GRUPO DE TRABAJO «ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS»

00461/13/ES
WP 202

Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes

Adoptado el 27 de febrero de 2013

Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo europeo independiente en materia de protección de datos y privacidad. Su cometido se describe en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

Las labores de secretaría las realiza la Dirección C (Derechos Fundamentales y Ciudadanía de la Unión) de la Comisión Europea, Dirección General de Justicia, B-1049 Bruselas, Bélgica, Despacho nº MO-59 02/013.

Página web: http://ec.europa.eu/justice/data-protection/index_es.htm

Resumen

Existen cientos de miles de aplicaciones disponibles en toda una serie de tiendas de aplicaciones para cada tipo de dispositivo inteligente de cierta popularidad. Según los datos disponibles, estas tiendas reciben cada día 1 600 nuevas aplicaciones y el usuario medio de teléfono inteligente se descarga 37 aplicaciones. Estas pueden ofrecerse por un coste bajo o sin coste alguno para el usuario final y pueden contar con una base de usuarios de unos cuantas personas o muchos millones de ellas.

Las aplicaciones pueden recoger grandes cantidades de datos a partir de los dispositivos (por ejemplo, datos almacenados por el usuario en su dispositivo o datos de distintos sensores como la ubicación) y procesarlos para proporcionar servicios nuevos e innovadores al usuario final. Sin embargo, esas mismas fuentes de datos pueden ser objeto de un tratamiento adicional, normalmente para generar ingresos, de forma desconocida o no deseada por el usuario final.

Los desarrolladores de aplicaciones que desconozcan las normas de protección de datos pueden crear riesgos significativos para la vida privada y la reputación de los usuarios de dispositivos inteligentes. Los principales riesgos para la protección de datos de los usuarios finales son la falta de transparencia y conocimiento de los tipos de tratamiento que las aplicaciones pueden realizar, combinada con la falta de consentimiento significativo del usuario final antes de que se produzca el tratamiento de datos. Las insuficientes medidas de seguridad, la clara tendencia hacia la maximización de los datos y la elasticidad de los fines para los que se recogen datos personales también contribuyen a los riesgos relacionados con la protección de datos que se dan en el actual entorno de las aplicaciones.

Asimismo, el grado de fragmentación de los numerosos actores que intervienen en el desarrollo de aplicaciones también supone un riesgo grave para la protección de datos. Entre ellos, se incluyen: desarrolladores de aplicaciones, propietarios de aplicaciones, tiendas de aplicaciones, fabricantes de sistemas operativos y de dispositivos, y otras terceras partes que pueden intervenir en la recogida y el tratamiento de datos personales a partir de dispositivos inteligentes, como proveedores de análisis y publicitarios. La mayoría de las conclusiones y recomendaciones del presente dictamen van dirigidas a los desarrolladores de aplicaciones (son ellos quienes tienen mayor control sobre la forma en que se realiza el tratamiento o se presenta la información dentro de la aplicación), pero a menudo, para alcanzar el máximo nivel de privacidad y protección de datos, deben colaborar con otras partes del ecosistema de las aplicaciones. Esto es especialmente importante por lo que se refiere a la seguridad, donde la cadena de múltiples actores solo puede ser tan fuerte como su eslabón más débil.

Gran parte de los tipos de datos disponibles en un dispositivo móvil inteligente son de carácter personal. El marco jurídico aplicable es la Directiva sobre protección de datos, en combinación con la protección de los dispositivos móviles como parte de la esfera privada de los usuarios, incluida en la Directiva sobre la privacidad electrónica electrónica y las comunicaciones electrónicas. Estas normas cubren las aplicaciones destinadas a usuarios de la UE, independientemente del lugar de radicación de los desarrolladores o las tiendas de aplicaciones.

En el presente dictamen, el grupo de trabajo clarifica el marco jurídico aplicable al tratamiento de los datos personales en el desarrollo, la distribución y el uso de aplicaciones en

dispositivos inteligentes, centrándose en el requisito del consentimiento, los principios de limitación de la finalidad y de minimización de los datos, la necesidad de adoptar medidas de seguridad adecuadas, la obligación de informar correctamente a los usuarios finales y respetar sus derechos, los periodos de conservación razonables y, especialmente, el tratamiento leal de los datos recopilados a partir de niños o sobre ellos.

