FACULTAD DE DERECHO

LA PROTECCIÓN DE LA PRIVACIDAD EN LOS NUEVOS DISPOSITIVOS ELECTRÓNICOS. ANÁLISIS DE RESOLUCIONES RECIENTES DE LA AEPD

Autor: Carlos Norzagaray Aguilar
5º E-3 C
Área de Derecho Civil

Tutor: Ana Soler Presas

Madrid
Abril 2020

RESUMEN

Instalar una aplicación móvil en nuestros teléfonos supone, por lo general, registrarse en la misma aportando una serie de datos personales. De la misma manera, la aplicación una vez instalada puede acceder a una gran cantidad de datos personales contenidos en nuestros dispositivos móviles, como nuestra galería de fotos, geolocalización o agenda de contactos, entre otros.

En numerosas ocasiones las Políticas de Privacidad de las aplicaciones no son claras o contienen contradicciones, lo que provoca que los usuarios suelan aceptar las condiciones de privacidad de las aplicaciones sin apenas leérselas por lo aburridas y complejas que pueden parecerles, siendo esta circunstancia aprovechada por los desarrolladores de aplicaciones para obtener el consentimiento a tratamientos de datos personales.

El nuevo Reglamento General de Protección de Datos ha traído consigo una intensificación de las sanciones por vulneraciones de la normativa, a la vez que obliga a los desarrolladores de aplicaciones y otras partes implicadas a confeccionar las medidas necesarias para garantizar la privacidad de sus usuarios desde el diseño de la propia aplicación.

El presente trabajo busca definir cuáles son los riesgos y retos que plantean a la privacidad los nuevos dispositivos móviles y sus aplicaciones, así como descubrir qué obligaciones tienen los desarrolladores de aplicaciones y otros agentes implicados en su creación para proporcionar a sus usuarios una plataforma digital que sea respetuosa con sus datos personales y puedan llevar a cabo un tratamiento de esos datos de forma legítima dentro de la legalidad.

PALABRAS CLAVE: RGPD, aplicación móvil, responsable del tratamiento, datos personales, consentimiento, interesado, encargado del tratamiento, dispositivos móviles.

ABSTRACT

Installing a mobile app on our phones involves as a general rule registering with it by providing a number of personal data. In the same way, once installed, the application can

access a large amount of personal data contained in our mobile devices, such as our photo gallery, geolocation or address book, among others.

On many occasions the Privacy Policies of the apps are not clear or contain contradictions, which causes users to accept the privacy conditions of the applications without hardly reading them because of how boring and complex they may seem, this circumstance being taken advantage of by the app developers to obtain consent for the processing of personal data.

The new General Data Protection Regulation has brought with it an intensification of sanctions for violations of the regulation, while at the same time encourages app developers and other parties involved to draw up the necessary measures to guarantee the privacy of their users from the design of the app itself.

This work seeks to define the risks and challenges posed to privacy by new mobile devices and their apps, as well as to discover what obligations app developers and other parties involved in their creation have to provide their users with a digital platform that is respectful of their personal data and can carry out a processing of these data in a legitimate way within the law.

KEYWORDS: GDPR, mobile app, data controller, personal data, consent, concerned, data processor, mobile device.

ÍNDICE

ÍNDICE DE ABREVIATURAS

AAPP: Administraciones Públicas

APP: Aplicación móvil

AEPD: Agencia Española de Protección de Datos

APDCAT: Autoridad Catalana de Protección de Datos

EM: Estados miembros de la Unión Europea

ET: Encargado del Tratamiento

GT29: Grupo del trabajo del artículo 29

LOPD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

RGPD: Reglamento UE 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

RT: Responsable del Tratamiento

UE: Unión Europea

CAPÍTULO I.

INTRODUCCIÓN

1. JUSTIFICACIÓN DEL TEMA DE ESTUDIO

Entre todos los avances que podemos destacar de la revolución tecnológica y digital que hemos vivido en las últimas dos décadas, llama la atención que hoy en día casi la totalidad de la población mundial dispone de un teléfono móvil o aparato similar que le permite estar en contacto con sus conocidos, pero también con sus desconocidos. Además, a medida que avanzan los años podemos observar como los menores de edad adquieren un teléfono móvil cada vez a edades más tempranas.

Como por todos es sabido, un dispositivo móvil alberga en su interior una gran cantidad de datos personales no sólo de su titular, sino de muchas otras personas, como pueden ser las fotos que se encuentren en la galería del teléfono o la lista de contactos que se guarde en el mismo. Hoy en día, el teléfono puede incluso generar a su vez datos personales como consecuencia de su uso, por ejemplo, si el dispositivo recoge la geolocalización del usuario o si almacena el historial de navegación de su titular. En definitiva, podemos afirmar que un teléfono móvil es un depósito inmenso de datos personales que se actualiza constantemente.

Las aplicaciones que nos descargamos en nuestros teléfonos casi siempre nos solicitan que rellenemos una serie de datos personales para poder hacer uso de las mismas. No obstante, debemos tener en cuenta que una aplicación móvil al instalarse en el teléfono, puede tener acceso a una gran cantidad de datos personales que no hayamos decidido facilitar, como nuestros datos de geolocalización o micrófono. Asimismo, no es de extrañar que podamos haber accedido a que la aplicación use estos datos personales sin habernos dado cuenta, ya que ha sido hasta ahora una práctica frecuente por parte de los desarrolladores el presentar Políticas de Privacidad farragosas e incomprensibles por el usuario medio que no está familiarizado con el lenguaje jurídico, dando lugar a consentimientos otorgados de manera ilegítima con tal de avanzar en el uso de la

aplicación, lo que puede resultar intolerable desde el punto de vista de protección de la intimidad.

Es por ello por lo que considero necesario estudiar los desafíos que los nuevos dispositivos móviles y sus aplicaciones plantean a la privacidad de sus usuarios, comprender los riesgos que el uso de esta nueva tecnología supone para los usuarios, conocer los límites que los desarrolladores tienen a la hora de tratar nuestros datos personales y los requisitos y condiciones que deben cumplir para evitar incurrir en responsabilidad.

2. OBJETIVOS

El presente trabajo pretende definir cuáles son los riesgos a los que se enfrenta el usuario de una aplicación móvil y qué normativa los ampara en la protección de su derecho a la intimidad. Asimismo, este trabajo pretende dar respuesta a las medidas que deben adoptar los desarrolladores de una aplicación móvil y otros sujetos relacionados con las mismas para lograr un cumplimiento estricto de la normativa, velar por la privacidad de sus usuarios y evitar todos los riesgos mencionados. Asimismo, para dar un enfoque práctico al presente trabajo se analizará el papel que tiene la AEPD en este ámbito comentando alguna de sus resoluciones más importantes en la que se puede observar la incidencia que tiene la normativa de protección de datos en casos reales, así como las consecuencias derivadas de su incumplimiento. Por último, como consecuencia de la pandemia que ha tenido lugar en la realización del presente trabajo, analizaremos aspectos relacionados con la protección de la privacidad en tiempos del COVID-19.

Debemos señalar que el Dictamen 02/2013 del Grupo de Trabajo del artículo 29 se pronunció sobre gran parte de las cuestiones que se tratan en el presente trabajo. Sin embargo, dicho Dictamen se elaboró cuando aún estaba en vigor la Directiva 95/46/CE, la cuál se redacto en una época en la que los teléfonos móviles aún no existían, por lo que la mayoría de sus consideraciones tendrán que actualizarse conforme a los fundamentos

y principios del nuevo Reglamento General de Protección de Datos para dar respuesta a riesgos que han surgido conforme ha avanzado la tecnología móvil.

3. METODOLOGÍA

La metodología que se ha seguido en el presente trabajo consiste en un primer lugar, en aproximarnos a los principios y conceptos de protección de datos que serán más relevantes en el ámbito de los dispositivos móviles. Para ello, partiremos de la ley que los regula y analizaremos las posturas de diferentes autores con motivo de estos fundamentos. Una vez comprendido este marco conceptual a nivel general, nos sumergiremos en el ámbito concreto de los dispositivos móviles explicando los riesgos, desafíos y posibles soluciones que se plantean en este ámbito. Por último, para comprender la aplicación práctica que tiene el presente trabajo observaremos como actúa la AEPD en la resolución de casos de privacidad en dispositivos móviles.

La búsqueda de información se realizará a través de buscadores y bases de datos que la universidad nos facilita como Dialnet o Aranzadi. En ellos encontraremos bibliografía tal como artículos de revistas jurídicas, comentarios doctrinales o extractos de manuales jurídicos. Asimismo, debido a que en el presente ámbito la jurisprudencia es más bien escasa, se consultará en su lugar distintos Dictámenes emitidos por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, así como informes, resoluciones y comentarios de la AEPD. A su vez, cabe destacar que para salvar la dificultad que puede suponer encontrar doctrina posterior al RGPD y a la nueva LOPD, se han adquirido manuales jurídicos que completan dicha búsqueda de información. Por último, debido a que en algunas partes del trabajo tratamos algunos temas de actualidad, se utilizarán artículos de prensa que ayudarán a obtener diferentes puntos de vista del tema en cuestión.

4. ESTRUCTURA DEL TRABAJO

El presente trabajo se estructura en seis capítulos. El primero lo acabamos de ver y consiste en una introducción en la que se expone brevemente el interés del tema de estudio, los objetivos, la metodología y su estructura. El segundo capítulo contiene una revisión del marco regulatorio aplicable al ámbito de la protección de la privacidad en dispositivos móviles. Dedicamos el tercer capítulo al estudio de los conceptos y principios más relevantes para el tema de estudio teniendo en cuenta la entrada en vigor en 2018 del nuevo RGPD que da lugar a un cambio en el panorama de la protección de datos.

El cuarto capítulo es el núcleo del presente trabajo; en él desarrollamos todos los riesgos que plantean los nuevos dispositivos móviles a la privacidad, realizamos un estudio individualizado de cada uno de ellos y analizamos de forma exhaustiva el papel que tienen los diferentes sujetos implicados en el desarrollo de las aplicaciones y las funciones y responsabilidad que corresponde a cada uno de ellos. En el quinto capítulo, podremos observar casos recientes de protección de la privacidad en aplicaciones móviles y cómo está afectando la pandemia COVID-19 a este ámbito. Por último, concluimos con un balance general del trabajo, una serie de recomendaciones o prácticas que se deducen del presente trabajo que ayudarán a los desarrolladores a respetar la legalidad de sus aplicaciones móviles y una postura crítica sobre las resoluciones estudiadas.

CAPÍTULO II.

MARCO REGULATORIO

1. MARCO REGULATORIO DE LA PROTECCIÓN DE LA PRIVACIDAD EN APLICACIONES MÓVILES

De la lectura del Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, podemos extraer que el marco jurídico aplicable en la UE al presente ámbito es la Directiva sobre protección de datos (95/46/CE). No obstante, dicha directiva se encuentra actualmente derogada por el Reglamento Europeo de la Protección de Datos (RGPD), desde su entrada en vigor el 25 de mayo de 2018, por lo que será, el presente Reglamento,

el marco jurídico aplicable a la privacidad en las aplicaciones móviles. En este sentido, el Considerando 171 establece:

"La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor."

Por tanto, del presente Considerando podemos extraer que habrá tratamientos de algunas aplicaciones, anteriores a la entrada en vigor del RGPD a los que seguirán siendo de aplicación las disposiciones de la Directiva, pero que deberán ajustarse a las disposiciones del RGPD antes del 25 de mayo de 2020.[1]

En cuanto al ámbito territorial, en palabras de Fernández Acevedo (2018, p.242) "la normativa europea en materia de protección de datos es aplicable con independencia a dónde esté ubicado el desarrollador de la aplicación o la tienda que la comercialice". La justificación que utiliza el autor al respecto, es que estos programas suelen utilizar medios ubicados en la UE, como son los propios terminales de los usuarios.

También es de aplicación, en el ámbito español de las aplicaciones móviles, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD), que supone la adaptación del RGPD al ordenamiento jurídico español.

Asimismo, según el Dictamen 02/2013 resulta de aplicación la Directiva 2002/58/CE sobre la privacidad electrónica. No obstante, debemos apuntar que dicha Directiva se encuentra actualmente derogada por la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de datos personales en el sector de las comunicaciones electrónicas (Reglamento e-Privacy).

[1] Art 5 C.C: *"... si los plazos estuviesen fijados por meses o años, se computarán de fecha a fecha."*

Siguiendo con el marco legal aplicable, en una escala jerárquicamente inferior, podemos encontrar el Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, que será comentado en el siguiente apartado.

Por último, debemos destacar diversas notas técnicas publicada por la AEPD como son: *"El deber de informar y otras medidas de responsabilidad proactiva en Apps para dispositivos móviles."*, o *"Guía para el cumplimiento del deber de informar",* que amplían y completan las recomendaciones aportadas por el Dictamen 02/2013 estableciendo directrices específicas en el caso de las aplicaciones para dispositivos móviles.

2. DICTAMEN SOBRE LA PRIVACIDAD EN LAS APLICACIONES MÓVILES O APPS DE 27 DE FEBRERO DE 2013

El estudio más exhaustivo llevado a cabo sobre la privacidad en las aplicaciones móviles fue elaborado por el Grupo de Trabajo del artículo 29 de la Directiva sobre protección de datos (95/46/ CE) bajo el nombre de *"Dictamen sobre las aplicaciones de los dispositivos inteligentes".* En palabras de Álvarez Hernando (2015) el presente dictamen "detalla las obligaciones específicas para los desarrolladores y creadores de aplicaciones, las tiendas, los fabricantes de sistemas operativos y dispositivos y los proveedores de servicios publicitarios." Además, en dicho dictamen se analizan los riesgos que las aplicaciones móviles plantean a la privacidad como consecuencia de la utilización inadecuada de los datos personales de los mismos.

