La privacidad en las aplicaciones móviles

Estudio del cumplimiento del marco jurídico aplicable al tratamiento de datos personales en el ámbito de la UE

Juny 2014

Autors:
Carlos López Martínez
Cristina Cos Pedraza

MENCIÓ ESPECIAL DEL MASTER EN DRET DE SOCIETAT DE LA INFORMACIÓ
2013-2014

EdicionsDigitals

Barcelona 2014

Edita: Biblioteca de l'Il·lustre Col·legi d'Advocats de Barcelona.
Mallorca 283, 08037 Barcelona
http://www.icab.cat e-mail: biblioteca@icab.cat

Primera edició, 2014
www.icab.cat

D.L. B. 20916-2014

Abstract

Actualmente, existen miles de aplicaciones dirigidas a un conjunto de dispositivos inteligentes que, con el fin de proporcionarnos distintos servicios que nos faciliten las tareas y actividades cotidianas, pueden recabar cantidades ingentes de datos.

Gran parte de los datos disponibles en un dispositivo móvil inteligente son de carácter personal. Por lo tanto, es absolutamente necesario que los múltiples actores que intervienen en el desarrollo de aplicaciones conozcan y apliquen las normas de protección de datos.

Sin embargo, la realidad es que la falta de conocimiento por el usuario final de los tipos de tratamiento que las aplicaciones pueden realizar, la ausencia de consentimiento específico por su parte antes de que se produzca el tratamiento y el alto grado de fragmentación de los agentes que intervienen en el desarrollo, la comercialización y la explotación de las aplicaciones, suponen un riesgo importante para la vida privada y la reputación de los usuarios.

El objeto de esta tesina es poner de manifiesto que un porcentaje importante de las aplicaciones más descargadas no cumple el marco jurídico aplicable al tratamiento de datos personales en el ámbito de la UE. Para ello, se ha tomado como base de este estudio el Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes del Grupo de Trabajo del Artículo 29[1] sobre Protección de Datos o WP (*Working Paper*) 202 (en adelante, el Dictamen) así como la legislación europea y española en materia de protección de datos. Por otro lado, la información publicada por la Doctora canadiense Ann Cavoukian ha sido de gran ayuda para abordar el punto relativo a *Privacy by Design*.

Finalmente, se debe hacer especial mención al proyecto español PATiA, impulsado por la Universidad de León, que analiza las aplicaciones gratuitas más populares de la *App Store* que ha sido muy útil para realizar la auditoría comparativa de respeto a la privacidad entre las aplicaciones *iOS* y *Android* que recoge esta tesina.

[1] Se trata de un órgano consultivo europeo independiente en materia de protección de datos y privacidad. Su cometido, resumidamente, es: aconsejar a los Estados miembros en materia de protección de datos, promover la aplicación homogénea de la legislación europea y emitir dictámenes en relación con esta materia.

Índice

1. Introducción

La voracidad tecnológica es algo que socialmente ha ido acaparando el estilo de vida de la ciudadanía a través de los años. Leer el periódico en papel, realizar la lista de la compra en una libreta, pedir un taxi o incluso hacer deporte únicamente con el equipamiento esencial son cosas que, posiblemente, ya sólo quedan para los románticos.

Nos encontramos con un panorama ya bautizado como la *appificación* en el que, generosamente, o no, se nos brindan un sinfín de posibilidades para nuestros dispositivos móviles con el pretexto de hacernos la vida más fácil. La era tecnológica nos conduce hacia un estilo de vida en el que cada ciudadano ahora ya tiene una aplicación para cada tarea en concreto, por lo que, desde un único dispositivo, podemos realizar actividades tan dispares como la lista de la compra, enviar correos electrónicos, ojear noticias, compartir fotografías o documentos, realizar una videoconferencia a cualquier lugar del mundo… y todo ello sin necesidad de sentarnos ante un ordenador.

Esta *appificación* está tan presente que a nivel mundial, en 2013, se estimaba que las tiendas de aplicaciones o *stores* recibían diariamente 1.600 aplicaciones nuevas y cada usuario medio descargaba de promedio 37 aplicaciones. En este sentido, los datos siguen en auge y de los 68 mil millones de dólares en los que se valoraba entonces este mercado, actualmente, se estima que para el 2016 este valor aumente hasta 143 mil millones. Uno de los factores que pueden contribuir a ello, además de la tendencia social a descargar más, es la aparición de otras *stores* que, junto a las grandes *App Store* de Apple y *Play Store* de Google, están ganando adeptos.

Pero, en el uso de estas aplicaciones ¿qué ocurre con nuestros datos? Con este afán de facilitar nuestras tareas cotidianas, las aplicaciones nos ofrecen cada vez más oportunidades; ya no sólo nos permiten hacer la lista de la compra, sino también localizar qué comercio tiene el mejor precio y cuál es su situación, o conocer qué rutas de *running* hacen otros usuarios o si tenemos a alguno alrededor. Resulta evidente, pues, que para que las aplicaciones puedan funcionar y ofrecernos el servicio para el que han sido desarrolladas, se nutren de los datos almacenados en nuestros dispositivos inteligentes o generados por estos, datos que, en muchos casos, son de carácter personal.

El problema es que, en numerosas ocasiones, el tratamiento de datos no se ciñe únicamente y exclusivamente a la prestación del servicio concreto de la aplicación, sino que los datos pueden ser objeto de un tratamiento adicional, normalmente para generar ingresos, de manera desconocida o no deseada por el usuario final.

La finalidad de la presente tesina es establecer el marco jurídico aplicable al tratamiento de datos personales y poder así determinar en qué medida los distintos actores intervinientes en el ecosistema de las aplicaciones lo cumplen, con los riesgos que para los usuarios comporta un cumplimiento parcial o laxo de la normativa.

2. Regulación: normativa aplicable

¿Qué ley nos da la definición legal de "aplicación" de dispositivo inteligente? Haciendo un examen de la legislación, ya sea europea o nacional, observamos que la definición como tal no existe. Por este motivo tenemos que recurrir a la que mejor se ajuste a sus características.

El Dictamen define las aplicaciones (en adelante, apps) como programas de ordenador. En este sentido tenemos que recurrir al art. 96 del Texto Refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, que define el programa de ordenador como "*toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuera su forma de expresión y fijación*". Entendemos que dicha definición se ajusta a la naturaleza de las apps, en tanto que éstas utilizan los códigos objeto y fuente como secuencia de instrucciones destinadas a ser utilizadas por un sistema operativo instalado en el dispositivo, con el objeto de realizar una función o tarea determinada (enviar mensajes, realizar llamadas…).

Situado el concepto de "aplicación", dentro del ámbito de la Unión Europea la regulación de la privacidad o protección de datos en las apps se encuentra, básicamente, en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva sobre protección de datos), siempre que en la gestión de dichos programas haya tratamiento de datos personales. Esta normativa, a nivel nacional, ha sido transpuesta en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

En la materia se puede tener en cuenta a la hora de trabajar con aplicaciones de dispositivos móviles la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico para, por ejemplo, la descarga de aplicaciones de pago, o el Texto Refundido de la Ley de Propiedad Intelectual, en tanto que éste protege expresamente los programas de ordenador en su art. 10.1.i). No obstante, el objeto de esta tesina se limitará al estudio de la Directiva sobre protección de datos haciendo mención a la regulación en la LOPD y a su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Para determinar si esta legislación es aplicable cuando una app es utilizada por un usuario de la Unión Europea, en primer lugar, es necesario identificar al responsable del tratamiento. Según el artículo 4.1.a) de la Directiva sobre protección de datos, la legislación nacional de un Estado miembro es aplicable a todo tratamiento de datos personales efectuado en el marco de las actividades de un establecimiento del responsable en el territorio de dicho Estado Miembro. Pero, ¿qué pasa con esas aplicaciones cuyo responsable está establecido en un Estado extracomunitario? La Directiva sobre protección de datos establece que en estos casos aplicaría el art. 4.1.c) en cuanto establece que la legislación nacional de un Estado miembro también se aplica cuando el responsable del tratamiento no está establecido en el territorio de la UE pero hace uso de equipos situados en el territorio de ese Estado Miembro. La manera que encuentra el Grupo de Trabajo del Art. 29 de aplicar nuestra legislación cuando el responsable no está establecido en la UE, es entendiendo que el dispositivo inteligente es precisamente lo que la Directiva llama "equipos situados en el territorio".

3. Las apps y el riesgo para la protección de los datos

Una vez introducido el concepto de "app" y establecida qué legislación es aplicable en materia de protección de los datos de carácter personal, tenemos que pasar a analizar los riesgos que pueden comportar para la intimidad de sus usuarios.

En primer lugar, hay que tener en cuenta que las aplicaciones organizan la información de acuerdo con las características específicas del dispositivo y suelen interactuar estrechamente con el soporte físico y las características del sistema operativo del mismo. Esto significa que estas aplicaciones, en muchos casos, se harán valer del propio dispositivo por cuanto incluye *software* o estructuras de datos y *hardware.* Estos componentes se encuentran abiertos a dichas apps mediante interfaces de programación de aplicaciones o API[2] que dan acceso a multitud de sensores como brújulas, cámaras, micrófonos o sensores de proximidad. Gracias a estas interfaces las aplicaciones pueden cumplir con la finalidad que publicitan, como acceder a los contactos para el envío de mensajería instantánea o al geolocalizador para el cálculo de una ruta vial, entre otras.