Índice

1. Introducción

Las aplicaciones son programas informáticos generalmente concebidos para un cometido concreto y dirigidos a un determinado conjunto de dispositivos inteligentes como teléfonos inteligentes, tabletas o televisores conectados a internet. 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.

Existen cientos de miles de aplicaciones que están disponibles en toda una serie de tiendas de aplicaciones para cada tipo de dispositivo inteligente de cierta popularidad. Las aplicaciones sirven para una amplia gama de fines como son la navegación en internet, las comunicaciones (correo electrónico, telefonía y mensajería de internet), el entretenimiento (juegos, películas o vídeo, y música), las redes sociales, la banca y los servicios basados en la localización. Según datos disponibles, las tiendas de aplicaciones reciben cada día 1 600 nuevas aplicaciones[1]. El usuario medio de teléfono inteligente se descarga 37 aplicaciones[2]. Estas pueden ofrecerse por un coste bajo o si coste alguno para el usuario final y pueden contar con una base de usuarios de unos cuantas personas o muchos millones de ellas.

El sistema operativo subyacente incluirá también *software* o estructuras de datos que resultan importantes para servicios básicos de los dispositivos como, por ejemplo, el directorio de los teléfonos inteligentes. El sistema operativo se diseña para que esos componentes estén abiertos a aplicaciones mediante interfaces de programación de aplicaciones (API por sus siglas inglesas). Las API dan acceso a la multitud de sensores que pueden contener los dispositivos inteligentes como son: giroscopios, brújulas y acelerómetros digitales para proporcionar datos de velocidad y dirección del movimiento; cámaras delanteras y traseras para tomar imágenes de vídeo y fotografías, y micrófonos para grabar sonido. Los dispositivos inteligentes también pueden contar con sensores de proximidad[3] y conectarse mediante múltiples interfaces de red Wi-Fi, Bluetooth, NFC o Ethernet. Por último, los servicios de geolocalización pueden proporcionar una localización exacta (según se describe en el dictamen 13/2011 del WP29 relativo a los servicios de geolocalización de los dispositivos móviles inteligentes[4]). El tipo, la exactitud y la frecuencia de estos datos de sensores varían en función del dispositivo y el sistema operativo.

---

1 Artículo publicado en ConceivablyTech el 19 de agosto de 2012, disponible en www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of . Citado por Kamala D. Harris, Fiscal General de California, Departamento de Justicia, Privacidad en movimiento, recomendaciones para el ecosistema móvil, enero de 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf .

2 Se trata de una estimación mundial para 2012 de ABI Research (http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o).

3 Sensores que permiten detectar la presencia de un objeto físico sin necesidad de contacto físico. Véase: http://www.w3.org/TR/2012/WD-proximity-20121206/

4 Véase el dictamen 13/2011 del WP29 relativo a los servicios de geolocalización de los dispositivos móviles inteligentes (mayo de 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf (en inglés).

Gracias a las API, los desarrolladores de aplicaciones pueden recoger esos datos de forma continua, acceder a los datos de contacto y registrarlos, enviar mensajes electrónicos, SMS o de redes sociales, leer, modificar o borrar el contenido de las tarjetas SD, grabar sonido, utilizar las cámaras y acceder a imágenes almacenadas, leer el estado y la identidad del teléfono, modificar los parámetros del sistema global y evitar que el teléfono entre en reposo. Las API también pueden proporcionar información sobre el propio dispositivo mediante uno o varios identificadores únicos e información sobre otras aplicaciones instaladas. Estas fuentes de datos pueden ser objeto de un tratamiento adicional, normalmente para generar ingresos, de manera desconocida o no deseada por el usuario final.

El objetivo del presente dictamen es aclarar el marco jurídico aplicable al tratamiento de los datos personales en la distribución y el uso de aplicaciones en dispositivos inteligentes y tomar en consideración los tratamientos posteriores que puedan producirse al margen de la aplicación, como utilizar los datos recogidos para crear perfiles y listas de usuarios objetivo. El dictamen analiza los principales riesgos para la protección de los datos, ofrece una descripción de las distintas partes que intervienen y pone de relieve las diversas responsabilidades jurídicas. Dichas partes incluyen: desarrolladores de aplicaciones, propietarios de aplicaciones y tiendas de aplicaciones; fabricantes de sistemas operativos y de dispositivos, y otras terceras partes que pueden participar en la recogida y el tratamiento de datos personales a partir de dispositivos inteligentes, como los proveedores de análisis y de publicidad.