El GT29 se forma en virtud del artículo 29 de la Directiva (95/46/CE), derogada por el RGPD, que establecía lo siguiente en su apartado 1: *"Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado «Grupo». Dicho Grupo tendrá carácter consultivo e independiente."*

El artículo 30 de la Directiva se encargaba de enumerar sus funciones, entre la que se encontraba en el apartado c, el asesoramiento a la Comisión sobre cualesquiera *"medidas adicionales o específicas que deba adoptarse para salvaguardar los derechos y*

libertades de las personas físicas en lo que respecta al tratamiento de datos personales." Por tanto, el GT29, elabora dicho Dictamen en ejercicio de sus funciones.

No obstante, tras la entrada en vigor del RGPD se forma el Comité Europeo de Protección de Datos, un órgano de coordinación entre autoridades que sustituye al GT29. Sus funciones se encuentran desarrolladas en el artículo 70 del RGPD y en palabras de López Calvo (2018, p. 630) "su labor de cohesión no es subsidiaria o alternativa, sino que el Comité debe emitir directrices, recomendaciones y buenas prácticas en múltiples aspectos.[2]"

Por último, según informa la APDCAT, el Comité Europeo de Protección de Datos, en la sesión de 25 de mayo de 2018, asumió las directrices sobre el RGPD aprobadas por el GT29, por lo que podemos concluir que el Dictamen sigue estando vigente a pesar de que el Grupo que lo emitió haya sido derogado. No obstante, no debemos olvidar que la redacción de dicho Dictamen se realizó siguiendo lo dispuesto en la Directiva (95/46/ CE), por lo que, su lectura tendrá que realizarse tomando en consideración la nueva regulación del RGPD.

CAPÍTULO III.

ESPECIAL TRASCENDENCIA DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

1. NECESIDAD Y JUSTIFICACIÓN DEL NUEVO MODELO EUROPEO DE PROTECCIÓN DE DATOS PERSONALES

Según Cervera-Navas (2018, p. 70) el nuevo RGPD tiene su principal razón de ser en el enorme crecimiento tecnológico y digital que ha tenido lugar en la última década. Este autor señala que la Directiva 95/46/CE no era un modelo previsto para la revolución

[2] Entre los que se encuentran: la elaboración de dictámenes (art. 64) y decisiones vinculantes (art.65)

tecnológica que hemos vivido y que ha incorporado algunos fenómenos en aquella época desconocidos como el Big Data o el Internet de las cosas.

De hecho, en 1995, cuando entró en vigor la Directiva, apenas existían dispositivos inteligentes como los teléfonos móviles o los ordenadores y, los pocos que existían tenían sistemas operativos y softwares muy básicos, por lo que ha sido necesaria esta nueva regulación para adaptar la realidad jurídica a las nuevas tecnologías.

El nuevo RGPD incorpora una serie de principios y conceptos que anteriormente no estaban previstos en la Directiva 95/46/CE y que serán objeto de estudio en el presente capítulo. No obstante, autores como García Herrero citado por Biurrun Abad (2017) sostienen que el principio más relevante de esta nueva regulación es el "Accountability", o lo que es lo mismo, el principio de proactividad o responsabilidad activa en el cumplimiento de la normativa de protección de datos, lo que supone que, a partir de ahora, "corresponderá a las empresas acreditar que cumplen el RGPD, en lugar de a la Administración". Al mismo tiempo, destaca en esta nueva regulación la intensificación de las sanciones administrativas para el caso de incumplimiento de la normativa, ya que, con el régimen anterior, no existía en la UE un régimen sancionador común, y esto daba lugar a un grado elevado de impunidad ante infracciones cada vez más numerosas, según señala Rallo Lombarte (2018, p. 77).

En palabras del último autor mencionado, estamos ante un Reglamento que incorpora una gran cantidad de nuevos "derechos digitales" que han surgido a raíz de la revolución tecnológica en la que seguimos sumergidos. Es por ello, por lo que presento en los apartados siguientes una aproximación a los conceptos y principios, en su mayoría novedosos o actualizados del RGPD, que son a mi parecer, más relevantes en el ámbito de la protección de la privacidad en dispositivos móviles.

2. CONCEPTOS RELEVANTES EN EL RGPD

El artículo 4 del RGPD contiene un glosario de definiciones cuyo objetivo es facilitar la comprensión del resto del articulado. La Directiva 95/46/CE también ofrecía una serie de definiciones, que en el presente Reglamento se han actualizado como consecuencia del uso y la jurisprudencia europea y nacional. El objetivo del presente apartado no es explicar todos y cada uno de los conceptos y principios recogidos, sino aquellos que considero más relevantes de cara al estudio de la privacidad en las aplicaciones móviles y dispositivos inteligentes; es por ello por lo que desarrollaré aquellas definiciones que considero oportunas que se comprendan a nivel general, para el ulterior análisis en el ámbito concreto del presente trabajo.

2.1. Concepto de dato

A efectos jurídicos, es importante destacar que los datos personales están protegidos por la Ley de Protección de Datos a diferencia de las "obras" intelectuales o creaciones originales literarias, artísticas o científicas, que se encuentran en su caso, protegidas por la Ley de Propiedad Intelectual, tal y como señala Adsuara Varela (2018, p.165) quién nos ofrece la etimología de la palabra dato: "«Dato» viene de «datum», participio pasado del verbo latino «dare» (dar) y significa «algo que nos viene dado»." Según dicho autor, existen numerosas clasificaciones de datos, aunque jurídicamente la más importante es la que distingue los datos personales de los que no lo son y que veremos a continuación.

2.1.1. Dato personal

El RGPD en su artículo 4.1 establece la siguiente definición de dato personal:

"«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un

identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"

Por tanto, el concepto de dato personal no solo abarca aquellos que identifican a una persona de forma directa y aquellos que lo hacen de manera indirecta, recibiendo estos últimos el nombre de «identificadores[3]», sino que también abarca según Adsuara Varela (2018, p. 166) "cualquier dato relacionado con una persona identificada o identificable."

Se considerarán datos personales, aunque sea necesario poner en relación los datos que se tengan para llegar a identificar a la persona en cuestión, excepto cuando ello "suponga un esfuerzo desproporcionado en cuanto a los medios o el tiempo que se ha de emplear para llegar a identificarle", en palabras de Muñoz Ontier (2018, p.340).

En el mismo sentido se pronunció el GT29 en su Dictamen 4/2007 sobre el concepto de datos personales, cuando afirma que *"para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona."* Se llega a la conclusión, en el presente Dictamen, que, si teniendo en cuenta el conjunto de los medios que puedan ser razonablemente utilizados, no es posible singularizar a un individuo, entonces, *"la persona no debe ser considerada como «identificable» y la información no debe catalogarse como «datos personales»."*

En relación con lo anterior, De Miguel Asensio (2015) considera que es necesario tener en cuenta que el hecho de que un elemento se considere suficiente o no, para identificar a una persona "puede depender del contexto" y también afirma que "la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos, en particular en Internet." Con esta última afirmación, el autor hace referencia a elementos que pueden resultar identificativos de personas en Internet, como las direcciones IP o las direcciones de correo electrónico.

[3] No existe una lista taxativa de identificadores, sino que bastará con que sirvan para la individualización e identificación de una persona concreta.

Sin ánimo de extendernos demasiado, adelantamos que tanto la AEPD como el antiguo Grupo de Trabajo, en el Dictamen 4/2007, han considerado tanto la dirección IP la dirección de correo electrónico como datos sobre personas identificables. La Audiencia Nacional en su Sentencia de 25 de mayo de 2006 también ha considerado la dirección de correo como dato personal ya que *"esa dirección del correo electrónico aparecerá vinculada a un dominio concreto, por lo que sólo será necesario consultar al servidor en que se gestione dicho servicio."*

Debemos destacar que Muñoz Ontier (2018, p. 340-341), habla de los datos personales seudonimizados[4] y la información anónima. Respecto de los primeros, considera que deben considerarse "información sobre una persona física identificable", mientras que de los segundos opina que "no les son aplicables los principios de protección de datos, ya que se trata de información que no guarda relación con una persona física identificada o identificable."

Adsuara Varela (2018, p.166) no comparte la calificación de los seudónimos como dato personal y siguiendo lo dispuesto en el RGPD establece que un seudónimo no podrá ser calificado como dato personal "siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable", ya que en su opinión, "de nada vale la seudonimización de unos datos personales, si éstos se pueden cruzar con otros para revertir la disociación y reidentificar así al titular de los mismos."

Por tanto, la conclusión que sacamos comparando las posturas de los dos autores, es que un seudónimo no podrá ser considerado dato personal si la información adicional para atribuir dicha información al «interesado», no es accesible porque se encuentre sujeta a medidas técnicas que impidan realizar la asociación necesaria para identificar a la persona. En caso contrario, si es posible realizar dicha asociación, un seudónimo si será considerado dato personal.

[4] Son aquellos que dependen de información adicional para atribuírselos a una persona física.

En definitiva, podemos afirmar que no estaremos ante un dato personal y, por tanto, no estará protegido cuando no se pueda asociar a una persona física determinada, bien porque no esté identificada, bien porque no se la pueda identificar. Y esto con independencia de que suceda *«ab initio»* o de manera sobrevenida, como bien señala Adsuara Varela (2018, p. 166).

Por último, cabe cuestionarse que sucede cuando nos encontramos ante datos profesionales de contacto, que en numerosas ocasiones coincidirán con los datos personales del sujeto en cuestión. En este sentido debemos apuntar que el RGPD no se ha pronunciado expresamente sobre este asunto, pero si lo ha hecho la LOPD en su artículo 19 estableciendo que dicho tratamiento *"se presumirá amparado en el artículo 6.1 f) del Reglamento (UE) 2016/679…"* Como podremos observar más adelante, la base jurídica que legitima el presente tratamiento es un interés legítimo.

No obstante, la LOPD supedita este tratamiento a dos requisitos: *"i) que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional; (ii) que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios."* Según Castrillo de la Fuente (2018), dentro del primer requisito se incluirían datos como números de teléfonos privados o correos personales, que se utilicen profesionalmente. No obstante, según señala Cives (2017) de este artículo no podemos extraer que la LOPD no sea aplicable al tratamiento de estos datos profesionales, sino que "se trata de una excepción a la necesidad de contar con el consentimiento de los interesados", siendo necesario el cumplimiento de otras obligaciones, por ejemplo, el deber de informar. (Castrillo de la Fuente, 2018).

2.1.2. Datos personales en aplicaciones móviles

Siguiendo con el Dictamen 02/2013, podemos considerar datos personales todos aquellos almacenados en dispositivos inteligentes o generados a partir de ellos, que nos permitan identificar de forma directa o indirecta a la persona física o interesado. Así el

considerando 24 de la Directiva 2002/58/CE, establecía que tanto los equipos terminales de los usuarios de redes de comunicación electrónica, como la información almacenada en dichos dispositivos *"forman parte de la esfera privada de los usuarios que debe ser protegida."*

El Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes nos ofrece una serie de ejemplos de datos personales en aplicaciones móviles entre los que se encuentran, localización, lista de contactos, ID del teléfono móvil, identidad del usuario del teléfono, historial de navegación, correo electrónico, fotografías, vídeos, datos de tarjetas de créditos y datos biométricos[5], entre otros.

Como hemos mencionado anteriormente, es irrelevante que los datos pertenezcan para identificar al dueño del dispositivo o a un tercero, ya que generalmente en los dispositivos móviles y aplicaciones se almacenan datos concernientes a muchas personas[6]. Lo importante para calificarlos como datos personales es que se pueda identificar directa o indirectamente a la persona física titular de dichos datos.

2.2. Sujetos que intervienen en el tratamiento de datos

El RGPD nombra a una serie de sujetos que participan en el tratamiento de datos personales. Conceptos como "responsable del tratamiento", "encargado del tratamiento" o "interesados" aparecerán a lo largo del estudio sobre el tratamiento de datos en dispositivos móviles, por lo que es fundamental comprender el significado de dichos conceptos a nivel general, para poder entender qué funciones desempeñan y que responsabilidades tienen en concreto en el ámbito al que nos referimos.

2.2.1. Responsable del tratamiento

[5] Actualmente es común utilizar la huella dactilar, voz o reconocimiento facial para acceder al móvil, en lugar de la clásica contraseña.
[6] Por poner un ejemplo, guardo 521 contactos de terceras personas en mi teléfono móvil.

La figura del RT viene regulada en el artículo 4 RGPD como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento."* La presente definición no ha variado con respecto a la que ofrecía la antigua Directiva 95/46/CE y fue en su día, objeto de estudio por el GT29 en el Dictamen 1/2010.

Según el mencionado Dictamen y autores como Vidal Laso y Aparicio Salom (2019) la obligación principal del RT consiste en "asignar la responsabilidad"; esto es, determinar quién debe ser responsable de ajustar el tratamiento de datos a la normativa europea y nacional y velar porque los interesados puedan ejercitar sus derechos. Así, el RT puede decidir que los datos se traten en el seno de su organización e influencia, o, por el contrario, delegar una parte o la totalidad del tratamiento de datos a otro sujeto o unidad organizativa, que recibirá el nombre de "encargado del tratamiento".

El artículo 24 del RGPD establece como obligación del responsable del tratamiento la aplicación de las *"medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al presente reglamento."* Medidas que, según Costa Hernandis (2018, p. 421) deben establecerse en función del riesgo, probabilidad y gravedad que entrañen a los derechos y libertades de las personas físicas.