En su interacción con el sistema operativo las apps realizan una gran recogida de datos a partir del dispositivo, datos que, muchas veces, no podemos identificar quién está tratándolos ya que en el proceso de creación y gestión intervienen tantos actores que pueden hacerlos peligrar. El motivo es que a menudo, estos actores intervinientes, ya sean expertos informáticos o no, crean las apps sin tener conocimiento de la legislación en materia de protección de datos provocando riesgos significativos para la vida privada y la reputación de los usuarios de dispositivos.

Decimos que se provocan riesgos significativos para la vida privada y la reputación de los usuarios porque, en última instancia, no podemos olvidar que muchos de los datos que se generan o se almacenan a partir de los dispositivos son datos personales en el sentido de nuestra LOPD, es decir, datos de una persona física que puede ser identificada o identificable por el responsable del tratamiento o un tercero. Y si además tenemos en cuenta que los datos a los que pueden acceder estos agentes no son sólo del propietario del dispositivo, sino que también pueden ser de terceras personas con las que se pueda relacionar el propietario a través del listado de contactos, es evidente que los riesgos se multiplican.

En este sentido, el Grupo de Trabajo del Art. 29 adoptó el 27 de febrero de 2013 el *Working Paper* 202 o Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, que se centra precisamente en analizar la forma de hacer efectivos los principios de la protección de datos personales en las aplicaciones. Así pues, este Dictamen trata el requisito del consentimiento, los principios de limitación de la finalidad y de minimización de datos, la necesidad de adoptar medidas de seguridad adecuadas, la obligación de informar correctamente a los usuarios finales y de respetar sus derechos, los periodos de conservación razonables y, especialmente, el tratamiento leal de los datos recopilados a partir de niños o sobre ellos.

Una de las principales preocupaciones del Dictamen, además, es la diversidad de los actores que intervienen en el desarrollo de las apps pues, como apuntábamos anteriormente, estos pueden poner en riesgo los datos personales que tratan las apps debido a una posible falta de transparencia y conocimiento de los tipos de tratamiento que las apps pueden realizar combinada con la falta de

[2] Interfaz de programación de aplicaciones (IPA) o API (del inglés *Application Programming Interface*) es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro *software* como una capa de abstracción. Son usadas generalmente en las bibliotecas.

consentimiento significativo por parte de los usuarios finales antes de que se produzca el tratamiento de datos.

Para tratar de evitar todos estos riesgos a los que hemos hecho mención, el Dictamen plantea una serie de directrices dirigidas a los agentes intervinientes en la creación y comercialización de las apps. Estos agentes son los desarrolladores de aplicaciones, los fabricantes de sistemas operativos y de dispositivos, las tiendas de aplicaciones y las terceras partes (básicamente, redes publicitarias y proveedores de análisis), y todos ellos tienen su parcela de responsabilidad en relación con los datos personales tratados por las apps, responsabilidad que analizaremos en el punto dedicado a *Privacy by Design*. En este sentido cabe avanzar que, en la mayoría de los casos, todos estos agentes actúan como responsables del tratamiento y, por lo tanto, les serán de aplicación las directrices expuestas en el Dictamen y que son las siguientes:

3.1. **Consentimiento previo a la instalación y tratamiento de datos personales** (art. 6 de la LOPD)

Al instalarse una app, sólo con este hecho, ya se está introduciendo información en el dispositivo del usuario final, es más, muchas aplicaciones incluso ya están accediendo a los datos almacenados en dispositivo, como bien podrían ser los contactos. Con el fin de evitar que esto ocurra, el Dictamen nos remite al art. 5.3 de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que establece una norma específica a nivel mundial para todas las partes interesadas en almacenar o acceder a datos almacenados en los dispositivos de los usuarios del Espacio Económico Europeo (EEE). Este art. determina que *"los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos […]"*.

El consentimiento al que hace referencia se aplica a toda la información, independientemente de la naturaleza de los datos que se almacenan o a qué se accede. Por lo tanto, el requisito del consentimiento no se limita a los datos personales y afectará a todo residente en el EEE con independencia del lugar en que se encuentre el proveedor de servicios.

En definitiva, el consentimiento debe solicitarse previamente a la captación de los datos en todo caso y éste, además, debe solicitarse después de haber informado de manera clara y completa sobre qué datos se van a tratar y con qué finalidades.

Llegados a este punto debemos diferenciar entre el consentimiento para el tratamiento de los datos personales y el que se requiere para introducir o leer información en el dispositivo, que pudiéndose dar simultáneamente o no, ambos deben operar bajo las condiciones de ser libre, especifico e informado (art. 2.h) de la Directiva sobre protección de datos).

En este sentido, el Dictamen entiende que la manifestación de voluntad "libre" se da cuando el usuario tiene la opción de aceptar o rechazar el tratamiento de sus datos personales sin verse forzado a tener que elegir una opción única de "Sí, acepto" para completar la instalación. El usuario debe poder elegir una opción de "Cancelar" o poder detener la instalación.

La manifestación de voluntad "informada" significa que el interesado debe disponer de todos los datos necesarios para formarse una opinión precisa, lo que implica que la misma esté disponible antes de que se produzca cualquier tratamiento de datos personales.

El tercer requisito del consentimiento es que sea "específico", lo cual significa que el mismo se refiera a un dato o un tipo de datos concretos. Es por ello que el Dictamen considera que la simple pulsación de un botón "Instalar" no puede considerarse consentimiento válido para el tratamiento de datos personales, ya que el consentimiento no puede consistir en una autorización formulada en términos generales. Sería más ajustado que el usuario final pudiera prestar un consentimiento diferenciado o "granular" para satisfacer dos importantes requisitos legales: el de informar al usuario sobre elementos importantes del servicio y la solicitud de consentimiento específico para cada uno de ellos. Con el objeto de evitar que los desarrolladores de apps puedan evadir estas normas, el Dictamen aclara que tampoco se dará por dado el requisito de consentimiento con la aceptación de una larga serie de términos y condiciones y/o de la política de privacidad.

Junto a lo anterior, se añade que el consentimiento "específico" también se refiere a la práctica del seguimiento del comportamiento de los usuarios por parte de anunciantes y otras terceras partes.

No obstante, el Dictamen señala que incluso si se cumplen estos tres elementos, ello no permite tratamientos ilícitos o desleales, pues "*si la finalidad del tratamiento es excesiva y/o desproporcionada, incluso cuando el usuario haya dado su consentimiento, el desarrollador de apps no tendrá un fundamento jurídico válido y es probable que esté infringiendo la Directiva sobre protección de datos*".

Uno de los problemas a los que nos enfrentamos ahora es ¿qué ocurre con las apps que vienen preinstaladas en el dispositivo como el tiempo o la alarma? El Dictamen insta a los responsables del tratamiento a estudiar si realmente hay un consentimiento válido tal y como hemos estudiado anteriormente y, para ello, sugiere que se dé un mecanismo de consentimiento por separado mediante el cual, al abrirse la aplicación por primera vez, se soliciten todos los permisos, ya que no ha existido momento previo de descarga para el usuario final.

Por último, se debe de ofrecer la posibilidad al usuario final de retirar el consentimiento de forma sencilla y eficaz, aspecto que veremos más desarrollado en el punto referente a los derechos del interesado.

Suponiendo que la app cumple con todos los requisitos mencionados sobre el consentimiento, una vez ésta ha sido instalada, ya puede disponer de aquellos datos cuyo consentimiento ha obtenido en virtud de su vínculo contractual y atendiendo a la naturaleza de la misma, pues de otra manera no podría funcionar. Es decir, cuando una app solicita un dato como por ejemplo un número de teléfono, cada vez que la misma va a requerirlo para poder funcionar no necesita reclamarlo de nuevo.

3.2. **Limitación de la finalidad y minimización de datos** (art. 4 apartados 1 y 2 de la LOPD)

Otro de los pilares sobre los que se basa la legislación sobre protección de datos es el deber de informar de manera clara antes de realizar el tratamiento que, los datos personales sobre los que los usuarios prestan su consentimiento serán destinados a una finalidad leal y lícita, y que únicamente se recogerán los datos que sean necesarios para la función de la app.

Por un lado, la limitación de la finalidad hace referencia a que el usuario, como ya hemos comentado sucintamente, va a poder optar deliberadamente por confiar sus datos personales ya que conocerá

previamente el uso que se les va a dar. Para ello se requiere que, antes de la recogida de los datos personales, los desarrolladores de apps definan sus argumentos comerciales y así evitar la posibilidad de cambios súbitos de las condiciones claves del tratamiento, pues ello supondría tener que dirigirse a todos los usuarios individualmente y solicitar su consentimiento previo e inequívoco para esa nueva finalidad del tratamiento.