El dictamen se centra en el requisito del consentimiento, los principios de limitación de la finalidad y de minimización de los datos, la necesidad de adoptar medidas de seguridad adecuadas, la obligación de informar correctamente a los usuarios finales y respetar sus derechos, los periodos de conservación razonables y, especialmente, el tratamiento leal de los datos recopilados a partir de niños o sobre ellos.

El ámbito de aplicación es aplicable a diversos tipos de dispositivos inteligentes pero se centra especialmente en las aplicaciones disponibles para dispositivos móviles inteligentes.

2. Riesgos para la protección de datos

La estrecha interacción con el sistema operativo permite a las aplicaciones acceder a un número de datos significativamente superior a aquél al que tiene acceso un navegador de internet tradicional[5]. Las aplicaciones pueden recoger gran cantidad de datos a partir del dispositivo (datos de ubicación, datos almacenados por el usuario en el dispositivo o datos de los distintos sensores) y procesarlos para proporcionar servicios nuevos e innovadores al usuario final.

Por otro lado, la fragmentación de los numerosos actores que intervienen en el desarrollo de aplicaciones también supone un riesgo grave para la protección de datos. Un determinado dato puede ser transmitido, en tiempo real, desde el dispositivo para ser procesado en cualquier parte del planeta o ser copiado entre cadenas de terceras partes. Algunas de las

[5] No obstante, los navegadores de los ordenadores de sobremesa van incrementando su acceso a los datos sensoriales de los dispositivos de los usuarios finales, impulsados por los desarrolladores de juegos en red.

aplicaciones más populares son desarrolladas por empresas tecnológicas de primer orden, pero muchas otras son diseñadas por pequeñas empresas de nueva creación. Un simple programador con una idea y poco o ningún conocimiento previo sobre programación puede llegar a una audiencia planetaria en un breve espacio de tiempo. Los desarrolladores de aplicaciones que desconozcan las normas de protección de datos pueden crear riesgos significativos para la vida privada y la reputación de los usuarios de dispositivos inteligentes. Simultáneamente, se van desarrollando rápidamente servicios a terceros como la publicidad, que, si son integrados por un desarrollador de aplicaciones sin la debida atención, puede revelar cantidades significativas de datos personales.

Los principales riesgos para la protección de los datos de los usuarios finales son la falta de transparencia y conocimiento de los tipos de tratamiento que las aplicaciones pueden realizar, combinada con la falta de consentimiento significativo por parte de los usuarios finales antes de que se produzca el tratamiento de datos. Las insuficientes medidas de seguridad, la clara tendencia hacia la maximización de los datos y la elasticidad de los fines para los que se recogen datos personales también contribuyen a los riesgos relacionados con la protección de datos que se dan en el actual entorno de las aplicaciones. Muchos de estos riesgos ya han sido examinados y tratados por otros reguladores internacionales, como la *US Federal Trade Commission* (Comisión federal de comercio de Estados Unidos), el *Canadian Office of the Privacy Commissioner* (Comisariado de protección de la vida privada de Canadá) y el Fiscal General del Departamento de Justicia de California[6].

- Un riesgo grave para la protección de datos es la falta de transparencia. Los desarrolladores de aplicaciones están condicionados por las características habilitadas por los fabricantes de sistemas operativos y las tiendas de aplicaciones para garantizar que al usuario final se le ofrece información completa a su debido tiempo. Sin embargo, no todos los desarrolladores de aplicaciones aprovechan esas características, ya que muchas aplicaciones no cuentan con política de privacidad o no informan a sus posibles usuarios, de forma clara, sobre el tipo de datos personales que la aplicación puede procesar ni sobre los fines con que lo hace. La falta de transparencia no se limita a las aplicaciones gratuitas o pertenecientes a desarrolladores sin experiencia: en un estudio reciente se indicaba que solo el 61,3 % de las 150 aplicaciones más usadas contaba con una política de privacidad[7].