De todos los sujetos que intervienen en el tratamiento de datos personales, el RT es quien tiene una libertad y un margen de maniobra mayor para decidir sobre los medios y fines del tratamiento, tal y como dispone el Dictamen 1/2010. Es importante destacar que el RT se identificará por criterios de hecho, caso por caso, atendiendo a las relaciones contractuales que existan, pero sobretodo al grado de control y dominio sobre los datos por parte de dicho sujeto. Incluso *"el propio hecho de que alguien determine cómo se procesan los datos personales",* puede dar lugar a la calificación de un sujeto como RT, aún sin existir relaciones contractuales.

Por último, la determinación de un sujeto como RT también puede derivar de una atribución legal explícita o una atribución jurídica implícita, tal y como señala el Dictamen 1/2010.

2.2.2. Encargados del tratamiento

La figura del ET está regulada en el artículo 28 del RGPD que en su apartado 1 establece: *"Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado."*

Por tanto, se trata de una persona que trata datos personales por cuenta del RT y lo hace según señalan Vidal Laso y Aparicio Salom (2019, p.17) a través de un contrato de arrendamiento de servicios, por el cuál el ET siguiendo unas determinadas instrucciones, ejecutará el tratamiento de los datos personales por cuenta del responsable.

El artículo 28.9 RGPD establece que el contrato o acto jurídico por el que se nombre a un ET *"constará por escrito, inclusive en formato electrónico."* No obstante, el Dictamen 1/2010 no considera el presente contrato como decisivo para la existencia de una relación jurídica entre responsable y encargado, ya que, en este caso también se debe realizar un análisis de los elementos de hecho, de tal manera que se puede exigir responsabilidad respecto de alguien que actúe como ET sin la existencia de un contrato que lo faculte como tal.

La responsabilidad del ET se determinará atendiendo al grado de cumplimiento de las instrucciones otorgadas por el responsable. En este sentido, el artículo 82.2 del RGPD establece lo siguiente: *"Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente*

Reglamento dirigidas a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable." En el mismo sentido se pronuncia De Miguel Asensio (2015, p.56) al afirmar que el ET será considerado como responsable del tratamiento si, extralimitándose de las instrucciones recibidas, comunica los datos a terceras personas o los utiliza para fines distintos para los que los recibió.

No obstante, según señala Brito Izquierdo (2018, p. 650) se trata de una presunción de responsabilidad respecto de la que cabe prueba en contrario, ya que, "el responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios."

Según Vidal Laso y Aparicio Salom (2019, p. 19), la antigua LOPD daba un mayor margen de maniobra al encargado del tratamiento para decidir sobre los medios técnicos y organizativos del tratamiento, correspondiendo la determinación de los fines en todo caso, al RT. No obstante, según los mencionados autores, con el nuevo RGPD "se exige que se determinen todos y cada uno de los servicios que habrán de realizarse por el encargado y que los que no estén previstos se autoricen por el responsable previamente a su ejecución."

Por último, es necesario destacar que el ET debe asegurarse de que las órdenes que recibe del responsable se ajustan a la normativa de protección de datos, porque de lo contrario, podría responder de las actividades realizadas en contra de la normativa de protección de datos, incluso cuando estas actividades hayan sido ordenadas por el responsable, según señalan Vidal Laso y Aparicio Salom (2019, p. 21).

2.2.3. Corresponsable del tratamiento

A lo largo del RGPD podemos encontrar algunas expresiones que nos inducen a pensar que puede haber más de un responsable en el tratamiento de unos datos concretos. Así, el

artículo 4 RGPD al introducir el concepto de responsable del tratamiento se refiere a aquellos *"que solo o junto con otros, determine los fines y medios del tratamiento."*

El artículo 26 RGPD nos introduce el concepto de "corresponsable del tratamiento" refiriéndose a aquellos responsables que *"determinen conjuntamente los objetivos y los medios del tratamiento"*. Del presente artículo también se desprende que corresponde a los corresponsables la determinación de mutuo acuerdo y de modo transparente de las responsabilidades respectivas en el cumplimiento de las obligaciones derivadas de dicho Reglamento. El Dictamen 1/2010, argumenta que los corresponsables tienen un margen considerable de flexibilidad a la hora de asignar sus respectivas responsabilidades, pero advierte de que un elevado número de responsables puede derivar en "complejidades indeseadas y a una posible falta de claridad en la atribución de responsabilidades."

El grado de responsabilidad que se asignen los corresponsables del tratamiento debe "reflejar la realidad del tratamiento de datos subyacente" tal y como dispone el mencionado Dictamen, ya que, de lo contrario, se tendría que acudir a las circunstancias de hecho para determinar en qué medida cada parte es responsable.

Por último, del artículo 26.3 y del artículo 82.4 RGPD se desprende la responsabilidad solidaria de los corresponsables del tratamiento, para garantizar la indemnización del que sufre el daño, debiendo ser considerada cada parte responsable de la "totalidad de los daños y perjuicios", tal y como señala Brito Izquierdo (2018, p. 651), sin perjuicio del derecho del que dispone el que satisface la indemnización para reclamar a los demás responsables la parte correspondiente a su responsabilidad.

2.2.4. Tercero

El concepto de "tercero" queda regulado en el artículo 4 RGPD como la *"persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas*

para tratar los datos personales bajo la autoridad directa del responsable o del encargado." Según Vidal Laso y Aparicio Salom (2019, p.7), el tercero es aquel que trata datos sin que pueda determinar sus medios ni sus fines, a diferencia de lo que ocurre con el RT. Por otro lado, la diferencia principal del tercero con respecto al ET, es que, mientras el encargado trata los datos por cuenta del responsable sin tener ningún interés respecto del resultado, más allá de la compensación económica que pueda recibir del responsable, el tercero lo hace por cuenta propia y teniendo algún interés legítimo "respecto de los fines perseguidos mediante el tratamiento de datos."

En resumen, el tercero es aquel que trata los datos por cuenta propia teniendo algún interés legítimo respecto de los fines, pero sin estar capacitado para determinar los medios y los fines del tratamiento. Por último, es necesario destacar que el RT tiene la obligación de informar previamente a los interesados de la cesión de datos que se va a realizar a terceros, en virtud del artículo 15 RGPD.

2.2.5. Interesado

En cuanto al "interesado" podemos definirlo como aquella persona física identificada o identificable a la que pertenecen los datos personales que van a ser tratados por el responsable del tratamiento o, en su caso, por el encargado del tratamiento. Desde un punto de vista general, los derechos del interesado quedan regulados en los artículos 12-19 del RGPD.

No obstante, debido a la multitud de especialidades y ámbitos a los que se aplica hoy en día la normativa de protección de datos, los derechos del interesado varían de una a otra, por lo que considero oportuno centrarnos en los derechos del interesado en el ámbito de las aplicaciones móviles, los cuáles serán desarrollados más adelante.

3. PRINCIPIOS DE PROTECCIÓN DE PRIVACIDAD DEL RGPD APLICADOS AL ÁMBITO DE LOS DISPOSITIVOS MÓVILES

Del mismo modo que hicimos en el apartado anterior con los sujetos que participan en el tratamiento de datos personales, en el presente apartado explicaremos los fundamentos del RGPD que son más relevantes en el ámbito de los dispositivos móviles.

3.1. Licitud del tratamiento

El principio de licitud del tratamiento hace referencia a aquellas premisas que dan cobertura legal al responsable para llevar a cabo el tratamiento de datos personales. Según Martos (2018, p. 353) lo fundamental para la licitud del tratamiento es que los datos personales del interesado sean tratados con su consentimiento explícito o bien sobre alguna otra base legítima establecida conforme a derecho. De este modo, el RGPD se pronuncia en su artículo 6.1 sobre las bases que pueden legitimar este tratamiento y que según Martos (2018, p.353) son las siguientes:

a) Mediante consentimiento.[7]
b) Para la ejecución de un contrato del que el interesado es parte.
c) En cumplimiento de una obligación legal aplicable al responsable del tratamiento.
d) Para proteger los intereses vitales del interesado u otra persona física.
e) Por motivos de interés público.[8]
f) Para la satisfacción de intereses legítimos.[9]

No obstante, según contempla el apartado 2 del presente artículo, en el caso del tratamiento de los apartados c) y e) se legitima al Derecho de la Unión y al Derecho de los EM para que completen el alcance de dicha legitimidad. Por último, según señala el mencionado autor, aún cuando no se haya obtenido el consentimiento del interesado ni

[7] Será objeto de estudio en el capítulo IV.
[8] En este apartado tienen cabida los tratamientos realizados en el ámbito de la salud pública, por lo que dedicaremos el capítulo V al estudio de un tema de actualidad como es el COVID-19.
[9] Explicado con más detenimiento en el apartado siguiente.

estemos ante uno de los supuestos señalados anteriormente, el tratamiento se podrá realizar "en pos de la libertad y salvaguarda de los derechos y libertades fundamentales", siempre y cuando se pondere la necesidad y proporcionalidad de dicho tratamiento.

3.2. Interés legítimo

El artículo 6.1 f) del RGPD menciona el "interés legítimo" como fundamento para la licitud del tratamiento de datos personales. Según Martos (2018, p. 354) es necesario delimitar el alcance de dicho concepto ya que "abre una espita importante en la que podrían ampararse las empresas o entidades para realizar tratamientos de datos sin el oportuno consentimiento o base legal que lo justifique." No obstante, el RGPD no establece una definición jurídica de este concepto, sino tan solo una serie de ejemplos en sus Considerados 47-50 en los que el RT podrá alegar dicho interés, entre los que encontramos: la prevención del fraude y situaciones en las que el interesado sea cliente o esté al servicio del responsable (C.47), tratamiento de datos de clientes o empleados dentro de un mismo grupo empresarial (C.48), tratamientos basados en garantizar la seguridad de la red y de la información ante ataques que comprometan datos personales (C.49) o tratamientos con fines estadísticos o de investigación científica (C.50).

Por tanto, tendremos que acudir a la normativa nacional que nos permita delimitar el alcance de lo que se entiende por "interés legítimo" con mayor exactitud. La LOPD en su Título IV establece unas disposiciones aplicables a tratamientos concretos basadas en este concepto jurídico, que según señala en su Preámbulo V "en ningún caso debe considerarse exhaustiva de todos los tratamientos lícitos", sino tan solo presunciones *iuris tantum* de interés legítimo, por lo que fuera de estos casos, el responsable que quiera alegar interés legítimo en un determinado tratamiento deberá llevar a cabo la ponderación que garantice que este no prevalece "sobre los intereses o derechos y libertades del interesado".

Si bien el principio de interés legítimo también puede predicarse en el ámbito de las comunicaciones electrónicas y, por ende, en los dispositivos y aplicaciones móviles, algunos autores como Flaquer Riutort (2018, p. 17) afirman que su presencia es mucho

menor que en otros ámbitos, siendo realmente el consentimiento del interesado la causa justificativa del tratamiento de datos en este ámbito, máxime cuando la Propuesta de RPCE ha omitido cualquier referencia al interés legítimo.

3.3. Protección de datos desde el diseño.

El principio de "privacidad desde el diseño" se regula en el artículo 25 RGPD y básicamente consiste en incorporar la salvaguarda de la protección de datos a los productos y servicios desde sus primeros estadios de desarrollo. (Solar Calvo, 2018, p.5) En otras palabras, como expone el Considerado 46 del RGPD se trata de un mecanismo de prevención que obliga a adoptar medidas técnicas y organizativas apropiadas "tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, para garantizar la seguridad e impedir todo tratamiento no autorizado." (Miralles López, 2018, p. 429). Según García Mexía y Perete Ramírez (2018, p. 180) a través de este principio, el RGPD instaura un "modelo de cumplimiento preventivo y proactivo en lugar de defensivo y sancionador", se trata por tanto de un sistema destinado a prevenir e impedir el daño, en lugar de reparar o indemnizar cuando este ya se haya producido.

En el ámbito de las aplicaciones móviles y redes sociales esto implicaría, por ejemplo, la obligación de los desarrolladores de diseñar la aplicación de tal manera que los perfiles de sus usuarios estén cerrados a otros usuarios por defecto, teniendo que ser el propio usuario quien otorgue su consentimiento para que otras personas puedan visualizar su perfil. (Solar Calvo, 2018, p.5). Asimismo, autores como Fernández Acevedo (2018, p. 243) recomienda a los desarrolladores llevar a cabo un Informe de Análisis de Impacto de la Privacidad de la APP antes de su comercialización y el Dictamen 02/2013 sugiere que, la seguridad de las aplicaciones haya sido estudiada mediante auditoría independiente que garanticen su conformidad con el RGPD.

3.4. Limitación de la finalidad y minimización de datos en aplicaciones móviles

El principio de limitación de la finalidad exige que la recogida de datos personales se realice atendiendo a "fines determinados, explícitos y legítimos" y garantizando que dichos datos no serán objeto de un tratamiento ulterior de manera incompatible con dichos fines. (Muñoz Ontier, 2018, p. 349). En palabras del presente autor y según lo dispuesto en el artículo 89.1 RGPD un tratamiento posterior de dichos datos solo podría justificarse con fines de archivo de interés público o de investigación científica, histórica o estadística.

Por su parte, el principio de minimización de datos regulado en el artículo 5.1. c) del RGPD implica que los datos personales deben ser *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"* lo que llevado a la práctica significa que el RT deberá recabar y utilizar la menor información posible del interesado para cumplir con las finalidades legítimas del tratamiento. (Muñoz Ontier, 2018, p. 349).