Por otro lado, el principio de minimización de datos trata de evitar el tratamiento de datos innecesarios y potencialmente ilícitos ciñéndose a los estrictamente necesarios para cumplir con la función para la que fue creada la app. Hay que tener en cuenta, además, que la mayoría de las tiendas de aplicaciones ofrecen actualizaciones (semi)automáticas que pueden incorporar nuevas atribuciones a las apps y ello puede hacer perder el control al usuario de qué datos se están tratando o si conlleva la solicitud de más permisos de acceso a datos personales. Por este motivo, el Dictamen trata de concienciar a los agentes de que informen al usuario final para que éste pueda ejercer, en su caso, el derecho a renunciar al tratamiento o al conjunto del servicio si tras una actualización no estuviera conforme.

3.3. **Necesidad de adoptar medidas de seguridad adecuadas** (art. 9 de la LOPD)

Este apartado, por su especial trascendencia y conexión con *Privacy by Design* o "privacidad desde el diseño", se desarrollará en un momento posterior de esta tesina.

Ahora bien, consideramos necesario reiterar en este punto, para seguir con el hilo del estudio, que son múltiples los agentes que intervienen en el proceso de creación, distribución y explotación de las apps y que, en la mayoría de los casos, estos son responsables del tratamiento. De conformidad con el art. 17 de la Directiva sobre protección de datos, estos agentes deben adoptar medidas técnicas y organizativas para garantizar la protección de los datos personales. Para ello, el Dictamen insta a estos actores intervinientes a tener en cuenta los principios de protección de la intimidad desde el diseño y por defecto, evaluando continuamente los riesgos actuales y futuros para la protección de los datos, y aplicando y evaluando medidas correctoras eficaces, incluyéndose la minimización de datos.

Queremos destacar en este punto la influencia que puede tener la actuación de los usuarios de aplicaciones en la seguridad en la medida en que crean y almacenan los datos personales en sus dispositivos móviles. Aunque la intervención de los usuarios es posterior al proceso de creación y distribución de las apps, un uso irresponsable de las mismas por su parte puede llegar a quebrantar la normativa sobre protección de datos. En este sentido, el Dictamen 5/2009 sobre las redes sociales en línea del Grupo de Trabajo del Artículo 29 o WP 163 establece que, "*en la mayoría de los casos, los usuarios se consideran personas interesadas. La Directiva no impone las obligaciones de un responsable del tratamiento de datos a una persona que trata datos personales en el ejercicio de actividades exclusivamente personales o domésticas. En algunos casos, la exención doméstica puede no cubrir las actividades de un usuario de servicios de redes sociales y puede entonces considerarse que el usuario ha asumido algunas de las responsabilidades de un responsable de datos. […]*

[…] La aplicación de la exención doméstica se ve también limitada por la necesidad de garantizar los derechos de los terceros, especialmente por lo que se refiere a los datos sensibles. Además, cabe señalar que, aunque se aplique la exención doméstica, un usuario puede ser responsable en virtud de las disposiciones generales del derecho civil o penal nacional en cuestión."

3.4. **Deber de información a los usuarios finales** (art. 5 de la LOPD)

La información al usuario final de la app es primordial para que el consentimiento se considere válido según las reglas ya estudiadas. A partir de los arts. 10 y 11 de la Directiva sobre protección de datos, el Dictamen dispone que cada usuario final tiene derecho a conocer, como mínimo:

- La identidad del responsable del tratamiento de datos, junto a sus datos de contacto,
- Las categorías exactas de datos personales que el desarrollador de apps recogerá y tratará,
- Los objetivos precisos o la finalidad del tratamiento,
- Si los datos se comunicarán a terceros, y
- La forma en que los usuarios pueden ejercer sus derechos (retirar el consentimiento y eliminar datos).

El consentimiento únicamente será válido si dicha información se ha ofrecido previamente al tratamiento de los datos. El Dictamen entiende que facilitarla tras el inicio del tratamiento de datos personales no es suficiente y no tiene validez jurídica.

En definitiva, es necesario informar sobre la identidad del responsable del tratamiento de los datos sin que quede en manos del usuario la tarea de investigar las relaciones entre las distintas partes intervinientes para poder ejercer sus derechos. Además, el responsable del tratamiento debe explicar, con un lenguaje claro y sencillo, qué datos se van a recoger y por qué, y si pueden ser reutilizados por otras partes y, de ser así, con qué fines. Se recomienda para ello la utilización de significadores visuales o iconos relativos al uso de los datos para informar a los usuarios de los tipos de tratamiento de datos.

A los presupuestos mínimos establecidos anteriormente, se aconseja que los responsables del tratamiento de datos informen también sobre:

- Las consideraciones de proporcionalidad en cuanto a los tipos de datos recogidos o a que se ha accedido en el dispositivo,
- Los periodos de conservación de los datos,
- Las medidas de seguridad aplicadas,
- Cómo la app se ajusta a la normativa europea de protección de datos, incluidas las posibles transferencias de datos personales desde Europa a, por ejemplo, Estados Unidos, y si se ajusta al denominado “marco de puerto seguro” y de qué manera.

Con independencia de que la información ofrecida vaya más allá o no de los requisitos mínimos establecidos por el Dictamen, se insta a los desarrolladores de apps a que diferencien de manera clara qué información es la obligatoria y cuál es la opcional, posibilitando que el usuario pueda denegar el acceso a la segunda.

En cuanto a la forma en la que se tiene que dar la información, el Dictamen determina que, como mínimo, toda aplicación debe contar con una política de privacidad legible, comprensible y fácilmente accesible, donde se incluya toda aquélla información y, en el caso de que no se recojan datos personales, también deberá especificarse este extremo. Ésta debe ofrecerse y ser accesible tanto antes de instalar la app a través de la tienda de aplicaciones, como desde dentro de la misma aplicación tras su instalación, siendo inaceptable que el usuario tenga que buscar en la web la política de tratamiento de datos de la aplicación en lugar de ser informado directamente por el desarrollador de la misma u otro responsable del tratamiento de datos, que normalmente será la tienda de aplicaciones.

En relación con lo que se acaba de exponer, el Dictamen recomienda a las tiendas de apps comprobar que todas las apps ofrecen la información esencial u obligatoria, así como que los hiperenlaces incluyen páginas de información sobre la privacidad, eliminando las apps que tengan enlaces inactivos o información inaccesible por otras razones sobre el tratamiento de datos.

Finalmente, el Dictamen hace una reflexión sobre el deber de información a los usuarios finales que gira en torno a las limitaciones físicas de los dispositivos móviles. La presentación de toda la información en una pantalla tan pequeña puede complicar el cumplimiento de las especificaciones estudiadas. Ello no debe servir como excusa para su incumplimiento, por ello se recomienda la utilización de avisos breves que, como pasa en materia de *cookies*, ofrezcan la información mínima exigida y contengan un enlace que ponga a disposición del usuario una información más completa. Esta información debe presentarse directamente en la pantalla, siendo de fácil acceso y con gran visibilidad. En última instancia, el Dictamen hace un llamamiento al sector para que desarrollen su talento creativo con el fin de informar eficazmente, pudiéndose valer de iconos, imágenes, vídeo y audio, y hacer uso de notificaciones contextuales en tiempo real cuando una aplicación accede a un tipo de dato que requiera consentimiento, como los contactos o fotografías almacenadas.

3.5. **Derechos de los usuarios finales** (arts. 15 a 17 de la LOPD)

Los derechos de acceso, rectificación, cancelación y oposición (en adelante, derechos ARCO[3]) constituyen otro gran bloque en materia de protección de datos. Los desarrolladores de apps y otros responsables del tratamiento deben permitir a los usuarios ejercerlos y, en su caso, deben proporcionarles información sobre qué datos se están tratando y la fuente de los mismos (arts. 12 y 14 de la Directiva sobre protección de datos).

Para que los usuarios puedan ejercer los derechos de acceso y rectificación, las apps deben informar a los usuarios de manera clara y visible de los mecanismos existentes. El Dictamen apunta que las herramientas de acceso deben estar accesibles preferiblemente dentro de cada aplicación o a través de un enlace a un mecanismo en línea, especialmente en los casos en que la app trata perfiles de usuarios ricos en información, como las redes sociales. Además, dicho acceso debe concederse únicamente tras haber comprobado la identidad del interesado para evitar la fuga de datos a terceros sin que, en ningún caso, esta verificación de la identidad implique recabar más datos personales.

Por otro lado, y como ya adelantamos cuando hablamos del deber de información, el Dictamen establece que el usuario final tiene que tener siempre la posibilidad de retirar su consentimiento de manera simple y cómoda, de diversas maneras y por motivos diferentes. La retirada del consentimiento debería ofrecerse a través de las herramientas de fácil acceso antes mencionadas.

Por último, se añade que debe ser posible la desinstalación de la aplicación unida a la eliminación de los datos personales, incluso de aquellos almacenados en los servidores de los responsables del tratamiento. El Dictamen propone que el sistema operativo se configure de manera que, cuando haya un borrado de una app, se envíe un aviso al desarrollador de la misma para que dé cumplimiento a la supresión de los datos personales. En caso de que los desarrolladores de apps deseen conservar determinados datos para, por ejemplo, facilitar la reinstalación de la aplicación, deben solicitar por separado el consentimiento durante la desinstalación, pidiendo al usuario su autorización durante un determinado periodo de conservación añadido. Se exceptúan de esta norma aquellos datos que por

[3] El Dictamen habla de derechos de acceso, rectificación, supresión y bloqueo de datos personales, que son los equivalentes a los derechos ARCO regulados en la legislación española.

mandato legal deban conservarse como, por ejemplo, cuando hablamos de obligaciones fiscales relativas a transacciones financieras.