---

[6] Véanse, entre otros, el informe de la FTC *Mobile Privacy Disclosures, Building Trust Through Transparency*, de febrero de 2013 (http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf), el informe de la FTC *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* de febrero de 2012 (http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf), el informe *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, de diciembre de 2012 (http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf), el informe del Comisariado de protección de la vida privada de Canadá *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*, de octubre de 2012 (http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf), y el informe de Kamala D. Harris, Fiscal General del Departamento de Justicia de California *Privacy on the go, Recommendations for the mobile ecosystem*, de enero de 2013 (http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf).

[7] Informe del Future of Privacy Forum (FPF) de junio de 2012 *Mobile Apps Study*, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf.

- La falta de transparencia está estrechamente relacionada con la falta de consentimiento libre e informado. Una vez descargada la aplicación, el consentimiento suele reducirse a marcar una casilla que indica que el usuario final acepta los términos y condiciones, sin ofrecerse siquiera una opción «No, gracias». Según un estudio de la GSMA de septiembre de 2011, el 92 % de los usuarios de aplicaciones desean tener opciones más diferenciadas o «granulares»[8].

- Unas medidas de seguridad insuficientes pueden provocar el tratamiento no autorizado de información personal (sensible), por ejemplo si un desarrollador de aplicaciones sufre una violación de datos personales o si la propia aplicación permite filtraciones de datos personales.

- Otro riesgo está relacionado con el incumplimiento (intencionado o por desconocimiento) del principio de limitación de la finalidad, que exige que los datos personales solo pueden ser recogidos y tratados para fines concretos y legítimos. Los datos personales recogidos por las aplicaciones pueden distribuirse ampliamente entre toda una serie de terceras partes con fines indeterminados o elásticos como «estudios de mercado». El mismo incumplimiento alarmante existe respecto al principio de minimización de los datos. Estudios recientes han revelado que muchas aplicaciones recopilan datos de los teléfonos inteligentes sin que exista una relación clara con la función aparente de la aplicación[9].

3 Principios de la protección de datos

3.1 Legislación aplicable

El marco jurídico aplicable en la UE es la Directiva sobre protección de datos (95/46/CE), que se aplica siempre que el uso de las aplicaciones de los dispositivos inteligentes implica el tratamiento de datos personales. Para establecer la legislación aplicable, resulta esencial definir, en primer lugar, el papel de las distintas partes interesadas: la identificación del responsable del tratamiento efectuado mediante las aplicaciones del dispositivo es fundamental en relación con la legislación aplicable. La determinación del responsable del tratamiento resulta decisiva para poner en marcha la aplicación de la normativa europea sobre protección de datos, pero no es el único criterio. De conformidad con el artículo 4, apartado 1, letra 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. De conformidad con el artículo 4, apartado 1, letra c), de la Directiva sobre protección de datos, la legislación nacional de un Estado miembro es también aplicable cuando el responsable del tratamiento *no está establecido* en el territorio de la Comunidad pero hace uso de equipos situados en el territorio de ese Estado miembro. Dado que el dispositivo resulta

---

[8] «El 89 % [de los usuarios] considera importante saber cuándo las aplicaciones transmiten datos personales suyos y poder activar y desactivar esa posibilidad.» Fuente: *User perspectives on mobile privacy*, septiembre de 2011 (http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf).

[9] Wall Street Journal, *Your Apps Are Watching You* (http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html).

fundamental para el tratamiento de los datos personales del usuario y sobre él, este criterio suele cumplirse[10]. Sin embargo, esto solo es pertinente cuando el responsable del tratamiento no está establecido en la UE.

Por tanto, siempre que una de las partes que intervienen en el desarrollo, la distribución y la explotación de aplicaciones es considerada responsable del tratamiento de datos, le corresponde, de forma única o subsidiaria, la responsabilidad de velar por el cumplimiento de todos los requisitos establecidos en la Directiva sobre protección de datos. La determinación del papel de las partes que intervienen en las aplicaciones para móviles se analiza más abajo, en la sección 3.3.