En el ámbito de las aplicaciones móviles el GT29 se pronuncia sobre estos principios en el Dictamen 02/2013, sugiriendo que los desarrolladores de aplicaciones deben describir antes de la instalación de la aplicación y de una forma clara, la finalidad a la que se destinan los datos personales que tratarán, en un lenguaje que pueda ser comprendido por un usuario medio sin conocimientos técnicos ni jurídicos. Asimismo, deben informar al usuario en la misma medida acerca de qué datos serán tratados exactamente. Por último, el presente Dictamen prohíbe a los desarrolladores de aplicaciones "cambios súbitos" en cuanto a los datos tratados y su finalidad, debiendo ofrecer para ello anuncios informativos que permitan al usuario renovar el consentimiento, renunciar al tratamiento o incluso la desinstalación de la APP.

Por su parte, las tiendas de aplicaciones y los fabricantes de dispositivos móviles y sistemas operativos deben habilitar mecanismos que faciliten a las aplicaciones únicamente el acceso a los datos estrictamente necesarios, de tal manera que la aplicación

por el simple hecho de estar instalada no tenga acceso a todos los datos del dispositivo. Del mismo modo, debe impedirse que la aplicación como consecuencia de una actualización pueda acceder a datos a los que anteriormente no podía. Asimismo, deben informar al usuario de los datos a los que dicha aplicación que se comercializa en la tienda podrá acceder, para que el usuario pueda decidir libremente si descargarla o no. Por último, señala el Dictamen 02/2013 que las tiendas de aplicaciones y los fabricantes de dispositivos y sistemas operativos deben establecer normas internas coherentes con estos principios, de tal manera, que podrán decidir si una determinada aplicación será o no puesta a disposición en el catálogo de la tienda o apta para su instalación en función de si cumple o no dichas normas, lo que supone un control *ex ante* de la privacidad en la aplicación.

CAPÍTULO IV.

LA PROTECCIÓN DE LA PRIVACIDAD EN APLICACIONES MÓVILES

1. LOS DISPOSITIVOS MÓVILES. LA RECOGIDA DE DATOS POR PARTE DE LAS APLICACIONES

Hoy en día, es difícil imaginar que una persona no disponga de un teléfono móvil, ya que se trata de un dispositivo inteligente que se encuentra en la sociedad de manera omnipresente. Junto a los móviles, existen otros tantos dispositivos inteligentes que reinan la vida de las personas, como pueden ser tabletas, videoconsolas o televisiones con acceso a internet, que tienen en común el disponer de una gran variedad de aplicaciones desarrolladas para maximizar y optimizar el uso de dichos dispositivos.

Por lo general, la mayoría de las aplicaciones requieren que el usuario que las utiliza rellene una serie de datos personales para registrarse.[10] No obstante, es frecuente que las

[10] Por lo general estos datos de carácter personal serán: nombre, apellidos, correo electrónico, dirección, fecha de nacimiento o sexo. No obstante, algunas aplicaciones pueden requerir del usuario otra serie de datos más específicos o sensibles: DNI, tarjeta bancaria, experiencias personales o datos relativos a la salud, entre otros.

aplicaciones puedan recoger datos que se encuentran en los dispositivos en los que se encuentran instaladas, o generados a partir de dichos dispositivos, de tal manera que puedan facilitar al usuario una serie de servicios que se adapten lo máximo posible a sus necesidades, intereses o gustos.[11] Estos datos son especialmente interesantes para los titulares de las aplicaciones y para las empresas de publicidad, ya que podrán utilizar información relativa a usuarios para maximizar sus ingresos y obtener información útil y relevante de cara al desarrollo de nuevas funcionalidades.

Más interesante son aún estos datos cuando proceden de interfaces de programación de aplicaciones, es decir, aquellos datos procedentes de sensores anexos al dispositivo móvil y que permiten llevar un seguimiento de la actividad del individuo en cuestión. [12] Especialmente controvertida resulta la recolección de dichos datos cuando no han sido expresamente consentidos por el usuario, como podremos observar más adelante.

Además, estas aplicaciones suelen ser aparentemente gratuitas u ofrecidas a un coste muy bajo. No obstante, en opinión de Fernández Acevedo (2018, p. 242), esta gratuidad en la descarga y uso se ve compensada con creces con la información personal que se obtiene con la descarga. El problema que surge en estos casos, es que los usuarios no han consentido expresamente o no conocen el alcance del tratamiento que se le van a dar a sus datos personales, pudiendo ser objeto de un tratamiento adicional al uso de la aplicación en cuestión. Por ello, los desarrolladores de aplicaciones que no conozcan o no apliquen la legislación relativa a la protección de datos con la debida diligencia, pueden poner en riesgo la vida privada y reputación de los usuarios.

A lo largo del presente apartado estudiaremos los riesgos que estas situaciones pueden entrañar a los usuarios finales, los distintos actores que intervienen en el desarrollo de una aplicación y su descarga, así como las obligaciones de cada uno de ellos y el grado de responsabilidad que les corresponde en caso de vulnerar la privacidad de sus usuarios.

[11] Nos referimos ahora a datos derivados de la propia utilización del dispositivo móvil como pueden ser: geolocalización, fotos de la galería, historial de navegación, listado de contactos, entre otros.
[12] Estos datos pueden ser captados a través de la grabadora, cámara, geolocalización o micrófono del móvil.

Por último, intentaré, con la mejor voluntad posible, dar respuesta a los problemas planteados y proponer las soluciones que, a mi juicio, deberían ponerse en práctica y que son las más acertadas para que los desarrolladores de aplicaciones móviles no vulneren la privacidad de los usuarios finales.

2. RIESGOS PARA LA PROTECCIÓN DE LA PRIVACIDAD EN LAS APP

Como hemos comentado, el hecho de que un dispositivo inteligente pueda acceder a una gran cantidad de datos personales a partir del dispositivo móvil del usuario de una aplicación puede entrañar importantes riesgos a la privacidad. Según De Miguel Asensio (2015, p. 4) estos riesgos se encuentran, en el ámbito de las aplicaciones móviles "vinculados a la pluralidad de actores relevantes: los numerosísimos creadores de aplicaciones, los fabricantes de los dispositivos móviles y sus sistemas operativos, las tiendas que comercializan aplicaciones y ciertos terceros, como las redes publicitarias." Según este mismo autor, la importancia de dichos riesgos radica en que "tales aplicaciones implican el tratamiento no sólo de una gran cantidad de datos personales sino además de datos de una gran trascendencia en relación con la tutela de los derechos fundamentales del grueso de la población, usuaria de tales dispositivos."

Para la identificación de los riesgos que se plantean a la privacidad en el ámbito de las aplicaciones móviles, se ha consultado el Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, del que podemos extraer los siguientes:

1. La fragmentación de los numerosos actores que intervienen en el desarrollo de aplicaciones y la determinación del alcance de la responsabilidad de cada uno de ellos.

2. La falta de transparencia y conocimiento de los tipos de tratamiento que las aplicaciones pueden realizar: A menudo el usuario se descarga aplicaciones con permisos excesivos de acceso a datos personales, que permiten a entidades y terceros acceder a información personal a través de dicha aplicación. Según un

estudio reciente de la AEPD, se han identificado más de 4.845 permisos en aplicaciones Android que les permiten incumplir el modelo de permisos exigidos por Android para acceder a los datos de los usuarios sin solicitar su consentimiento en el momento de la instalación de la aplicación, lo que supone un déficit de trasparencia según la AEPD [13]. Como consecuencia, los usuarios no son conscientes de que otras entidades y terceros están accediendo a sus datos personales, y mucho menos del tratamiento que se darán a dichos datos.

3. Falta de consentimiento libre, informado y previo: Según Fernández Acevedo (2018, pp. 242-243), el consentimiento prestado por el usuario suele "reducirse a una casilla de verificación, en la que el usuario aceptará los términos y condiciones de la aplicación sin disponer de ninguna opción que le permita o rechazarlas o modificarlas según las necesidades de cada usuario.*"* En este sentido, Marín López (2013, p.1) aconseja "solicitar el consentimiento diferenciado o granular para cada tipo de datos a que accederá la aplicación". Se trata, por tanto, de pedir al usuario de la aplicación que consienta de manera explícita, el uso de cada uno de sus datos personales, pudiendo limitar el trato de los datos personales que no haya consentido expresamente. En cuanto al carácter previo del consentimiento, establece el Dictamen que, es importante que la información se haya facilitado de forma clara y completa, antes de la introducción y extracción de datos del dispositivo. En el mismo sentido, Álvarez Hernando (2015) sostiene que "el Grupo de Trabajo insiste en que los desarrolladores de aplicaciones deben proporcionar información suficiente sobre los datos que van a tratar antes de hacerlo, de forma que puedan obtener un consentimiento válido."

4. Insuficiencia en las medidas de seguridad: Brechas de seguridad por parte del desarrollador de la aplicación puede dar lugar a tratamiento no autorizado y violaciones de datos personales de los usuarios de las aplicaciones, por lo que será necesario adoptar las medidas de seguridad pertinentes para evitar este riesgo.

[13] Dicho estudio cubre más de 82.000 apps preinstaladas en más de 1,700 dispositivos Android fabricados por 214 marcas.

5. Incumplimiento del principio de limitación de la finalidad: Este principio hace referencia a que los datos sean recogidos siempre asegurando fines determinados, explícitos y legítimos, y garantizando que no serán tratados posteriormente de manera incompatible con dichos fines.

De manera resumida, estos son los principales riesgos que el uso de las aplicaciones móviles y dispositivos inteligentes plantean a la privacidad de sus usuarios. Dichos riesgos serán analizados de una forma más exhaustiva en los apartados siguientes teniendo en consideración que el Dictamen al que nos venimos refiriendo es anterior al RGPD, por lo que tendremos que adaptar lo dispuesto en el Dictamen, a la nueva normativa de la forma más acertada posible.

3. PARTES INVOLUCRADAS EN EL TRATAMIENTO DE DATOS EN APLICACIONES MÓVILES Y LAS MEDIDAS DE SEGURIDAD QUE DEBEN ADOPTAR

Como hemos señalado anteriormente, uno de los riesgos que se plantean a la protección de la privacidad en los dispositivos móviles es la enorme cantidad de actores que participan en el desarrollo y funcionamiento de aplicaciones móviles, así como determinar el alcance de la responsabilidad que corresponde a cada uno de ellos en el tratamiento de los datos personales. Por ello, en este apartado, me veo obligado a señalar quiénes son las partes involucradas en este proceso conforme al Dictamen 02/2003 y qué variaciones significativas en sus funciones y responsabilidad han de tenerse en cuenta conforme al nuevo RGPD. Por último, analizaremos las medidas de seguridad que cada parte ha de adoptar por obligación del RGPD.

3.1. Desarrolladores de aplicaciones y propietarios de aplicaciones

Esta categoría la conforman aquellas empresas y personas que crean las aplicaciones móviles y las distribuyen para su uso, así como toda aquella entidad que subcontrate la creación de las mismas. Según el Dictamen 02/2003, los desarrolladores y propietarios de aplicaciones tendrán la consideración de responsables del tratamiento en la medida en que serán quienes determinen la finalidad y los medios del tratamiento, ya que la aplicación podrá acceder a una gran cantidad de datos una vez instalada en el dispositivo, por lo que, les corresponde determinar los datos a los que podrá tener acceso la aplicación. Por tanto, tendrán que cumplir las obligaciones que el RGPD les otorga, y que serán detalladas en los siguientes apartados como responsables del tratamiento.

Para el correcto funcionamiento de las aplicaciones es frecuente que la propia aplicación pueda acceder a datos almacenados en el dispositivo o exija que el usuario rellene una serie de datos para su acceso. Son datos que los desarrolladores y propietarios de la aplicación procesan para sus propios fines, por lo que, podrían incurrir en responsabilidad si no cumplen con las obligaciones del RGPD.

Especialmente relevante resulta para estos sujetos la fase de diseño y desarrollo de la APP, ya que, desde la entrada en vigor del RGPD, deberán llevar a cabo una evaluación de impacto relativa a la protección de datos, según dispone el artículo 35.1 RGPD *"Cuando sea probable que un tipo de tratamiento, en particular, si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales."*

Y este requisito tiene como finalidad la correcta aplicación de los principios de privacidad por diseño y privacidad por defecto, según señala Fernández Acevedo (2018, p. 243). El autor sostiene que esto se logra a través de un Informe de Análisis de Impacto de la Privacidad (PIA), que deberá incluir como mínimo el contenido previsto en el artículo 35.7 del RGPD, que incluye, entre otras medidas, una descripción de las operaciones previstas, de los fines del tratamiento y del interés legítimo del responsable, así como la evaluación de la necesidad, proporcionalidad y riesgos asociadas a las mismas.

En el caso de que participase en el tratamiento de datos algún ET al que se hayan externalizado los datos del usuario, este tendrá que haber sido previamente seleccionado por el desarrollador de la APP, tras exigirle las garantías suficientes para la aplicación de las medidas técnicas y organizativas adecuadas, conforme dispone el artículo 28 RGPD. Si fuese un tercero quien participase en el tratamiento de datos, el desarrollador tendrá que obtener el consentimiento informado del usuario de la aplicación tal y como dispone el Dictamen 02/2003. En ambos casos, la responsabilidad correspondiente a cada una de las partes deberá determinarse caso por caso.

Una de las novedades que incorpora el RGPD en su artículo 33 es la obligación del responsable del tratamiento, en el caso de producirse una brecha de seguridad que comprometa los derechos y libertades de los usuarios, de notificar a la autoridad de control competente en un plazo máximo de 72 horas desde que se tiene constancia de la violación de la seguridad. Se trata de una medida que ha de adoptarse cuando ya se ha producido el daño, a pesar de las medidas técnicas y organizativas que el artículo 24 RGPD impone al desarrollador de la aplicación a incorporar para garantizar la protección de los datos personales que tratan, en todas las fases del diseño y la puesta en práctica de la aplicación, según señala Marín López (2013, p.2).