3.6. Periodos de conservación (art. 4.5 de la LOPD)

Todos los datos almacenados deben serlo con carácter temporal. En este sentido, el Dictamen no determina o acota un periodo de conservación concreto pues considera que dependerá de la finalidad de la aplicación y de la relevancia de los datos para el usuario final. Así, por ejemplo, una app para compartir agendas, diarios o fotos pondría el plazo de conservación bajo el control del usuario final mientras que en el caso de una app de navegación puede bastar con almacenar sólo las últimas diez visitas hechas recientemente.

Los desarrolladores de apps deberán tener en cuenta aquellos datos de los usuarios que no hayan utilizado la aplicación durante un periodo prolongado, ya sea por haber perdido el dispositivo móvil o por haberlo cambiado por otro sin haber desinstalado activamente las apps del primero. Para estos casos, el desarrollador debe establecer previamente un periodo de inactividad a efectos de considerar expirada la cuenta e informar al usuario de ese plazo y, tras este periodo, el desarrollador deberá comunicar al usuario que puede recuperar sus datos personales. En caso de que el usuario no responda al aviso, sus datos deben hacerse anónimos o suprimirse de forma irreversible.

Finalmente, el Dictamen recuerda a las aplicaciones que "*la obligación de conservación de datos no les es aplicable y, por tanto, no puede invocarse como fundamento jurídico para seguir tratando datos sobre usuarios de aplicaciones una vez estos hayan eliminado la aplicación*."

3.7. Tratamiento leal de los datos recopilados a partir de los niños o sobre ellos (art. 13 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre)

El Dictamen concluye su análisis haciendo mención a la protección de los niños en el uso de las apps y por eso establece una serie de obligaciones que deben respetar los agentes intervinientes en el proceso de creación de las mismas. Estas obligaciones, aunque resumidas, parten del Dictamen 02/2009 sobre la protección de los datos personales de los niños del Grupo de Trabajo del Artículo 29, y consisten esencialmente en exigir a los desarrolladores de apps y otros responsables del tratamiento de datos que presten una especial atención a los límites de edad de las distintas legislaciones nacionales a efectos de solicitar, el consentimiento parental, o no, al tratamiento de datos para que éste sea lícito. En el caso de la legislación española (art. 13 del Reglamento de desarrollo de la LOPD) establece que los mayores de catorce años pueden prestar su consentimiento para el tratamiento de sus datos, de manera que para los menores de catorce años se requerirá el consentimiento de sus padres o tutores.

Considerando la implicación de las nuevas tecnologías en la vida de los menores de edad, ya sea por ser propietarios de dispositivos o por compartirlos con sus padres o tutores legales, si la app se destina a ellos y el consentimiento puede darlo el mismo menor, el responsable del tratamiento debe prestar atención a las limitaciones de comprensión a la hora de informarles sobre el tratamiento, es decir, presentarles la información de manera sencilla y con un lenguaje propio de la edad en cuestión y, en especial, deben tener en cuenta rigurosamente el principio de limitación de la finalidad y de minimización de datos. Por ello, no deben procesar sus datos con finalidad publicitaria

comportamental[4], ni directa ni indirectamente, por quedar fuera del ámbito de comprensión del niño y, por tanto, exceder de los límites de tratamiento lícito.

4. *Privacy by Design* (PbD) y seguridad

4.1. Concepto y principios fundamentales

Privacy by Design (PbD), "la privacidad desde el diseño", es un elemento primordial a tener en cuenta en la creación de las apps. La idea fundamental de este concepto es que todos los intervinientes en el desarrollo, la distribución y la explotación de las aplicaciones respeten, desde el momento de su proyección, es decir, desde la fase de diseño, la privacidad de los usuarios.

Los fabricantes de sistemas operativos y de dispositivos, junto con todos los actores que mencionamos anteriormente, esto es, las tiendas de aplicaciones, los desarrolladores de aplicaciones e incluso las terceras partes, tienen la responsabilidad de ofrecer salvaguardas para la protección de los datos personales y la intimidad de los usuarios de las apps. La aplicación del concepto PbD tiene como finalidad última poner a disposición del usuario final mecanismos apropiados a través de los cuales sea informado adecuadamente de las funciones que realizan las apps y a qué datos tienen acceso, así como ofrecer la posibilidad de que los parámetros del tratamiento sean modificados en cualquier momento.

El concepto *Privacy by Design* fue acuñado y desarrollado en los años 90 por la Doctora Ann Cavoukian, Comisionada de Información y Privacidad en Ontario (Canadá), quien establece siete principios básicos que deben orientar el diseño y el desarrollo de sistemas y tecnologías que traten datos de carácter personal. Estos principios se detallan a continuación:

1. Proactividad y Prevención: se caracteriza por basarse en medidas proactivas que anticipan y previenen eventos de invasión de privacidad antes de que estos ocurran. *Privacy by Design* llega antes del suceso, no después.

2. Privacidad como la Configuración Predeterminada: PbD en este punto absorbe el concepto *Privacy by Default* o "privacidad por defecto" para establecer que la privacidad debe venir protegida desde la configuración de las apps. Se busca que los datos personales estén protegidos automáticamente sin necesidad de que el usuario tenga que tomar acción alguna, es decir, que la configuración por defecto proteja la privacidad del usuario final.

3. Privacidad Incrustada: la arquitectura de la propia app debe llevar aparejada el respeto a la privacidad, de forma que ésta constituya un componente esencial de la funcionalidad central de la app, sin disminuir su funcionalidad.

4. Funcionalidad Total: el hecho de que la app respete la privacidad no debe mermar los intereses de ninguna de las partes intervinientes.

5. Seguridad Extremo-a-Extremo: habiendo sido incrustada la privacidad en el diseño de la app, la seguridad de los datos está garantizada durante el ciclo de vida de los mismos, de inicio a fin, siendo

[4] La publicidad comportamental se basa en la instalación de *cookies* de rastreo en los dispositivos de los usuarios, con el objeto de recabar información de su navegación durante periodos de tiempo y así segmentar el perfil de esa concreta navegación atendiendo a los gustos e intereses deducidos a partir de la navegación.

los datos retenidos con seguridad y luego también destruidos con seguridad al final del proceso, sin demoras.

6. Visibilidad y Transparencia: PbD trata de asegurar a los involucrados que la app operará de acuerdo con la declaración de principios y objetivos que se hayan informado previamente de manera visible y transparente, y que además podrá verificarse que ello sigue siendo así en todo momento.

7. Respeto por la Privacidad de los Usuarios: los arquitectos y operadores deben mantener los intereses de los usuarios por encima de los suyos propios, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada y opciones amigables para el usuario.

4.2. Directrices aplicables a los distintos actores que intervienen en el desarrollo de aplicaciones

El Dictamen también dedica ciertos puntos a esta temática. A pesar de que no se centra en PbD, que simplemente lo menciona, debemos entender que cuando habla de medidas técnicas y organizativas necesarias para garantizar la protección de los datos personales, hace alusión precisamente a tal concepto. En este sentido, establece las medidas de seguridad que deben adoptar los distintos intervinientes en la creación de las apps, teniendo en cuenta las responsabilidades que ostentan en cada caso:

- **Desarrolladores de aplicaciones:** como encargados de crear las aplicaciones y ponerlas a disposición de los usuarios finales, son los responsables de decidir a qué datos personales accederá la app y qué datos procesará, así como de determinar los fines y los medios del tratamiento de datos personales en los dispositivos inteligentes, lo que los convierte en **responsables del tratamiento**, según se define en el artículo 2, letra d), de la Directiva sobre protección de datos. En consecuencia, los desarrolladores de aplicaciones deben cumplir todos los principios hasta este punto mencionados con el objetivo de que la aplicación se ajuste a lo dispuesto en la Directiva sobre protección de datos.

  Una vez concretizada la responsabilidad de los desarrolladores de aplicaciones, y teniendo en cuenta que su función principal es la de diseñar apps, una decisión importante que deben tomar antes de iniciar la fase de diseño es decidir dónde se almacenarán los datos. Estos pueden almacenarse en el dispositivo o bien se puede utilizar una arquitectura cliente-servidor. En el primer caso, los usuarios finales tienen un mayor control sobre sus datos al permitirles suprimir los datos si retiran su consentimiento al tratamiento; sin embargo, el almacenamiento de datos a distancia puede ayudar a su recuperación en caso de pérdida o robo del dispositivo.

  Por lo tanto, los desarrolladores de aplicaciones deberían establecer unas políticas claras sobre la elaboración y la distribución de sus aplicaciones, así como diseñar y aplicar un entorno favorable a la seguridad, usando herramientas que impidan la propagación de aplicaciones maliciosas[5] y permitan la instalación y desinstalación sencillas de cada aplicación.

  Si aplicamos el concepto PbD anteriormente definido, las medidas que deberían adoptar estos actores en el momento de diseñar apps se podrían resumir en las siguientes:

  a) Minimizar las líneas y la complejidad del código y aplicar controles para excluir que los datos puedan transferirse o comprometerse involuntariamente.