Aparte de la Directiva sobre protección de datos, la Directiva sobre la privacidad electrónica electrónica (Directiva 2002/58/CE, modificada por la Directiva 2009/136/CE) 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).

El artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica electrónica establece 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, con arreglo a lo dispuesto en la Directiva 95/46/CE». *(...)*

Si bien muchas de las disposiciones de la Directiva sobre la privacidad electrónica electrónica son aplicables únicamente a los proveedores de servicios de comunicaciones electrónicas disponibles al público y a los proveedores de redes públicas de comunicaciones de la Comunidad, el artículo 5, apartado 3, es aplicable a todas las entidades que almacenen información en los dispositivos inteligentes o accedan a la misma. Dicho apartado se aplica independientemente de la naturaleza de la entidad (es decir, sea de carácter público o privado, un programador individual o una gran corporación, un responsable del tratamiento de los datos, un encargado del tratamiento de datos o un tercero).

El requisito del consentimiento del artículo 5, apartado 3, se aplica a <u>toda la información</u>, independientemente de la naturaleza de los datos que se almacenan o a que se accede. El ámbito de aplicación no se limita a los datos personales; la información puede consistir en cualquier tipo de datos almacenados en el dispositivo.

El requisito del consentimiento del artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica electrónica se aplica a los servicios ofrecidos «en la Comunidad», es decir, a todo residente en el Espacio Económico Europeo, con independencia del lugar en que se encuentre el proveedor de servicios. Es importante que los desarrolladores de aplicaciones sepan que ambas Directivas son imperativos legales en cuanto a que los derechos de las personas son intransferibles y no están sujetos a exenciones contractuales, lo que significa que la

[10] En la medida en que la aplicación genera tráfico de datos personales con los responsables del tratamiento de datos. Este criterio podría no cumplirse si los datos solo se tratan a nivel local, en el propio dispositivo.

aplicabilidad del Derecho europeo en materia de privacidad no puede excluirse mediante una declaración unilateral o un acuerdo contractual[11].

3.2 Datos personales tratados por las aplicaciones

Muchos tipos de datos almacenados en dispositivos inteligentes o generados por los mismos son datos personales. Con arreglo al considerando 24 de la Directiva sobre la privacidad electrónica electrónica:

> «Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.».

Son datos personales cuando se refieren a una persona que es identificable directamente (p. ej., por su nombre) o indirectamente por el responsable del tratamiento o un tercero. Los datos pueden referirse al propietario del dispositivo o a cualquier otra persona como ocurre, por ejemplo, con los datos de contacto de amigos que contiene el libro de direcciones[12]. Los datos pueden recopilarse y procesarse en el dispositivo o, una vez transferidos, en otro lugar mediante infraestructuras de los desarrolladores de aplicaciones o de terceros, a través de la conexión a una API externa, en tiempo real y sin el conocimiento del usuario final.

Algunos ejemplos de esos datos personales que pueden incidir significativamente en la vida privada de los usuarios y otras personas son:

- localización
- contactos
- identificadores únicos del dispositivo y del cliente (p. ej., IIEM[13], IIAM[14], IUD[15] y número de teléfono móvil)
- identidad del interesado
- identidad del teléfono (es decir, nombre del teléfono[16])
- datos de tarjetas de crédito y relativos a pagos
- registros de llamadas, SMS y mensajería instantánea
- historial de navegación
- correo electrónico

---

[11] Por ejemplo, las declaraciones en el sentido de que solo es aplicable la ley de una jurisdicción fuera del EEE.

[12] Los datos pueden ser generados: i) automáticamente por el dispositivo a partir de características predeterminadas por el sistema operativo y/o por el fabricante del dispositivo, o por el proveedor de telefonía móvil (p. ej., datos de geolocalización, especificaciones de red o dirección IP); ii) por el usuario mediante aplicaciones (listas de contactos, notas o fotografías); iii) por las aplicaciones (p. ej., el historial de navegación).

[13] Identidad internacional del equipo móvil.

[14] Identidad internacional del abonado móvil.

[15] Identificador único del dispositivo.

[16] Los usuarios tienden a llamar a su móvil con su verdadero nombre: «iPhone de Juan López».