No existe una lista cerrada de las medidas de seguridad que debe adoptar el desarrollador de la aplicación, por lo que el Dictamen 02/2003 ha recogido una serie de recomendaciones en materia de seguridad para los desarrolladores de APPs, entre las que se encuentran, entre otras:

- El almacenamiento de datos en sistemas pertenecientes al proveedor de servicios que facilite a los usuarios su recuperación en caso de pérdida o robo del dispositivo.
- Elaborar políticas acerca de la elaboración y distribución de sus aplicaciones y facilitárselas a los usuarios finales.
- Habilitar herramientas para facilitar la instalación y desinstalación de la APP a voluntad del usuario.

- Permitir a las aplicaciones únicamente el acceso a aquellos datos que son realmente necesarios para el funcionamiento de la APP.
- Exigir al usuario una contraseña robusta, a través de tests de solidez, reautentificación y utilización de canales diversos.
- Permitir a los usuarios comprobar los datos que se estén tratando y facilitar que puedan activar y desactivar los permisos para su tratamiento.

3.2. Fabricantes de dispositivos inteligentes y sistemas operativos

La mayor parte de los datos personales que utilizan las aplicaciones provienen del dispositivo móvil del propio usuario de la aplicación. El dispositivo móvil almacena tanto datos que son generados por su titular como datos que son generados por el propio dispositivo móvil, como consecuencia de su uso.

De este modo, los fabricantes de dispositivos inteligentes y sistemas operativos ponen a disposición de las aplicaciones móviles estos datos que dispone de sus titulares, sin los cuáles no sería posible el funcionamiento de la aplicación.[14] Esto sitúa a dichos sujetos en una condición de "responsables del tratamiento" respecto de esos datos que ceden a las aplicaciones móviles, ya que son ellos quienes determinan los medios a través de los cuáles las aplicaciones acceden a los datos del titular del móvil.

Según señala De Miguel Asensio (2015, p.4) el afectado no tiene en estos casos un control estricto sobre los datos que el dispositivo móvil comunica a los desarrolladores de las aplicaciones. Es por ello, por lo que el Dictamen 02/2013 establece que los fabricantes deben establecer herramientas que impidan que los desarrolladores de aplicaciones puedan acceder a datos que no sean estrictamente necesarios para el buen funcionamiento de su aplicación, así como herramientas que permitan al sistema operativo revocar dicho acceso de forma simple y efectiva. Del mismo modo, el usuario del dispositivo debe tener

[14] Un ejemplo de este caso sería el de la aplicación de mensajería instantánea "Whatsapp", que tiene acceso a la lista de contactos del teléfono móvil o el del juego online "Pokémon Go" que utiliza la geolocalización del usuario para la captura de Pokémon.

constancia de los datos que se ceden a la aplicación móvil y disponer de herramientas que permitan otorgar y revocar el consentimiento a dicha cesión.

Anteriormente, el Dictamen 13/2011, prohibió que los fabricantes de dispositivos móviles y sistemas operativos pusiesen en funcionamiento de forma automática aplicaciones de geolocalización, siendo necesario para la activación de dichos servicios "un consentimiento informado y específico a los diferentes fines para que los datos sean captados o almacenados." (Roger Shultz, 2011). Este consentimiento tendrá que ser renovado anualmente y será necesario que el dispositivo móvil advierta que se está haciendo uso de la función de geolocalización "a través de un icono que se encuentre permanentemente visible."

Junto a esta medida, el GT29 añadió otras que los fabricantes deben respetar en el Dictamen 02/2013, entre las que cabe destacar el diseño de mecanismos de autenticación de alta seguridad, la aplicación de mecanismos para obtener el consentimiento individualizado para el tratamiento de cada dato[15], el desarrollo de auditorías que permita al usuario comprobar las aplicaciones que han tratado sus datos y la actualización periódica del sistema operativo que permita subsanar las deficiencias de seguridad que se detecten.

3.3. Tiendas de aplicaciones

Hoy en día, cada dispositivo móvil dispone de su propia tienda de aplicaciones a través de la cuál puede descargarse cualquier aplicación que dicha tienda ofrezca. Estas tiendas, exigen que el usuario aporte su tarjeta de crédito para la realización de compras, además de otros datos personales, como el nombre del usuario o su dirección. Del mismo modo, la tienda de aplicaciones puede disponer de información muy valiosa que puede ayudar a

[15] Ya que, en numerosas ocasiones, se solicita el consentimiento de los datos de forma conjunta, sin individualizarlos.

los desarrolladores de aplicaciones a llevar a cabo su trabajo de manera más eficaz. [16] Respecto del tratamiento de dichos datos, el Dictamen 02/2013 considera que la tienda de aplicaciones será "responsable del tratamiento", por lo que recomienda una serie de medidas de seguridad como son controlar y comprobar que las aplicaciones que se comercializan en la tienda cumplen con la normativa europea de protección de datos e informar al usuario de la manera en que se realiza dicho control, habilitar sistemas de evaluación pública de las aplicaciones, facilitar mecanismos de desinstalación sencillos y establecer canales de retroalimentación que permita al usuario informar de los problemas de seguridad que sufra, así como informar al usuario en caso de que se produzca alguna brecha de seguridad en la tienda. (Marín López, 2013, p. 2-3).

3.4. Otros sujetos

El Dictamen 02/2013 señala que, en el ámbito de la protección de la intimidad en aplicaciones móviles, también tienen un papel importante otros sujetos como las redes publicitarias y los proveedores de análisis.

En lo referente a la publicidad, el GT29 en su Dictamen 2/2010 sobre publicidad comportamental en línea, sostiene que este tipo de publicidad suscita inquietudes graves sobre protección de datos y privacidad, ya que los proveedores de publicidad rastrean los comportamientos de navegación de los usuarios a través de *cookies* para descubrir el perfil de usuario y proporcionarle, en un momento posterior, publicidad adecuada a sus gustos. Los proveedores de publicidad son calificados tanto por el Dictamen 2/2010, como por el Dictamen 02/2013 como "responsables del tratamiento" debido a que determinan la finalidad y los medios del mismo.

Por ello, la Directiva 2002/58/CE, en su artículo 5.3 imponía a los proveedores de publicidad la obligación de informar de forma clara y completa al usuario acerca de la

[16] Datos como el historial de descargas, las aplicaciones más descargadas o la categoría de APPS que más gustan a los consumidores son datos que las tiendas de aplicaciones suele ceder a los desarrolladores de APPS.

información almacenada en el dispositivo a la que se va a acceder y la finalidad del tratamiento, lo que también se recoge en la actual Propuesta de RPCE en su artículo 8. Asimismo, también se exige que el proveedor le de la posibilidad de negarse a que se produzca dicho acceso.

En cuanto a los proveedores de análisis, suelen ser entidades cuyo objeto es la recopilación de datos a través de *cookies* acerca de la facilidad en el uso de la aplicación, su popularidad u otras características para sacar conclusiones que serán útiles a los desarrolladores de aplicaciones para mejorarlas o actualizarlas. En este caso, según dispone el Dictamen 02/2013 actuarían como "encargados del tratamiento", pues no determinan los medios ni los fines del tratamiento, esto corresponde al desarrollador de la aplicación, que sería el responsable por cuya cuenta trabajan.

No obstante, en el caso de que el tratamiento de datos por los proveedores de análisis fuera sus propios fines, se calificarían como "responsables del tratamiento", teniendo que cumplir las obligaciones que el RGPD impone a este sujeto.

4. REQUISITO DEL CONSENTIMIENTO POR PARTE DEL INTERESADO

Entre todas las premisas que se establecen en el artículo 6 RGPD para poder afirmar que un determinado tratamiento de datos es lícito, podemos afirmar que el consentimiento del interesado es las más importante de todas y el fundamento sobre el que gira la licitud del tratamiento de datos personales en el ámbito de las aplicaciones móviles.

La antigua Directiva 95/46/CE establecía en su artículo 2 h) una definición de lo que se entendía por "consentimiento del interesado": *"toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan."* Asimismo, el artículo 7 añadía que este se debe prestar *"de forma inequívoca"*. Esta misma definición de consentimiento era la que se recogía en la Directiva 2002/58/CE, para la protección de datos en comunicaciones electrónicas y en la LOPD en su artículo 3.h).

En el momento que se produce la instalación de la aplicación en el dispositivo móvil, esta podrá tratar datos personales que alberguemos en el mismo, por lo que hará falta delimitar los datos que estamos consintiendo que se traten, de los que no. Por tanto, será necesario encontrar la aplicación práctica que tiene la definición de consentimiento en el ámbito de las aplicaciones móviles. Para ello, acudimos al Dictamen 15/2011 sobre la definición del consentimiento y al ya conocido Dictamen 02/2013.

En primer lugar, el consentimiento debe ser "libre", lo que según el Dictamen 15/2011 implica que el interesado "pueda elegir una opción real y no haya ningún riesgo de engaño, intimidación, coerción o consecuencias negativas en caso de que no consienta." En el ámbito que nos ocupa es especialmente importante que el interesado pueda escoger una "opción real", y esto, según el Dictamen 02/2013 y Fernández Acevedo (2018, p. 243) implica que el usuario pueda no solo aceptar sino también, rechazar el tratamiento; es decir, el interesado debería visualizar una casilla que le permita la instalación de la APP y otra que le permita el rechazo o la cancelación para dar un consentimiento "libre".

En segundo lugar, el consentimiento debe ser "específico", esto es, el consentimiento no puede "consistir en una autorización formulada en términos generales" como señala el Dictamen 02/2013, sino que, debe referirse a cada dato concreto que se va a tratar y delimitar la finalidad de dicho tratamiento. Por ello, la AEPD (2018) señala que no será suficiente que se acepten en conjunto las condiciones de la política de privacidad y propone un consentimiento "granular", de forma independiente para cada dato que se vaya a tratar. De esta manera, se evita, en opinión de la AEPD (2019) que los desarrolladores condicionen el uso de la APP a obtener un consentimiento para un tratamiento no necesario para los servicios que se prestan.[17]

En tercer lugar, el consentimiento ha de ser "informado". El alcance de esta información se analizará con más detenimiento en el apartado siguiente, pero tanto el mencionado

[17] Por ejemplo, para enviar notas de audio por Whatsapp, tendríamos que otorgar el consentimiento "específico" de acceso al micrófono para este fin. Esto significa que, si Whatsapp quisiese recoger datos a través de nuestro micrófono cuando la aplicación no está en uso, o para fines distintos del señalado, sería necesario que solicitase ese consentimiento "específico" en pieza separada del anterior.

autor como el Dictamen 02/2013 señalan que dicha información debe proporcionarse antes de la instalación.

Por último, el consentimiento debe ser "inequívoco", lo que según el Dictamen 15/2011 significa que "el procedimiento de su obtención y otorgamiento no tiene que dejar ninguna duda sobre la intención del interesado al dar su consentimiento" No obstante, el presente Dictamen añade que el consentimiento inequívoco podrá ser: a) expreso o; b) basado en determinados tipos de procedimientos para que las personas manifiesten un claro consentimiento deducible.

Según autores como Adsuara Varela (2018, p. 169), García Mexía y Perete Ramírez (2018, p. 180) esta última opción ha dado lugar en el pasado a algunos abusos o malas prácticas por parte de muchas de empresas digitales, como calificar el mero silencio, la inacción o las casillas pre-marcadas al instalar la aplicación como consentimientos válidos, bajo el argumento de que son procedimientos por los que se manifiesta "un claro consentimiento deducible."

No obstante, el nuevo RGPD ha eliminado cualquier duda, ya que ha incorporado un nuevo requisito en su art. 4.11 al establecer que el consentimiento, además de los requisitos mencionados anteriormente, debe expresarse *"ya sea mediante una declaración o una clara acción afirmativa."* Según García Mexía y Perete Ramírez (2018, p. 169), de esta manera serán válidos los "consentimientos prestados por escrito, inclusive por medios electrónicos y las declaraciones verbales", no pudiendo ser válidos a la luz de esta nueva norma las casillas pre-marcadas, el silencio o los epígrafes formulados de forma negativa. (Martos, 2018, p. 357). En la Directiva 95/46/CE este "consentimiento explícito" solo se preveía para el tratamiento de "categorías especiales de datos" por ejemplo, el historial médico. Con el nuevo RGPD se extiende este consentimiento a todos los datos personales que se vayan a tratar, lo que redundará en una mayor seguridad jurídica, ya que, en opinión de Villarino Marzo (2018, p.307), en la era del "Internet de las cosas" aplicar los mecanismos clásicos para obtener el consentimiento daban lugar a "la imposibilidad fáctica de facilitar un consentimiento ajustado en línea con las preferencias expresadas por los usuarios."

Asimismo, el Dictamen 02/2013 establece que los desarrolladores de aplicaciones deben facilitar que el consentimiento pueda ser revocado o retirado en cualquier momento de forma sencilla y eficaz.

Por último, debemos señalar que, una vez prestado el consentimiento en la forma expresada anteriormente para la instalación de la aplicación y el tratamiento de datos personales, puede suceder que el desarrollador necesite tratar algunos datos de los que no se haya aportado un "consentimiento específico". En ese sentido señala el Dictamen 02/2013 que el desarrollador podrá invocar los fundamentos jurídicos de los artículos 7.b) y 7.h) de la Directiva 95/46/CE[18], que son "la necesidad para la ejecución de un contrato con el interesado" y "la necesidad de satisfacer intereses empresariales legítimos" siempre y cuando dicho tratamiento de datos cumpla los siguientes requisitos:

- No se supediten los intereses legítimos al interés de los derechos y libertades fundamentales del usuario.
- Se trate de datos personales no sensibles.
- El tratamiento de dichos datos sea estrictamente necesario para el cumplimiento del contrato con el interesado o prestación del servicio que ofrece la aplicación.