[5] Tipo de *software* (en este caso hablamos de una aplicación móvil) que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

b) Adecuar las estrategias de gestión de los parches de seguridad y realizar auditorías independientes de seguridad del sistema.

c) Aplicar el principio del mínimo privilegio por defecto, en virtud del cual las aplicaciones pueden acceder únicamente a los datos realmente necesarios para poner una función a disposición del usuario.

d) Tomar medidas para evitar el acceso no autorizado a datos personales, garantizando así la protección de datos tanto en tránsito como almacenados.

e) Las aplicaciones móviles deben funcionar en puntos específicos de la memoria de los dispositivos (separados por aislamiento de procesos[6]) para reducir las consecuencias de las aplicaciones maliciosas.

f) Usar mecanismos que permitan a los usuarios ver qué datos se están tratando en qué aplicaciones y permitirles activar o desactivar de manera selectiva los permisos. No usar funciones ocultas.

g) No utilizar identificadores persistentes (específicos del dispositivo), sino identificadores específicos de cada aplicación o identificadores temporales del dispositivo para evitar el seguimiento de los usuarios a lo largo del tiempo.

h) Prestar atención a la gestión de los códigos de identificación y las contraseñas de los usuarios. Estas últimas deben almacenarse cifradas y de forma segura. Poner a disposición de los usuarios un test de solidez de las contraseñas que eligen es una técnica útil para promover contraseñas más seguras.

i) Cuando se deba acceder a datos sensibles y recursos de pago, se podría contemplar la autenticación repetida o reautenticación, por medio de factores múltiples y canales diversos (p. ej., código de acceso enviado por SMS).

Una vez analizadas las medidas de seguridad desde la óptica PbD, el Dictamen propone que, durante el ciclo de vida de la app, el desarrollador tenga en cuenta los requisitos establecidos en la Directiva sobre la privacidad electrónica en cuanto a las violaciones de los datos personales y la necesidad de trabajar activamente para informar a los usuarios[7]. Esto explica la necesidad de disponer de un plan de seguridad detallado continuamente evaluado, que cubra la recogida, el almacenamiento y el tratamiento de datos personales.

Junto a lo anterior, se insta al desarrollador a elaborar soluciones o parches para las deficiencias de seguridad y los puntos vulnerables de las aplicaciones, informar a los usuarios finales por adelantado sobre el periodo en el que pueden esperar actualizaciones de seguridad y suministrar dichas actualizaciones, con o sin parches, a los usuarios finales. En consecuencia, los desarrolladores deberían fomentar, entre los usuarios finales, la descarga de las actualizaciones.

[6] Se trata de mecanismos de seguridad para separar los programas en funcionamiento.
[7] Aunque estos requisitos actualmente sólo son de obligado cumplimiento para los proveedores de servicios de comunicaciones electrónicas disponibles al público, se espera que esta obligación se extienda también a todos los responsables y encargados del tratamiento mediante el futuro Reglamento sobre protección de datos.

- **<u>Fabricantes de sistemas operativos y de dispositivos</u>:** también deben considerarse **responsables del tratamiento** respecto a los datos personales procesados para fines como el buen funcionamiento del dispositivo inteligente o la seguridad. Esto incluye los datos generados por el usuario, los datos generados automáticamente por el dispositivo o los datos derivados de la instalación o el uso de las apps.

  Esta responsabilidad también encuentra su fundamento en el hecho de que los fabricantes de sistemas operativos y de dispositivos son responsables de las API que, como vimos anteriormente, permiten el tratamiento de datos personales por las aplicaciones de los dispositivos. Así pues, estos agentes también determinan los medios y el grado de acceso a los datos personales. Por ello, el Dictamen insta a los fabricantes de sistemas operativos y de dispositivos a asegurarse de que se ofrece a los desarrolladores de aplicaciones un control suficientemente diferenciado o granulado, de modo que se dé acceso sólo a los datos necesarios para el funcionamiento de la aplicación. Así mismo, deben garantizar que dicho acceso pueda revocarse de forma sencilla y eficaz.
  La aplicación de PbD por los fabricantes de sistemas operativos y dispositivos les exige adoptar las siguientes medidas:

  a) Distribuir algoritmos de cifrado fuertes y bien conocidos y soportar longitudes de clave apropiadas.

  b) Poner a disposición de los desarrolladores de aplicaciones mecanismos de autenticación robustos y seguros (p. ej. el uso de certificados firmados por autoridades de certificación para verificar la autorización de una fuente remota).

  c) Garantizar que los métodos y las funciones que permiten acceder a datos personales incluyen características destinadas a aplicar las solicitudes de consentimiento granular.

  d) Emprender acciones para excluir o limitar al acceso a datos personales utilizando funciones de bajo nivel u otros medios que pudieran eludir los controles y las salvaguardias incorporadas en las API.

  e) Desarrollar líneas de auditoría claras en los dispositivos, de modo que los usuarios puedan ver qué aplicaciones han estado accediendo a los datos de sus dispositivos.

  De igual modo que para los desarrolladores de aplicaciones, el Dictamen recomienda proporcionar a los usuarios finales información por adelantado sobre el periodo en el que pueden esperar actualizaciones de seguridad periódicas, así como cuando un aspecto de seguridad deba repararse mediante una actualización.

- **<u>Tiendas de aplicaciones</u>:** de la misma manera que los actores analizados previamente, las tiendas de aplicaciones también son **responsables del tratamiento** ya que procesan pagos por adelantado por las apps descargadas y permiten realizar compras dentro de la aplicación, por lo que requieren el registro de los usuarios con el nombre, la dirección y los datos financieros. Estos datos pueden combinarse con los datos sobre el comportamiento de compra y uso así como con datos leídos en el dispositivo o generados por el mismo.

  La función de las tiendas de aplicaciones es muy importante dado que permiten a los desarrolladores de aplicaciones entregar información adecuada sobre las apps, incluidos los tipos

de datos que la aplicación puede procesar y para qué fines. Es más, estas tiendas pueden poner a punto, en colaboración con el fabricante de sistemas operativos, un marco que permita a los desarrolladores ofrecer avisos claros y significativos con información sobre el respeto a la privacidad y presentarlos de forma destacada en el catálogo de la tienda.

Llegados a este punto, nos podríamos formular la siguiente pregunta, ¿las tiendas de aplicaciones podrían considerarse un agente que quede incluido en el concepto de PbD? A priori podríamos entender que como su intervención es post-diseño no estaríamos hablando de PbD propiamente, pero si tenemos en cuenta los siete principios anteriormente detallados, consideramos que estos agentes sí quedan incluidos en dicho concepto en la medida en que se extiende a sistemas de tecnologías de la información, prácticas de negocios responsables y diseño físico e infraestructura de red. En este caso, las tiendas de aplicaciones son un actor cuya labor es garantizar que la app cumpla, antes de su salida al mercado, los siete principios de PbD. Se trata, según nuestro entender, de una práctica de negocio responsable.

De acuerdo con lo que se acaba de exponer, el Dictamen recomienda a las tiendas de apps adoptar las siguientes medidas:

a) Establecer controles sólidos y eficaces de las apps antes de admitirlas en el mercado con el objetivo de reducir la aparición de funciones maliciosas.

b) Someter las apps a un mecanismo de evaluación pública mediante el cual los usuarios puedan calificar las apps en un sentido completo, centrándose especialmente en los mecanismos de protección de la intimidad y la seguridad y evitando en todo caso las falsas calificaciones.

c) Aplicar un mecanismo de desinstalación a distancia de aplicaciones malintencionadas o no seguras respetando siempre la intimidad.

d) Proporcionar a los usuarios canales de retroalimentación para notificar problemas de seguridad relacionados con las apps y la eficacia de todo procedimiento de desinstalación remota por parte de la tienda.

Al igual que los desarrolladores de aplicaciones, las tiendas de apps deben ser conscientes de las futuras obligaciones de notificación de la violación de los datos personales y trabajar estrechamente con ellos para evitar dichas violaciones.

- **Terceras partes:** al margen de los agentes ya estudiados, existen numerosos tipos de terceras partes que intervienen en el tratamiento de los datos mediante el uso de las apps. Así, encontramos redes publicitarias, proveedores de análisis y prestadores de servicios de comunicaciones.

  La publicidad, fuente de financiación para muchas aplicaciones gratuitas, puede ser facilitada a través de un sistema de seguimiento como *cookies* u otros identificadores del dispositivo y puede ser presentada en un *banner* dentro de la app o en anuncios fuera de la misma. Dicha publicidad suele ser suministrada por redes publicitarias y acostumbra a implicar el tratamiento de datos personales.

  Otros ejemplos serían los proveedores de análisis, que permiten a los desarrolladores comprender el uso, la popularidad y la facilidad de uso de sus aplicaciones, y los prestadores de servicios de

comunicaciones, que determinan los parámetros por defecto y las actualizaciones de seguridad de muchos dispositivos y pueden tratar datos sobre el uso de las aplicaciones.

