

Además se debe tener presente que:

a) La protección de los menores se extremará cuando se utilicen sus datos personales para fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, así como en la obtención de datos personales relativos a menores cuando se utilicen servicios ofrecidos directamente a un menor (considerando 38).

b) Será necesario el consentimiento del titular de la patria potestad o tutela del menor para la descarga de una *app*, salvo que esta se enmarque en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños (considerando 38).

c) Atendiendo al principio de transparencia, cualquier información y comunicación cuyo tratamiento afecte a menores debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender (considerando 58 y artículo 12.1 RGPD). Según la Guía de Trabajo del WP29 sobre transparencia, se deberán evitar los términos como «puede», «podría», «algo», «a menudo» y «posible».

d) Los riesgos para los derechos y las libertades de los ciudadanos se incrementan en el caso de personas vulnerables, es decir, los menores (considerando 75).

e) La posibilidad de que el responsable del tratamiento acuda al interés legítimo, en base al principio de licitud del tratamiento, queda mucho más limitada cuando los datos tratados son de un menor, en la medida que el art. 6.1.f) RGPD establece que «siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.»

f) En relación con los códigos de conducta, las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente reglamento, como en lo que respecta, entre otras cuestiones, a la información proporcionada a los menores y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el menor (artículo 40.2.g).