5. DEBER DE INFORMAR

Como pudimos observar en el apartado anterior, uno de los requisitos que el consentimiento del interesado debe reunir para su validez es que fuese "informado". No obstante, en el presente apartado debemos definir cuál es la información mínima que se debe proporcionar, quién debe hacerlo, en qué momento y en qué forma.

[18] Este artículo se corresponde con el 6 RGPD, y recoge los fundamentos jurídicos para la licitud del tratamiento, vistos en el apartado III.

En el ámbito de las aplicaciones móviles, la AEPD en su *Guía para el cumplimiento del deber de informar* (en adelante, Guía) señala que el usuario final debe conocer como mínimo:

1. La identidad del responsable del tratamiento y sus datos de contacto: A este respecto, la AEPD señala que el responsable del tratamiento debe identificarse en la política de privacidad y en caso de ser una aplicación móvil cuyo responsable no esté establecido en la UE, debe designar un representante en territorio europeo e identificarlo en la política de privacidad. Por su parte, el Dictamen 02/2013 señala que, para evitar el problema de la fragmentación de responsables en el entorno de aplicaciones móviles, es importante que se establezca un punto de contacto único al que el usuario pueda dirigirse y donde se asuma responsabilidad de todo el tratamiento llevado a cabo en la aplicación. En definitiva, en la política de privacidad deben identificarse los distintos responsables del tratamiento y no dejar al usuario final la tarea de identificar al responsable. Los datos de contacto del responsable que deben facilitarse son: la identidad, dirección postal, teléfono y correo electrónico. (AEPD).

2. Los datos exactos que van a ser recogidos y la finalidad de su tratamiento: La política de privacidad debe señalar qué datos son los estrictamente necesarios para el uso de la aplicación y cuáles otros son opcionales. El Dictamen 02/2013 recomienda a los desarrolladores de aplicaciones móviles habilitar al usuario la opción de denegar el acceso a dicha información opcional. Del mismo modo debe quedar claro para qué fines se van a utilizar dichos datos. La AEPD en su Guía señala que se debe evitar finalidades "genéricas e inespecíficas" que pueda dar lugar a tratamientos que excedan de las expectativas del interesado.

3. Los derechos que asisten al interesado y su forma de ejercerlos: El desarrollo de los derechos del interesado se podrá observar en el apartado siguiente, pero en cuanto a la forma de ejercerlos la Guía de la AEPD establece que los desarrolladores de aplicaciones deben poner a disposición del usuario distintos modelos y formularios, así como las instrucciones que deben seguir para llevar a cabo su solicitud. Del mismo modo, la Guía señala que se debe informar al usuario

del derecho a revocar el consentimiento en cualquier momento, "sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada".

4. Los periodos de conservación de la información: Según Fernández Acevedo (2018, p. 244) los desarrolladores deben establecer unos protocolos específicos que limiten la retención o la continuidad del tratamiento de datos personales una vez el usuario haya desinstalado la aplicación o tras un periodo de inactividad. Este plazo, según señala el Dictamen 02/2013 dependerá de la finalidad de la aplicación y de la relevancia de los datos. El fundamento de este plazo, según el mencionado autor, reside en que el usuario puede haber perdido el teléfono móvil o haberlo cambiado por otro sin la desinstalación de las aplicaciones, por lo que el desarrollador deberá fijar en la política de privacidad un plazo de inactividad tras el cual, la cuenta se entenderá expirada. Señala el Dictamen 02/2013 que el responsable deberá alertar al usuario cuando ese plazo haya expirado para darle la oportunidad de recuperar sus datos personales. Esto podría realizarse, por ejemplo, a través del correo electrónico asociado a la aplicación, o a través de un SMS. Del mismo modo señala el Dictamen que si el usuario no responde a esta alerta, el responsable deberá proceder a la eliminación de los datos de forma irreversible o anonimizarlos.

5. La base jurídica que legitima el tratamiento: Como se pudo observar en el epígrafe "Licitud del tratamiento" el artículo 6 RGPD establece una serie de premisas sobre las que se construye un tratamiento lícito. Según cual sea la premisa que ha dado lugar al tratamiento la información que debe aportar el responsable será diferente. Señala así la Guía de la AEPD que, en caso de que la base jurídica sea la "ejecución de un contrato", constará sin ambigüedades una referencia a ese contrato; si se da en "cumplimiento de una obligación legal o por motivos de interés público", constará sin ambigüedades cuál es la norma, que impone la obligación o califica el interés público respectivamente. Del mismo modo se especificará el "interés legítimo del responsable" que da lugar al tratamiento si fuese esta la base jurídica. Por último, como sucederá frecuentemente, si en lo que

se fundamenta el tratamiento es en el consentimiento del interesado, este deberá reunir los requisitos señalados en el apartado anterior.

En cuanto a la forma en la que debe presentarse la información, señalan autores como García Mexía o Perete Ramírez (2018, p. 180) que el hecho de que la pantalla reducida de un dispositivo móvil suponga una limitación de espacio esto no debe suponer una excusa que lleve al desarrollador a omitir información relevante, ya que, tanto el Dictamen 02/2013 como la Guía de la AEPD ofrecen una serie de alternativas o soluciones el "uso de iconos normalizados o la presentación de la información por capas."

El método de presentación de la información por capas según la Guía de la AEPD consiste en presentar "la información básica en un primer nivel, de forma resumida", en el momento y en el mismo campo de visión en que el usuario tiene que prestar el consentimiento, mientras que la "información adicional" se puede llevar a cabo en un segundo nivel o capa de forma completa. Una manera de cumplir con este deber sería ofrecer la información básica en una pestaña al mismo tiempo que se adjunta el botón "Instalar", ofreciendo asimismo un enlace que permita acudir a toda la información adicional y completa.

Por último, Señala el Dictamen 02/2013 que la información debe ser "accesible y fácilmente localizable" tanto en la tienda de aplicaciones como dentro de la propia aplicación, y debe estar redactada de forma clara y comprensible para el usuario medio, siendo inaceptables las políticas de privacidad farragosas, ilegibles y difíciles de localizar en la APP.

6. DERECHOS DEL INTERESADO

Una de las cuestiones sobre las que el desarrollador de la aplicación y los demás responsables del tratamiento deben informar al usuario antes de que este preste su consentimiento son los derechos que le asisten y puede ejercer. En el presente apartado desarrollaremos aquellos derechos que, desde mi punto de vista, son los más relevantes en el ámbito de las aplicaciones móviles.

6.1. Derecho de acceso

Según Aparicio Salom (2018, p. 384) el derecho de acceso se regula en el artículo 15 RGPD y se define en el considerando 63 del RGPD, según el cuál:

"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 de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento."

En otras palabras, el derecho de acceso implica la obligación del responsable del tratamiento de confirmar al usuario si está tratando o no sus datos personales y, en su caso, facilitarle una copia de toda la información sobre los datos y su tratamiento. En este sentido, el Dictamen 02/2013 recomienda a los desarrolladores establecer herramientas de acceso a la información de forma visible dentro de la aplicación. Por último, el Dictamen señala que, para ejercer el derecho de acceso, se debe comprobar la identidad del usuario para evitar que los datos se filtren a terceros, lo que, en el caso de aplicaciones móviles podría bastar con autenticar la identidad a través de la contraseña del usuario o enviando la información al correo electrónico asociado.

6.2. Derecho de rectificación

El derecho de rectificación queda regulado en el artículo 16 RGPD. Según Aparicio Salom (2018, p. 388) es la materialización del principio de exactitud de los datos y en virtud de este derecho, el interesado puede exigir al responsable que los datos se rectifiquen o actualicen cuando sean inexactos o incompletos.

6.3. Derecho de supresión

El derecho de supresión se regula en el artículo 17 RGPD y hace referencia al derecho que tiene el interesado a solicitar al responsable del tratamiento la supresión o eliminación de los datos personales bien sea por no interesarle que dichos datos que sigan sometiendo a tratamiento, porque el tratamiento no se ajuste al RGPD o por imperativo legal. (Aparicio Salom, 2018, p.390). Según el presente autor no se debe confundir el derecho de supresión con la obligación que tiene el responsable de proceder a la eliminación de dichos datos cuando el tratamiento haya perdido su fundamento.

En el ámbito de las aplicaciones móviles un usuario podría hacer uso de este derecho, por ejemplo, si quiere eliminar los datos de su tarjeta de crédito de una determinada aplicación a través de la que realizaba ciertas compras sin tener que aportar ningún motivo que justifique la retirada de dicho consentimiento. Distinto es el caso cuando el tratamiento se lleva a cabo en cumplimiento de una obligación legal o contractual, en cuyo caso, Aparicio Salom (2018, p. 391) señala que "la cancelación solo podrá basarse en la culminación de la finalidad o la ilicitud del tratamiento de datos."

El Dictamen 02/2013 hace referencia al deber del responsable de eliminar los datos personales del usuario cuando este haya desinstalado la aplicación, ya que, desde este momento, "carece de un fundamento jurídico que justifique el tratamiento de datos personales". No obstante, señala el Dictamen que la aplicación puede prever periodos de conservación de los datos, para el caso en que el usuario desee, por ejemplo, reinstalar la APP en el futuro. En todo caso, según el grupo de trabajo, será necesario solicitar el consentimiento a esta retención temporal en el momento de la desinstalación.

6.4. Derecho a la portabilidad de los datos

Si bien los derechos que acabamos de mencionar ya se incluían en la Directiva 95/46/CE[19], debemos apuntar que el RGPD ha introducido nuevos derechos del interesado, entre los que cabe destacar el derecho a la portabilidad de los datos por su enorme aplicación práctica en el ámbito de las comunicaciones electrónicas.

El derecho a la portabilidad queda regulado en el artículo 20 RGPD y como apunta Miralles López (2018, p. 404) este derecho implica que el interesado podrá acudir al responsable del tratamiento para que le entregue sus datos o bien, podrá solicitar que el responsable del tratamiento transmita sus datos a otro responsable de su elección.

En el ámbito de las aplicaciones móviles, por tanto, es el derecho que asiste a usuario de irse de una aplicación a otra pudiéndose llevar consigo todos sus datos a la nueva aplicación. (Fernández Acevedo, 2018, p.244). Algunos autores como Calle (2018) nos ilustran este derecho a través de un ejemplo: *"de la misma manera que una persona se lleva su número de móvil cuando cambia de operador, también puede llevarse sus datos."*

Se trata, en opinión de Miralles López (2018, p. 401) de un derecho que otorga a los titulares de los datos de un mayor control sobre los mismos, a la vez que facilita su movilidad en entornos digitales. En el ámbito de las aplicaciones móviles algunos autores como Fernández Acevedo (2018, p. 244) y Calle (2018) consideran necesario que los fabricantes de sistemas operativos y desarrolladores de aplicaciones colaboren para desarrollar herramientas de descarga, términos de código abierto o estándares similares de manera que se fomente la interoperabilidad de los datos bajo la estricta supervisión y conocimiento del usuario de la aplicación.

7. CUESTIONES RELATIVAS AL CONSENTIMIENTO PRESTADO POR MENORES DE EDAD

[19] Sin embargo, al derecho de supresión se le denominaba anteriormente "derecho de cancelación". (Adsuara Varela, 2018, p.170).

Hoy en día, una gran cantidad de aplicaciones están dirigidas a un público objetivo menor de edad, como es el caso de aplicaciones de videojuegos y redes sociales muy frecuentadas por adolescentes. Es evidente, que en muchas ocasiones si los propios adultos no prestan suficiente diligencia en leer y comprender las políticas de privacidad de las aplicaciones, es de esperar que los menores edad, puede que ni conozcan su existencia ni sean capaces de entender todos los riesgos relativos a la protección de datos personales, por lo que el consentimiento prestado por los menores debe ser objeto de estudio de forma separada.

Sobre el consentimiento para el tratamiento de datos personales de menores de edad se pronuncia el RGPD en su artículo 8 estableciendo la edad mínima para el tratamiento lícito de datos personales en 16 años. No obstante, dicho artículo prevé que *"Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años."* En España esta regulación se lleva a cabo por el Proyecto LOPD en su artículo 7 y Fundamento Jurídico IV, en el cuál se establece esta edad mínima en 13 años. (Martos, 2018, p. 359). Por lo tanto, todo tratamiento de datos personales de un menor de 13 años requerirá el consentimiento de sus padres o tutores, tal y como señala Fernández Acevedo (2018, p. 244).

Según señala el párrafo 2º del artículo 8 RGPD corresponde al responsable del tratamiento realizar esfuerzos razonables para la verificación de que el consentimiento prestado por menores de 16 años fue autorizado por el titular de la patria potestad sobre el menor, teniendo en cuenta la tecnología disponible. (Piñar Real, 2019). Por lo que se puede observar, el responsable tiene ante sí una obligación de medios y no de resultado, y esto se debe a los escasos mecanismos tecnológicos existentes que permitan comprobar la identidad jurídica del usuario, en opinión de Martos (2018, p. 359).

En palabras de Fernández Acevedo (2018, p. 245) los responsables "deben respetar aún más estrictamente los principios de minimización de datos y limitación de la finalidad" cuando se trata de datos personales de menores de edad. Por último, el Dictamen 02/2013 añade que, los responsables no podrán tratar datos de menores con "fines de publicidad

comportamental" y la información sobre privacidad tendrá que adaptarse a un lenguaje sencillo acorde con la edad del usuario.