En relación con los desarrolladores de aplicaciones, las terceras partes pueden desempeñar dos tipos de funciones distintas:

a) La primera consiste en llevar a cabo operaciones en nombre del desarrollador. En estos casos, las terceras partes no procesan datos para sus propios fines y/o los comparten con los desarrolladores. Probablemente estén actuando como **encargados del tratamiento**.

b) La segunda función consiste en recoger información de las aplicaciones para prestar servicios adicionales (p. ej. evitar la presentación del mismo anuncio a un mismo usuario). En estos supuestos, las terceras partes tratan datos personales para sus propios fines y, por lo tanto, serán **responsables del tratamiento**.

En cuanto a la seguridad, el Dictamen establece que las consideraciones y medidas comentadas anteriormente deben ser aplicadas por las terceras partes al recoger y procesar datos personales para sus propios fines, es decir, cuando actúen como responsables del tratamiento. Esencialmente, la aplicación de PbD en este caso implicaría la transmisión segura y el almacenamiento cifrado de identificadores únicos de dispositivos y aplicaciones y otros datos personales.

Para concluir este apartado dedicado a *Privacy by Design* y a la seguridad, queremos hacer mención a una nueva herramienta conocida como *Privacy Impact Analysis* (PIA) o "Evaluación de Impacto en la Privacidad o Evaluación de Impacto en la Protección de Datos Personales" (en adelante, EIPD). Se trata de un instrumento que permite identificar y eliminar o mitigar los riesgos en las primeras fases de diseño de un producto o sistema. De esta manera, se incrementa la confianza entre los usuarios y se evitan costosos re-diseños y posibles daños a la imagen y la economía de las entidades si se producen invasiones no autorizadas en la privacidad de las personas.

Este instrumento, cuyo uso está muy extendido entre los países anglosajones, no se utiliza mucho en España. Actualmente, la Agencia Española de Protección de Datos (en adelante, la AEPD) está promoviendo su implantación mediante la elaboración de una guía de la que, a día de hoy, existe un borrador, y cuya aprobación definitiva está prevista para los próximos meses[8]. La AEPD considera que el uso de esta herramienta junto con otras como la realización de auditorías periódicas, la correcta documentación de los tratamientos o el nombramiento de un delegado de protección de datos, contribuyen significativamente a la mejora proactiva de la privacidad.

5. Proyecto PATiA

El control sobre los datos que recaban las apps y el conocimiento sobre su destinación queda, en muchos casos, fuera del alcance de los usuarios. En este sentido, ha nacido un proyecto de la mano de GISSIM o Grupo de Investigación en Seguridad de Sistemas Móviles de la Universidad de León llamado PATiA o *Privacy Analysis Tool for iOS Applications,* cuyo objeto es ofrecer información, a través de una herramienta en su web[9], sobre los datos que recogen las apps gratuitas en *iOS* para que el usuario,

[8] Actualmente la aplicación de la EIPD no es obligatoria en España, pero se prevé que sí lo sea con el futuro Reglamento sobre protección de datos.
[9] https://patia.unileon.es

previamente a la instalación de las mismas, pueda saber a qué datos accederán. Según los responsables del proyecto PATiA se ha creado esta iniciativa porque, en contraste con *Android*, las apps en *iOS* no muestran dicha información antes de la instalación de la app, sino que los permisos se recaban una vez ya se ha instalado y está en funcionamiento, o ni siquiera en ese momento. Como ya estudiamos, precisamente el Dictamen lo que pretende es que ello no ocurra.

El proyecto presenta una base de datos con información sobre múltiples apps que va aumentando gracias a la colaboración de los propios usuarios que realizan peticiones de inclusión de apps que hasta el momento no se habían analizado.

La información se presenta a través de una tabla donde el usuario puede observar:

- El nombre, junto a un hipervínculo que dirige a su página en la *App Store*.
- Última versión conocida por PATiA.
- Icono de la app, con redirección también a la *App Store*.
- Diferentes celdas que, bajo *"YES"* o *"NO"*, muestran si la app accede a:
    - los contactos, (en ocasiones además también los suben a sus servidores),
    - la dirección MAC[10] del dispositivo,
    - la identidad del usuario,
    - la galería de fotos y los videos almacenados en el dispositivo,
    - geolocalización,
    - el calendario,
    - los contenidos copiados a través de la función portapapeles,
    - internet,
    - el nombre y la dirección de la red wifi a la que está conectado.
- Puntuación o *Privacy Score* que da PATiA a las diferentes apps, que además de una representación numérica sigue una escala de colores:
    - Alto acceso a datos (color rojo): a partir de 100 puntos,
    - Medio acceso a datos (color amarillo): entre 16 y 99 puntos,
    - Bajo acceso a datos (color verde): menos de 16 puntos.

Como veremos, este proyecto resulta interesante a efectos del siguiente punto donde examinaremos, a través de un pequeño muestreo, si las aplicaciones tanto en *iOS* como en *Android* cumplen con los principios del Dictamen tal y como los hemos estudiado. El proyecto PATiA actualmente se encuentra paralizado por falta de financiación pero se espera que próximamente se reactive, por ello los datos que nos ofrecen se actualizaron por última vez en marzo de 2014.

[10] La dirección MAC (siglas en inglés de *media access control*; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

6. *App Store* vs *Play Store*: auditoria de privacidad según el sistema operativo

¿Cumplen las aplicaciones, en España, con lo establecido en la legislación europea sobre protección de datos y, en concreto, con el Dictamen? En este apartado vamos a analizar varias aplicaciones de las dos principales tiendas de apps, éstas son la *App Store* de *iOS* y la *Play Store* de *Android*, haciéndonos valer de la normativa estudiada así como, para el caso de *iOS*, del proyecto PATiA.

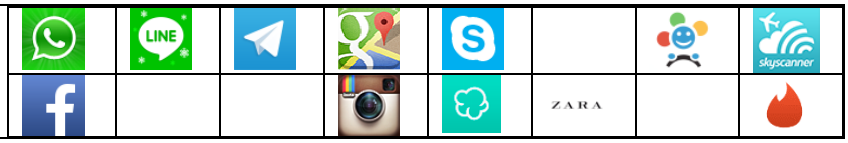
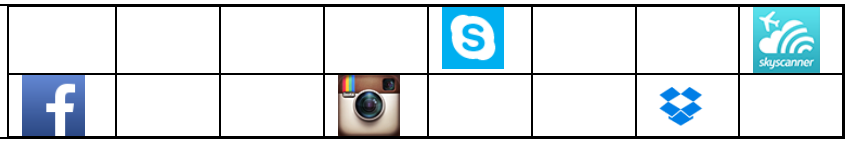
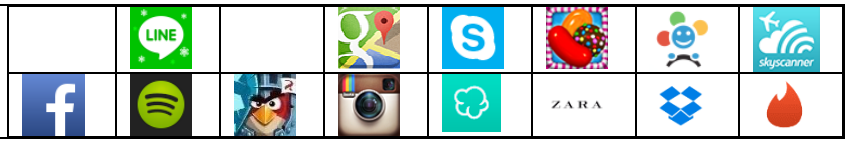
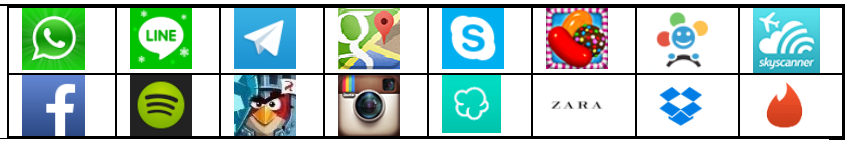
La auditoría versará sobre las siguientes aplicaciones:

iOS	Whatsapp	Line	Telegram	Google Maps	Skype	Candy Crush	BlaBlaCar	Skyscanner
Android	Facebook	Spotify	Angry Birds Epic	Instagram	Wallapop	Zara	Dropbox	Tinder

A partir de dichas apps, la auditoría se va a desarrollar a través de un *checklist* en el cual el lector identificará, en un primer estadio, a qué datos tiene acceso cada aplicación y, en un segundo estadio, qué premisas de las que se establecen en el Dictamen cumplen las distintas aplicaciones.

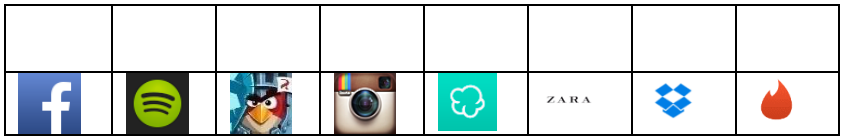
1. Datos a los que tienen acceso:

Contactos	✓	✓	✓		✓			
	✓			✓			✓	
Nombre y dirección de la red wifi a la que está conectado		✓			✓			
	✓	✓	✓		✓	✓	✓	✓
Dirección MAC del dispositivo	✓	✓	✓	✓	✓	✓	✓	✓
	✓	✓	✓		✓	✓		✓
Fotos y videos del dispositivo	✓	✓	✓	✓	✓			
	✓	✓	✓	✓	✓	✓	✓	✓

Geolocalización	
Calendario	
Identidad del usuario	
Internet	

2. Cumplimiento de las especificaciones del Dictamen:

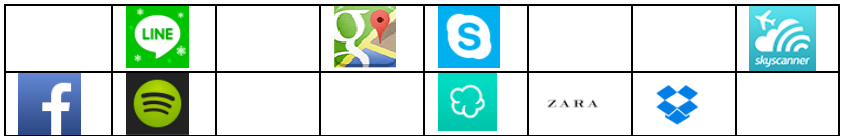
✓ Solicitar el consentimiento antes de que la app comience a recoger información del dispositivo o se instale en el mismo:



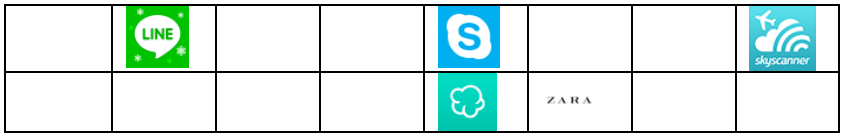
✓ Solicitar el consentimiento diferenciado o "granular" para los distintos tipos de datos a los que accederá la app:

✓ Informar sobre los fines del tratamiento de datos, de forma bien definida y comprensible, antes de instalar la app, incluyendo los fines relacionados con terceras partes (como publicidad o análisis):

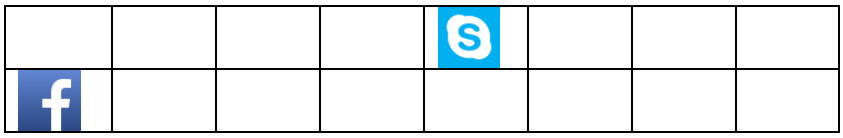
- ✓ Proporcionar una política de privacidad legible, comprensible y fácilmente accesible:



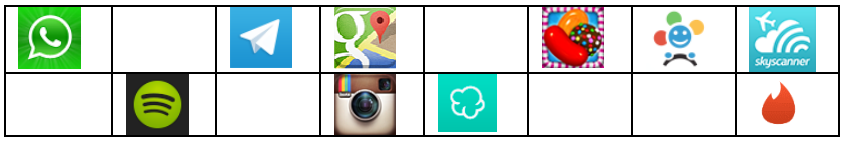
- ✓ Permitir a los usuarios ejercer los derechos ARCO e informarles de la existencia de dichos mecanismos:



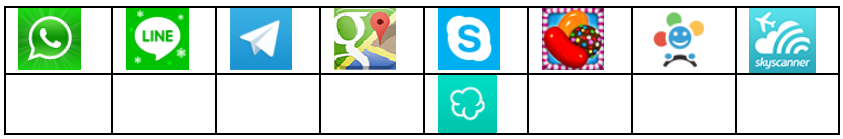
- ✓ Definir un periodo razonable de conservación de los datos recabados y fijar un periodo de inactividad tras el que la cuenta se considerará expirada:



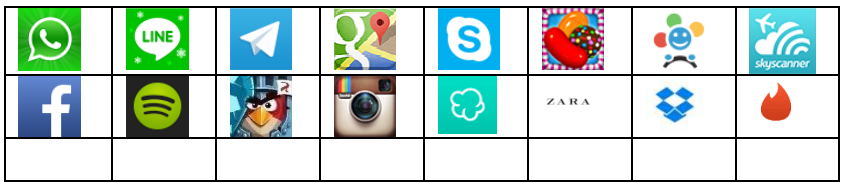
- ✓ Respetar el principio de minimización de datos y recoger sólo los datos estrictamente necesarios para realizar la función deseada:



- ✓ Permitir a los usuarios revocar la autorización:



- ✓ Permitir desinstalar la aplicación y, en su caso, suprimir los datos,
- ✓ Ofrecer un punto de contacto a los usuarios de la app,
- ✓ Facilitar mecanismos de evaluación pública,
- ✓ Proporcionar sistemáticamente actualizaciones periódicas de seguridad,
- ✓ Prestar atención al límite de edad que define a los niños o menores de edad:



Una vez representada gráficamente la auditoría de privacidad, podemos observar dos grandes diferencias entre los dos sistemas operativos: a diferencia de *iOS*, *Android* sí solicita el consentimiento antes de que la app comience a recoger información del dispositivo o se instale en él; ahora bien, *iOS* sí solicita el consentimiento diferenciado o "granular" para los distintos tipos de datos a los que accederá la app, aspecto que *Android* no contempla.

En relación con el deber de información sobre los fines del tratamiento de datos, de forma bien definida y comprensible, antes de instalar la app, se observa un elevado incumplimiento por la mayoría de las apps auditadas en ambos sistemas operativos. Para discernir las apps que cumplían con este deber de las que no, hemos seguido dos criterios no acumulativos:

1. Que desde la tienda de apps se ofreciera un enlace fácilmente accesible de manera que no fuera necesaria una navegación excesiva por la web del desarrollador de la app, o

2. Que dicha información estuviera en un lenguaje legible y comprensible, es decir, en este caso en español.

Así, de un total de 16 aplicaciones, sólo respetan esta premisa 5, de las cuales 3 en *iOS* (Google Maps, Skype, Skyscanner) y 2 en *Android* (Facebook y Dropbox).

Sin embargo, es curioso el hecho de que cuando hemos analizado la especificación relativa a la política de privacidad legible, comprensible y fácilmente accesible, la lista anterior aumenta, de manera que de 5 aplicaciones que informan previamente, ahora son 9 las que ponen a disposición del usuario dicha política. En consecuencia, se unen a la lista Line, en *iOS*, y Spotify, Wallapop y Zara en *Android*.

Cabe añadir que, las apps que hemos considerado que no ofrecen una política de privacidad, en la mayoría de casos es porque no cumplen los requisitos de "legible" y "comprensible", ya que presentaban su política en inglés u otro idioma diferente al español, como ocurre con Whatsapp o Candy Crush en *iOS* y con Angry Birds Epic, Tinder e Instagram en *Android.* Queremos hacer especial mención a la app BlaBlaCar en *iOS* ya que, a pesar de presentar su política en español, el acceso a la misma no es directo, pues requiere navegar por la pestaña de "Preguntas frecuentes" hasta localizar la política de privacidad en un apartado diferenciado.

A pesar de los datos que se acaban de exponer, no todas las políticas de privacidad cumplen con la especificación de permitir a los usuarios ejercer los derechos ARCO e informarles de su existencia. Únicamente cumplen con ello Line, Skype, Skyscanner, Wallapop y Zara, es decir, 5 apps del total que proporcionaban la política de privacidad. Y esta tendencia se agrava cuando hablamos de definir un periodo razonable de conservación de los datos recabados y fijar un periodo de inactividad tras el cual la cuenta se considerará expirada, ya que sólo Skype y Facebook lo prevén.

Skype, en su política de privacidad establece que conservará la información el tiempo necesario para cumplir con su función o con la legislación vigente, exigencias normativas y órdenes de tribunales

competentes. A pesar de no fijar un periodo de inactividad para considerar expirada la cuenta, sí que define un periodo de conservación de los datos referentes a los mensajes, comprendido entre 30 y 90 días, a menos que la ley permita o exija otra cosa. Por otro lado, Facebook distingue entre "desactivar" y "eliminar" la cuenta. En el primer caso no se suprime la información del usuario, sin embargo, la eliminación de la cuenta sí comporta el borrado permanente de la información, lo cual suele tardar aproximadamente un mes desde el momento de la solicitud, pero puede quedar información en las copias de seguridad y los registros durante un máximo de 90 días. En resumen, ninguna de estas dos apps cumplen en su totalidad con la especificación del Dictamen, pero teniendo en cuenta el incumplimiento generalizado de este requisito, hemos dado por válidas estas menciones a los periodos de conservación en el momento de realizar esta auditoría.

Otra premisa a destacar es el respeto al principio de minimización de los datos y recogida sólo de aquéllos estrictamente necesarios para realizar la función deseada por la app. Nos ha sorprendido positivamente que apps como Whatsapp, Telegram, Google Maps, Candy Crush, BlaBlaCar y Skyscanner en *iOS,* y Spotify, Instagram, Wallapop y Tinder en *Android* respeten, según la información que proporcionan, dicho principio. No obstante, Angry Birds Epic y Zara en *Android* se exceden en la recogida de datos personales. Estas apps no sólo recaban los datos necesarios para dar cumplimiento a su finalidad, sino que, además, Angry Birds Epic, que es un juego multimedia, recaba datos relativos a la identidad del usuario e información sobre la conexión wifi, y accede a las fotografías y archivos del dispositivo, mientras que Zara, que es una tienda online de moda, también accede a la ubicación, al número de teléfono, a las fotografías y archivos del dispositivo, a la cámara, al micrófono y a la información sobre la conexión wifi.

En cuanto a la posibilidad de revocar la autorización, ambos sistemas operativos difieren en el sentido de que *iOS* facilita desde el menú de ajustes la revocación "granular", mientras que *Android* sólo lo permite en uno de los casos analizados, Wallapop, a través de una dirección de correo electrónico al desarrollador de la app.

Por último, observamos que todas las aplicaciones auditadas cumplen con:

- ✓ Permitir desinstalar la aplicación y, en su caso, suprimir los datos,
- ✓ Ofrecer un punto de contacto a los usuarios de la app,
- ✓ Facilitar mecanismos de evaluación pública,
- ✓ Proporcionar sistemáticamente actualizaciones periódicas de seguridad,
- ✓ Prestar atención al límite de edad que define a los niños o menores de edad.