CAPÍTULO V.

ANÁLISIS DE CASOS RECIENTES DE PRIVACIDAD EN APLICACIONES MÓVILES. RESOLUCIONES DE LA AEPD

Para concluir el presente trabajo dedicaremos este apartado al estudio de algunos casos recientes de protección de la privacidad en el ámbito de los dispositivos móviles. En primer lugar, comentaremos una resolución de la AEPD en la que una aplicación es sancionada por el uso indebido de la función de geolocalización y, por último, atendiendo a la situación actual que vivimos analizaremos que incidencia está teniendo el COVID-19 en el tratamiento de datos personales.

1. RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR 00326/2018. EL CASO LALIGA

Una de las novedades que el RGPD introduce con respecto a la anterior Directiva, es el endurecimiento de las sanciones administrativas en materia de protección de datos. Según señala Adsuara Varela (2018, p. 172) con la anterior regulación la cuantía máxima que la AEPD podía fijar para una multa era de 600.000 euros. Con el nuevo reglamento, una sanción podría ascender a los 20 millones de euros o el 4% de facturación.

La resolución de la AEPD que presentamos en el presente apartado contiene la sanción más elevada que la AEPD ha impuesto desde que se aprobó el RGPD y nos sirve como ejemplo práctico e ilustrativo donde podemos observar la aplicación de la muchos de los conceptos y principios descritos en el presente trabajo, por lo que se recomienda su lectura exhaustiva. En dicha resolución se sanciona a la LaLiga con 250.000 euros por comercializar una app que, siendo su principal finalidad el proporcionar a los usuarios información sobre los partidos de fútbol en juego, activaba el micrófono y la

geolocalización de los usuarios para "detectar a los bares que proyectan partidos de fútbol sin pagar". (Sánchez, 2019).

Es cuestionable desde el punto de vista del derecho a la intimidad, que una aplicación tenga acceso al micrófono de un usuario para captar sonido ambiente por mucho que el usuario haya otorgado su consentimiento a este tratamiento, ya que, según la AEPD, esto podría implicar a su vez, la captación de conversaciones que podrían incluir datos personales de terceras personas que no hayan prestado su consentimiento.

No obstante, si bien es cierto que al usuario se le informa a la hora de instalar la aplicación que esta podrá acceder a su micrófono y geolocalización para la finalidad de "detección de fraudes en el consumo del fútbol", la AEPD (2019, p. 66) denuncia una vulneración del principio de transparencia del artículo 5.1 RGPD, como consecuencia de una inexistente información al usuario sobre las siguientes circunstancias:

(i) La ausencia de información en la Política de Privacidad acerca del momento exacto en que la aplicación activará el micrófono y la geolocalización. A pesar de que LaLiga sostenga que solo se activará el micrófono y la ubicación en las franjas horarias en las que se dispute un partido, según la AEPD tras la inspección llevada a cabo de la aplicación, no consta a la hora de instalar la aplicación ni en su política de privacidad, el "momento concreto en que se podrán activar las funcionalidades de micrófono y ubicación."

(ii) La ausencia de información que permita al usuario visualizar y tener conocimiento a tiempo real de que la aplicación está accediendo al micrófono del dispositivo. Si bien es cierto que al usuario se le informa a tiempo real a través de un icono que se está recogiendo datos relativos a su geolocalización, lo que se tiene en cuenta a la hora de ponderar la sanción, no se puede afirmar lo mismo respecto de la recogida de datos a través del micrófono, ya que la aplicación no muestra ningún elemento que le permita al usuario conocer este hecho. Según la AEPD habría bastado con un icono fácilmente identificable y reconocible que indicara que la aplicación ha activado el micrófono.

(iii) La aplicación puede acceder al micrófono y a la geolocalización, aunque esta no se esté ejecutando o lo haga en segundo plano. Sobre esta circunstancia tampoco se informa al usuario en ningún momento.

En mi opinión, además de la vulneración del principio de transparencia del artículo 5.1 RGPD podría argumentarse que esta desinformación puede dar lugar a un consentimiento inválido debido a que este no reúne uno de los requisitos necesarios, esto es, que sea un consentimiento "informado". Según lo analizado en apartados anteriores, aún en el caso de que dicha información pudiera no considerarse "básica" y susceptible de aparecer en una "primera capa informativa", nada de esto impediría incluirla en una "segunda capa informativa" donde debe aparecer toda la información adicional relativa al tratamiento de datos personales.

Asimismo, la AEPD (2019, p. 67) denuncia una vulneración del artículo 7.3 RGPD, en tanto no se le otorga al usuario la posibilidad de revocar el consentimiento otorgado al tratamiento de datos dentro de la propia aplicación. Para efectuar dicha revocación el usuario tendría que acudir a los ajustes del dispositivo móvil y desinstalar el acceso de la aplicación a las funciones del micrófono y geolocalización. Como podemos observar, el desarrollador de la aplicación incumple las directrices del Dictamen 02/2013 en tanto no facilita al usuario un mecanismo que posibilite "revocar el consentimiento de forma fácil y sencilla."

Otra cuestión que ha suscitado polémica es la relativa a la calificación como datos personales de la información que se recoge. Según LaLiga y juristas como Muñoz Ontier citado por Sánchez (2019), la aplicación no recoge datos personales, ya que a partir del audio recogido por el micrófono se generan "huellas digitales" en forma de código binario que eran enviados a un encargado del tratamiento, el cual se encargaba de cotejar la información recibida con la huella digital correspondiente a la emisión de un partido de fútbol. En caso coincidencia de las secuencias de sonido LaLiga podía comprobar si la emisión era ilegal o no. Por tanto, según Muñoz Ontier "la app no llega a escuchar si estás hablando con alguien, por eso el audio no recoge datos personales". (Sánchez, 2019) No obstante, la AEPD (2019, p. 45) considera que no hay ninguna duda de que lo que recoge

son datos personales, ya que se trata de "sonidos que pueden contener datos personales", independientemente de que a nivel interno se produzca un proceso ulterior que lo transforme en una huella digital.

Por tanto, a través de esta Resolución podemos comprobar que la protección de la privacidad es un ámbito que cada vez cobra más importancia y a raíz del nuevo RGPD, se han intensificado tanto los requisitos con los que deben cumplir las Políticas de Privacidad en las aplicaciones móviles como las sanciones derivadas de su incumplimiento. Queda por saber si el caso que presentamos será un caso aislado que servirá de precedente a los desarrolladores de aplicaciones para mejorar y revisar sus Políticas de Privacidad o, por el contrario, veremos más casos de sanciones de la AEPD de este calibre en el futuro.

2. TRATAMIENTO DE DATOS PERSONALES EN RELACIÓN CON EL COVID-19

Según lo analizado en el apartado relativo a la licitud del tratamiento, el artículo 6.1 RGPD establece una serie de supuestos en los que se legitima el tratamiento de datos personales sin consentimiento del interesado. A estos efectos, es necesario que recordemos los apartados d) y e) de dicho artículo, en los que se expresaba que el responsable del tratamiento podía encontrar la base jurídica del tratamiento en la protección *"de los intereses vitales del interesado o de otra persona física"* y por motivos de interés público, respectivamente. Asimismo, el Considerado 46 del RGPD establece que estos tratamientos pueden llevarse a cabo cuando sea necesario *"para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria…"*

En la situación actual de pandemia (COVID-19) en la que nos encontramos cabe preguntarse si pueden ser lícitos determinados tratamientos de datos personales llevados a cabo en situaciones excepcionales y, en su caso, quién puede realizarlos y con qué limitaciones. Sobre estas cuestiones se ha pronunciado la AEPD en su Informe

0017/2020, en el que afirma que dicho tratamiento encuentra su base jurídica en el artículo 6.1, pero que, además, es necesario "que exista una circunstancia que levante la prohibición de tratamiento de dicha categoría especial de datos", lo que según la AEPD se puede localizar en el art 9.2 RGPD en sus apartados b), c), g), h), i) siendo especialmente relevante este último en cuanto se refiere a interés público calificado como "protección frente a amenazas transfronterizas graves para la salud". (Sáenz, 2020).

Una vez fijadas la base jurídica del tratamiento y las circunstancias especiales que lo habilita, la AEPD sostiene que el responsable del tratamiento en cumplimiento de la normativa de protección de datos podrá adoptar las decisiones necesarias para la "salvaguarda de los intereses vitales y esenciales en el ámbito de la salud pública, siguiendo la normativa material aplicable.", que en el caso de España son la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública y la Ley 33/2011, de 4 de octubre, General de Salud Pública, en virtud de las cuales se otorgan competencias a las autoridades sanitarias de las AAPP para adoptar dichas medidas.

Los responsables del tratamiento, siguiendo las instrucciones de las autoridades sanitarias de las AAPP, podrán tratar datos personales relativos a la salud de las personas físicas con el fin de comunicar a las personas físicas con las que un contagiado haya tenido contacto la posibilidad de contagio y advertirles para que eviten la propagación de la enfermedad a terceras personas. (AEPD, Informe 0017/2020).

Del mismo modo, según señala la AEPD, en el ámbito laboral también cabría acogerse al artículo 6.1 c)[20] para el tratamiento, que en relación con el art. 9.2 b) RGPD impone que el trabajador deberá "informar a su empleador en caso de sospecha de contacto con el virus" pudiendo el empleador tratar dichos datos conforme al RGPD, adoptando "las medidas de seguridad y responsabilidad proactiva que demanda el tratamiento", siguiendo la normativa laboral, para garantizar la salud de los empleados y evitar contagios en los centros de trabajo.

[20] En cumplimiento de una obligación legal aplicable al responsable del tratamiento

Por último, la AEPD destaca que la excepcionalidad de las circunstancias no implica que la normativa de protección de datos personales no siga vigente, por lo que solo en las condiciones señaladas anteriormente podrá llevarse a cabo el tratamiento de datos personales sin el consentimiento del interesado. A este respecto, la AEPD señala que no puede "confundirse conveniencia con necesidad", por lo que esta circunstancia no puede dar lugar a tratamientos de datos personales por "terceros, empresarios, compañías de seguros o entidades bancarias", con otros fines.

En el ámbito de las aplicaciones móviles, no han sido pocos los casos de cibercriminales que han aprovechado estas circunstancias para obtener datos personales de terceros, robar dinero u otras estafas, a través de suplantaciones al Ministerio de Sanidad y a la OMS. (Juárez, 2020). Del mismo modo, la AEPD tiene constancia de que muchas empresas se están extralimitando en el tratamiento de datos personales, por lo que, con fecha 26 de marzo de 2020 la AEPD emitió un comunicado en el que analiza las incidencias que tiene el COVID-19 en el tratamiento de datos a través de APPS y webs de autoevaluación de la enfermedad.

En el presente comunicado, la AEPD recuerda que la única finalidad para la que puede realizarse el tratamiento de datos personales es el control de la epidemia[21], de tal forma que las autoridades públicas competentes, están autorizadas para tratar los datos que "consideren proporcionados o necesarios para cumplir con dicha finalidad" y las empresas privadas que lleven a cabo tratamientos solo podrán hacer bajo las instrucciones de dichas autoridades.

En los últimos días, no ha estado libre de polémica la decisión del Gobierno de habilitar al Ministerio de Sanidad para comprobar la geolocalización de los ciudadanos a través de sus dispositivos móviles con el objetivo de verificar que la cuarentena se está cumpliendo por los ciudadanos. A este respecto, la AEPD señala que se trata de competencias excepcionales dirigidas a "limitar la libertad de circulación de las personas" como consecuencia del estado de alarma, así como a conocer las zonas con mayor número de afectados por el COVID-19. En todo caso, señala la AEPD que el único dato personal

[21] Principio de limitación de la finalidad llevado a la práctica.

que será tratado a este respecto sería "el correspondiente al número de teléfono móvil", salvo que se considerase imprescindible para la erradicación y seguimiento de la enfermedad algún otro dato diferente.[22]

CAPÍTULO VI.

CONCLUSIONES

Tras el desarrollo del presente trabajo hemos podido comprobar que no son pocos los riesgos que plantean a la privacidad los nuevos dispositivos electrónicos. Hemos observado como la falta de transparencia que implican las Políticas de Privacidad incomprensibles y farragosas que suelen diseñar los desarrolladores de aplicaciones no cumplen con el deber de informar a los usuarios de los datos exactos que se van a recoger y la finalidad exacta para la que se va a realizar el tratamiento. Además, hemos podido comprobar que en muchas ocasiones las aplicaciones no dan la posibilidad otorgar un consentimiento específico al tratamiento de datos, sino que se nos incita a aceptar casillas a través de las cuales consentimos un tratamiento generalizado de nuestros datos. Estas circunstancias en opinión del Dictamen 02/2013 y de los autores que hemos ido mencionando a lo largo del presente trabajo dan lugar a consentimientos inválidos y a tratamientos de datos realizados de forma ilegítima.

Estos riesgos, unidos a la dificultad de identificar a los responsables de un tratamiento de datos ilegítimo como consecuencia de la gran cantidad de actores involucrados en el desarrollo y funcionamiento de una aplicación o dispositivo móvil, provocó que el GT29 en su Dictamen 02/2013 se pronunciase sobre las obligaciones específicas que los desarrolladores de aplicaciones y dispositivos móviles debían cumplir a la hora de desarrollar una aplicación móvil. No obstante, la redacción de dicho Dictamen 02/2013 se realizó atendiendo a la normativa existente en aquella época, esto es, la Directiva 95/46/CE que entró en vigor cuando aún no existían los teléfonos móviles ni sus aplicaciones. Esta circunstancia unida al hecho de que la anterior Directiva no preveía

[22] Medida en coherencia con el principio de minimización de datos.

sanciones demasiado rigurosas para los desarrolladores que incumplieran sus preceptos, ha dado lugar a numerosos tratamientos ilícitos de datos personales en dispositivos móviles.