Por lo que respecta a los menores de edad, todas las apps analizadas en *iOS* hacen mención a la edad mínima recomendada para el uso de las mismas. En este sentido, hemos observado que la *App Store* diferencia dos grupos de edades mínimas: "superior a 4 años" y "superior a 17". Por la naturaleza de las apps auditadas en *iOS,* todas ellas están dentro del grupo "superior a 4 años", y ante esta evidencia hemos decidido indagar si era una clasificación meramente formalista o si realmente se tenía en cuenta el contenido de la app respecto a los menores. Así, cuando hemos comprobado apps como Tinder, Meetic o eDarling en *iOS,* su clasificación se encontraba dentro del grupo "superior a 17 años", por lo que hemos llegado a la conclusión de que el criterio que sigue *iOS* para clasificar las apps en uno u otro grupo de edades mínimas es el hecho de que la app pueda contener elementos con connotaciones eróticas o sexuales.

Android emplea otro sistema para establecer los límites de edad. En la *Play Store* aparece un apartado con el título "Clasificación del contenido" utilizando cuatro niveles: "para todos", "nivel de madurez

bajo", "nivel de madurez medio" y "nivel de madurez alto". Esta tienda de aplicaciones, para clasificarlas según su nivel de madurez, usa los siguientes criterios: alcohol, tabaco y drogas, juegos de apuestas, contenido incendiario o promoción del odio, ubicación, blasfemias y humor grosero, contenido sexual y provocativo, contenido generado por el usuario y comunicación entre usuarios y violencia.

Ahora bien, las distintas maneras de gestionar la limitación de edad por parte de *App Store* y *Play Store* no serían totalmente adecuadas. Cuando el menor es propietario del dispositivo, si tenemos en cuenta que para acceder a las tiendas de aplicaciones se le solicitan distintos datos personales, entre los que se incluyen la fecha de nacimiento, en nuestra opinión, la plataforma correspondiente debería impedirle la descarga de la app cuando su edad no fuera la mínima recomendada, o bien limitarle el acceso una vez ya instalada la aplicación.

Sin embargo, cuando el menor comparte el dispositivo con sus padres o tutores legales, estos tienen la opción de utilizar métodos de control parental. *iOS* cuenta con una herramienta integrada en el sistema operativo para activar una función mediante la cual los padres/tutores, bajo contraseña, puedan limitar el acceso a sitios web, descarga de apps, compras *online*…. Mientras que en *Android* se ha optado por ofrecer un mecanismo dentro de la *Play Store* a través del cual se limite, también bajo contraseña, la búsqueda de aplicaciones según el nivel de madurez.

7. Conclusiones

Las Autoridades destacan los distintos riesgos que para la protección de los datos personales supone el elevado número de actores que intervienen en el ecosistema de aplicaciones móviles. Existen riesgos de diversa índole, desde la falta de transparencia y de sensibilización de los usuarios de aplicaciones hasta el desconocimiento de la normativa aplicable, escasas medidas de seguridad, mecanismos de consentimiento inválidos, una tendencia a recabar más datos de los necesarios y la desproporcionalidad de los fines del tratamiento.

Con el objetivo de reducir o mitigar estos riesgos, las diferentes partes que participan en el desarrollo, la distribución y la capacidad técnica de las aplicaciones, como responsables del tratamiento deben adoptar una serie de medidas de seguridad que garanticen la protección de la intimidad de los usuarios de las aplicaciones. Mediante esta tesina ha quedado acreditado que la aplicación del concepto *Privacy by Design* debe convertirse en la herramienta principal de los distintos agentes para dar cumplimiento a la Directiva sobre protección de datos y la LOPD.

La aplicación de *Privacy by Design* facilita la tarea de adecuar las aplicaciones a la normativa sobre protección de datos ya que, desde la fase de diseño, los diferentes agentes pueden controlar que se cumplen los requisitos de: consentimiento previo a la instalación, limitación de la finalidad y minimización de datos, informar correctamente a los usuarios finales, ofrecer la posibilidad de ejercer los derechos ARCO, establecer periodos de conservación de los datos y tratar lealmente los datos recopilados a partir de los niños o sobre ellos.

Mediante la auditoría de privacidad realizada en esta tesina hemos constatado que muchos de los requisitos mencionados no se cumplen o lo hacen parcialmente. Esta realidad evidencia que la puesta en práctica del concepto *Privacy by Design* no ha llegado aún a su punto álgido de implantación entre los agentes intervinientes. En este sentido, algunos de los incumplimientos detectados en la auditoría son: proporcionar políticas de privacidad en inglés cuando el destinatario final radica en España, hipervínculos inactivos o mal catalogados, solicitudes de consentimiento incompletas y/o

extemporáneas, ausencia de información sobre la posibilidad de ejercer los derechos ARCO así como de los periodos de conservación de los datos, recogida de datos innecesarios para la funcionalidad de la aplicación e imposibilidad o dificultad de revocar la autorización de acceso a datos.

A nivel nacional debe destacarse el proyecto PATiA, impulsado por la Universidad de León, que a través de un análisis sobre los datos que recaban las apps gratuitas en *iOS* se pone de manifiesto, en algunos casos, el incumplimiento sistemático del principio de minimización de datos por parte de los responsables del tratamiento.

Junto a lo anterior, cabe hacer mención a una iniciativa que se está gestando entre la firma jurídica Global Legaldata, dedicada a los servicios de consultoría en Derecho de las tecnologías de la información y la comunicación (en adelante, TIC), y el patronato Barcelona Digital Centre Tecnològic (BDigital), centro tecnológico avanzado especializado en la aplicación de las TIC en los ámbitos de salud, seguridad, movilidad, energía, alimentación y medio ambiente. Ambas entidades se han asociado para impulsar la creación de un "certificado de privacidad" de las aplicaciones móviles, cuya expedición certifique que una app concreta cumple con la normativa en materia de protección de datos, lo que constituye una garantía adicional de respeto a la privacidad. Actualmente, este certificado no se encuentra aún en el mercado, pero está previsto que salga próximamente.

Llegados a este punto, la reflexión que cabe hacerse es si será posible establecer ciertas restricciones al desarrollo tecnológico. Hasta la fecha, la tecnología avanza sin parar, sin límites, sin reglas, tratando de producir mejoras en el día a día aunque éstas, a menudo, responden a ciertos intereses. *Privacy by Design* tratará de poner fin al "todo vale" siendo necesario, antes de la construcción de un nuevo equipo o dispositivo, pensar en qué impacto potencial puede tener para la privacidad. Esto es lo que hemos citado anteriormente como *Privacy Impact Analysis.*

Obviamente, estas herramientas no van a ser del agrado de muchas organizaciones que, probablemente, van a presionar para evitar o minimizar su plena aplicación. No podemos olvidar que nos encontramos en una sociedad occidental basada en la explotación voraz de información en beneficio de las grandes empresas cuyo principal y único objetivo es aumentar sus beneficios. En consecuencia, la voluntad de implantar una filosofía que gire en torno al interés del afectado y al control de su privacidad generará con total seguridad tensiones que podrán condicionar los desarrollos reglamentarios de los marcos de protección de datos.

8. Bibliografía

Legislación:

Directiva 95/4/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos, de 24 de octubre. Parlamento Europeo y el Consejo.

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

Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, Working Paper 202, de 27 de febrero.
Grupo de Trabajo del Artículo 29.

Dictamen 5/2009 sobre las redes sociales en línea, Working Paper 163, de 12 de junio.
Grupo de Trabajo del Artículo 29.

Ley Orgánica 15/1999 de protección de datos de carácter personal, de 13 de diciembre. Cortes Generales.

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

Real Decreto Legislativo 1/1996 por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes en la materia, de 12 de abril.
Gobierno de España.

Artículo:

Cavoukian, Ann. *Privacy by Design, Los 7 Principios Fundamentales*. Canadá: Febrero de 2011. Traducción de: Esprit International Communications Ltd. Disponible en: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf

Sitios web:

Las Autoridades Europeas de protección de datos aprueban el primer dictamen conjunto sobre aplicaciones móviles, Nota Informativa. Agencia Española de Protección de Datos, 2013. Disponible en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/marzo/130314_NP_Dictamen_aplicaciones.pdf

Proyecto PATiA. Grupo de Investigación en Seguridad de Sistemas Móviles (GISSiM) Universidad de León. 2014. Disponible en: https://patia.unileon.es/

J., Alberto. *PATiA, el proyecto español que analiza la privacidad de las apps en iOS,* 11 de febrero de 2014.

Disponible en: http://appleweblog.com/2014/02/patia-privacidad-ios

Developer Economics Q1 2014 The State of the Developer Nation, Developer Economics, febrero de 2014.
Disponible en: http://www.developereconomics.com/reports/q1-2014/

Cómo clasificar el contenido de tu aplicación para Google Play, Google. Disponible en: https://support.google.com/googleplay/android-developer/answer/188189?hl=es

9. Anexo

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

Artículo 4. Calidad de los datos

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho a información en la recogida de datos

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable de fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 9. Seguridad de los datos

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 15. Derecho de acceso

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD

Artículo 13. Consentimiento para el tratamiento de datos de menores de edad

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.