Hemos observado, que con la llegada del nuevo RGPD los desarrolladores de aplicaciones y dispositivos móviles, así como las tiendas de aplicaciones y fabricantes de sistemas operativos deberán implantar las medidas necesarias para garantizar la protección de los datos personales de sus usuarios y hacer frente a los riesgos que plantean a la privacidad los nuevos dispositivos electrónicos desde el diseño de la propia aplicación, siguiendo el nuevo principio de privacidad por diseño introducido por el RGPD.

A raíz de esta nueva regulación, los desarrolladores de aplicaciones tendrán que tomarse más en serio la legalidad de la aplicación móvil, y para ello tras un estudio exhaustivo de los principios regulatorios más importantes en el ámbito de las aplicaciones móviles, podemos extraer del presente trabajo una serie de medidas y recomendaciones que les ayudarán a cumplir con la normativa vigente:

- Llevar a cabo una Informe de Análisis de Impacto de la Privacidad (PIA) y auditorías independientes de forma previa a la comercialización de la APP para garantizar el cumplimiento de la legalidad.
- Identificar claramente en la Política de Privacidad quién es el responsable del tratamiento y si los datos serán transferidos a terceros.
- Indicar a que datos exactos tendrá acceso la aplicación y la finalidad que legitima el tratamiento, limitando al mínimo la recogida de datos personales.
- Exponer la base jurídica que legitima el tratamiento de datos personales.
- Informar al usuario sobre los derechos que le asisten y facilitarle los mecanismos o la información que les permita ejercer dichos derechos.
- Presentar la información por capas, de manera que, en la pantalla principal a la hora de instalar la aplicación, el usuario pueda observar la información básica, facilitándole un enlace directo a toda aquella información adicional que sea necesaria.

- Que el consentimiento que se recoja del usuario sea "informado", "específico", "libre", "inequívoco" y se trate de una acción claramente afirmativa: Para el cumplimiento de estos requisitos, el desarrollador tendrá que abandonar prácticas frecuentes como son: el presentar celdas premarcadas a la hora de solicitar el consentimiento, el presentar solamente una opción para aceptar el tratamiento sin ofrecer al usuario la posibilidad de mostrar su negativa a la aceptación, el habilitar sistemas para obtener un consentimiento global al tratamiento de los datos personales, en lugar de dar la posibilidad al usuario de aceptar cada tratamiento de forma individualizada, y considerar el silencio o la inactividad como un consentimiento tácito.
- Informar en menos de 72 horas de cualquier brecha de seguridad que comprometa la privacidad de los usuarios.
- Redactar la Política de Privacidad en un lenguaje comprensible para el ciudadano medio y situarla en la aplicación de forma que sea fácilmente localizable en cualquier momento.
- Otorgar al usuario la posibilidad de revocar el consentimiento en cualquier momento y de forma fácil y sencilla.
- Implantar las medidas de seguridad que cada desarrollador estime conveniente para la protección de la intimidad de sus usuarios y que se desarrollan en el apartado IV.3.

En caso de que un desarrollador no actúe con la suficiente diligencia en el cumplimiento de la normativa y de las medidas descritas, debe saber que la AEPD ha comenzado a aplicar el endurecimiento de las sanciones previstas en el RGPD, como hemos podido comprobar con el caso LaLiga. Esta resolución ha sido duramente criticada por algunos expertos abogados en protección de datos como Muñoz Ontier que argumentan que la AEPD no ha hecho esfuerzos suficientes para comprender el funcionamiento de la tecnología que usa la aplicación y que en ningún momento se recogen datos personales a través del micrófono a pesar de que pueda parecer lo contrario.

En mi opinión, este caso puede servir como precedente para aconsejar a los desarrolladores de aplicaciones que no dejen lugar a dudas e interpretaciones sobre si

están cumpliendo o no la normativa regulatoria de la protección de datos, ya que parece que la tendencia de la AEPD a partir de ahora será claramente sancionadora. Los desarrolladores de aplicaciones deben, por tanto, cumplir estrictamente la normativa en protección de datos, así como las medidas descritas en el presente trabajo y dar un paso al frente en el ámbito de la protección de la privacidad, para evitar cualquier sanción por parte de la AEPD y garantizar la defensa de la privacidad de sus usuarios.

BIBLIOGRAFÍA

LEGISLACIÓN Y JURISPRUDENCIA

Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, adoptado el 27 de febrero de 2013 (00461/13/ES; WP 202)

Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", adoptado el 16 de febrero de 2010 (00264/10/ES; WP 169)

Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, adoptado el 16 de mayo de 2011 (881/11/ES; WP 185)

Dictamen 15/2011 sobre la definición del consentimiento, adoptado el 13 de julio de 2011 (01197/11/ES; WP 187)

Dictamen 2/2010 sobre publicidad comportamental en línea, adoptado el 22 de junio de 2010 (00909/10/ES; GT 171)

Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007 (01248/07/ES; WP 136)

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (DOCE, núm. 281, de 23 de noviembre de 1995.)

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.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE, núm. 294, de 6 de diciembre de 2018).

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de 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).

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

Sentencia de la Audiencia Nacional de 25 de mayo de 2006 (Sala de lo Contencioso-Administrativo, Sección 1ª) (FJ 5º) SAU 25-5-2006 (JUR 2006/ 174370)

LIBROS

Álvarez Hernando, J. (2015). *"Grandes Tratados. Practicum Protección de Datos 2015."* Madrid: Editorial Aranzadi

De Miguel Asensio, P.A. (2015). *"Estudios y Comentarios Legislativos (Civitas). Derecho Privado de Internet"* Madrid: Editorial Aranzadi.

ARTÍCULOS DE REVISTA

Flaquer Riutort, J. (2018) Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy). *Revista Aranzadi de Derecho y Nuevas Tecnologías,* (47), 1-24.

Paniza Fullana, A. (2017) Una nueva era en la privacidad y las comunicaciones electrónicas: 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. *Revista Doctrinal Aranzadi Civil-Mercantil,* (7), 105-122.

Reyes Rico, L. (2019). Límites de la normativa de protección de datos a la creación de perfiles con fines comerciales. *Actualidad Jurídica Aranzadi.* (953), 7-8.

Solar Calvo, P. (2018) Nueva regulación Europea en protección de datos. Urgente necesidad de una normativa nacional. *Revista Aranzadi Unión Europea.* (7), 1-13.

Villarino Marzo, J. (2013). La privacidad desde el diseño en la propuesta de reglamento europeo de protección de datos. *Revista Aranzadi de Derecho y Nuevas Tecnologías.* (33) 45-68.

CAPÍTULOS DE LIBRO

Adsuara Varela, B. (2018). El ciudadano frente al Reglamento. En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. (163-172) Madrid: Bosch

Álvarez Rigaudias, C. (2018) El tratamiento y sus responsables (Arts. 26-29) En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (433-442) Madrid: Bosch

Aparicio Salom, J. (2018) Derechos del interesado (Arts. 12-19) En López Calvo, J. (coord.) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (363-400) Madrid: Bosch

Brito Izquierdo, N. (2018) Recursos, responsabilidad y sanciones (arts. 77-84). En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (634-670) Madrid: Bosch

Cervera-Navas, L. (2018) El nuevo modelo europeo de protección de datos de carácter personal En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (70-74). Madrid: Bosch

Costa Hernanis, R. (2018) Responsabilidad del responsable del tratamiento (Art.24). En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (419-425) Madrid: Bosch.

Fernández Acevedo, J. (2018) Redes sociales y aplicaciones móviles En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (223-248). Madrid: Bosch.

García Mexía, P. y Perete Ramírez, C. (2018) Internet y el Reglamento General de Protección de Datos En López Calvo, J. (coord) *El nuevo marco regulatorio*

derivado del Reglamento Europeo de Protección de Datos. (173-194). Madrid: Bosch.

López Calvo, J. (2018). Cooperación y coherencia (Arts. 60-70). En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (609-632). Madrid: Bosch

Martos, N. (2018). Principios (Arts 6-11). En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (353-362). Madrid: Bosch

Miralles López, R. (2018). Protección de datos desde el diseño y por defecto (Art. 25). En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (427-431)

Miralles López, R. (2018). Derecho de portabilidad (Art. 20) En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (401-408) Madrid: Bosch.

Muñoz Ontier, J. (2018). Disposiciones Generales (Arts. 1-5) En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (335-351). Madrid: Bosch.

Rallo Lombarte, A. (2018) España en la vanguardia de la Protección de Datos: nuevos retos del Reglamento Europeo. En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (75-80). Madrid: Bosch.

Vidal Laso, M. y Aparicio Salom, J. (2019) Elemento subjetivo de la relación: las partes. En Aranzadi (ed), *Estudio sobre la protección de datos*, Madrid: Thomson Reuters.

Villarino Marzo, Jorge (2018) La Internet de las Cosas y el Reglamento General de Protección de Datos. En López Calvo, J. (coord) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* (301-312). Madrid: Bosch

REFERENCIAS DE INTERNET

AEPD (2018) Decálogo para la adaptación al RGPD de las políticas de privacidad en internet. Obtenida el 10/4/2020 de https://www.aepd.es/sites/default/files/2019-09/decalogo-politicas-de-privacidad-adaptacion-RGPD.pdf

AEPD (2018) Guía para el cumplimiento del deber de informar. Obtenida el 10/4/2020 de https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

AEPD (2019) Resolución de Procedimiento Sancionador PS/00326/2018. Obtenida el 15/4/2020 de https://www.aepd.es/es/documento/ps-00326-2018.pdf

AEPD (2019) Nota Técnica: Avance del estudio de IMDEA NETWORKS y UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios". Obtenida el 30/3/2020 de https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-IMDEA-android.pdf

AEPD (2019) El deber de informar y otras medidas de responsabilidad proactiva en Apps para dispositivos móviles. Obtenida el 10/4/2020 de https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf

AEPD (2020) Informe COVID-19 N/REF: 0017/202. Obtenida el 13/4/2020 de https://www.aepd.es/es/documento/2020-0017.pdf

AEPD (2020) Comunicado de la AEPD sobre apps y webs de autoevaluación del Coronavirus. Obtenida el 13/4/2020 de https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

Biurrun Abad, F. (2017) Accountability o responsabilidad activa en el Reglamento General de Protección de Datos. LEGALTODAY. Obtenida el 19/4/2020 de http://www.legaltoday.com/gestion-del-despacho/nuevas tecnologias/articulos/accountability-o-responsabilidad-activa-en-el-reglamento-general-de-proteccion-de-datos

Castrillo de la Fuente, M. (2018) Datos de contacto profesionales y su regulación en el Reglamento Europeo de Protección de Datos. PRODAT. Obtenida el 19/4/2020 de https://www.prodat.es/blog/los-datos-de-contacto-profesionales-y-su-regulacion-en-el-reglamento-europeo-de-proteccion-de-datos.html

Cives, J. (2017) Datos profesionales: ¿datos personales? LEGALTODAY. Obtenida el 19/4/2020 de http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-ecija-2-0/datos-profesionales-datos-personales

Marín López, J.J (2013) La protección de datos en las aplicaciones de los dispositivos inteligentes. Gómez-Acebo y Pombo. Obtenida el 24/2/2020 de https://www.ga-p.com/wp-content/uploads/2018/03/la-proteccion-de-datos-en-las-aplicaciones-de-los-dispositivos-inteligentes.pdf

Piñar Real, A. (2019) Los menores de edad en el Reglamento General de Protección de Datos. LEVEBVRE. Obtenida el 17/4/2020 de https://elderecho.com/los-menores-de-edad-en-el-reglamento-general-de-proteccion-de-datos

Calle, C. (2018) GDPR: atención al derecho de portabilidad de los datos. KPMG Tendencias. Legal. Obtenida el 16/4/2020 de https://www.tendencias.kpmg.es/2018/06/gdpr-derecho-portabilidad-datos/

ARTÍCULOS DE PRENSA

Juárez, B. (2020, 9 de marzo). Los cibercriminales suplantan al Ministerio de Sanidad para robar datos a los usuarios de Whatsapp. *El País.* Obtenido el 13/4/2020 de https://elpais.com/tecnologia/2020-03-09/los-cibercriminales-suplantan-al-ministerio-de-sanidad-para-robar-datos-a-los-usuarios-de-whatsapp.html

Roger Shultz, C.C (2011, 18 de mayo). Se prohíbe la geolocalización activada de serie en "smartphones" y "tablets". *Europa Press.* Obtenido el 1/04/2020 de https://www.europapress.es/portaltic/software/noticia-prohibe-geolocalizacion-activada-serie-smartphones-tablets-20110518185833.html

Sáenz, M. (2020, 17 de marzo). Covid-19 y tratamiento de datos personales. Informe de la AEPD. *Observatorio de RRHH* (Obtenido el 14/04/2020 de https://www.observatoriorh.com/orh-posts/covid-19-y-tratamiento-de-datos-personales-informe-de-la-aepd.html).

Sánchez, L.J. (2019, 12 de junio). La Audiencia Nacional dictaminará si la Liga de Fútbol Profesional utilizó datos personales en el micrófono de su aplicación móvil. *Confilegal*. Obtenido el 17/4/2020 de https://confilegal.com/20190612-la-audiencia-nacional-dictaminara-si-la-liga-de-futbol-profesional-utilizo-datos-personales-en-el-microfono-de-su-aplicacion-movil/