- credenciales de autenticación para los servicios de la sociedad de la información (en particular los servicios con características sociales)
- fotografías y vídeos
- datos biométricos (por ejemplo, modelos de reconocimiento facial y huellas dactilares).

3.3 Partes que participan en el tratamiento de los datos

En el desarrollo, la comercialización y la explotación de las aplicaciones participan muchas partes, cada una de las cuales puede tener diferentes responsabilidades en materia de protección de datos.

De ellas, cabe destacar las cuatro siguientes: i) los desarrolladores de aplicaciones (incluidos los propietarios)[17]; ii) los fabricantes de sistemas operativos y dispositivos[18]; iii) las tiendas de aplicaciones (el distribuidor de aplicaciones); y iv) otras partes implicadas en el tratamiento de datos personales. En algunos casos, las responsabilidades en materia de protección de datos están repartidas, sobre todo, cuando la misma entidad participa en diversas fases, por ejemplo cuando el fabricante de sistemas operativos también controla la tienda de aplicaciones.

También les corresponde un papel a los usuarios finales, en la medida en que crean y almacenan datos personales mediante sus dispositivos móviles. Si el tratamiento sirve para fines puramente personales o domésticos, la Directiva de protección de datos no sería aplicable (artículo 3, apartado 2) y el usuario estaría exento de las obligaciones formales en materia de protección de datos. Sin embargo, si los usuarios deciden compartir datos a través de la aplicación, por ejemplo poniendo la información a disposición de un número indeterminado de personas[19] que utilizan la aplicación de una red social, están tratando la información al margen de las condiciones de la exención doméstica[20].

3.3.1 Desarrolladores de aplicaciones

Los desarrolladores de aplicaciones crean aplicaciones y/o las ponen a disposición de los usuarios finales. Esta categoría incluye tanto a las entidades públicas y privadas que subcontratan el desarrollo de la aplicación como a las empresas y las personas que crean las aplicaciones y las distribuyen. Los desarrolladores diseñan y/o crean los programas que funcionarán en los teléfonos inteligentes y, por tanto, deciden la medida en que la aplicación accederá y procesará las distintas categorías de datos personales en el dispositivo y/o a través de recursos informáticos remotos (unidades informáticas de los desarrolladores o de terceros).
El desarrollador de aplicaciones es el responsable del tratamiento, según se define en el artículo 2, letra d), de la Directiva sobre protección de datos, en la medida en que él es quien

---

[17] El grupo de trabajo utiliza la terminología común de los desarrolladores de aplicaciones, pero subraya que el término no se limita a los programadores o los desarrolladores técnicos de aplicaciones sino que incluye a los propietarios, es decir, las empresas y organizaciones que encargan su desarrollo y fijan sus objetivos.

[18] En algunos casos, el fabricante del sistema operativo se solapa con el del propio dispositivo y en otros casos, el fabricante de dispositivos es una empresa distinta del proveedor de sistemas operativos.

[19] Véanse los asuntos del Tribunal de Justicia Europeo: C-101/01 proceso penal contra BodilLindqvist, sentencia de 6 de noviembre de 2003, y C-73/07 Tietosuojavaltuutettu contra SatakunnanMarkkinapörssiOy y SatamediaOy, sentencia de 16 de diciembre de 2008.

[20] Véase el dictamen 5/2009 de este grupo de trabajo sobre las redes sociales en línea, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf (junio de 2009).

determina los fines y los medios del tratamiento de datos personales en los dispositivos inteligentes. En tal caso, está obligado a cumplir la totalidad de las disposiciones de la Directiva sobre protección de datos, cuyas disposiciones esenciales se explican en los apartados 3.4 a 3.10 del presente dictamen.

Incluso cuando la exención de las actividades domésticas sea aplicable a un usuario, la responsabilidad seguiría correspondiendo al desarrollador de aplicaciones como responsable del tratamiento de los datos, siempre que procese los datos para sus propios fines. Así ocurre, por ejemplo, cuando, para prestar el servicio (mensajería instantánea, llamadas telefónicas, de vídeo, etc.), la aplicación exige el acceso a toda la lista de contactos.

Las responsabilidades de los desarrolladores de aplicaciones resultan muy limitadas si no se tratan datos personales o si no se distribuyen fuera del dispositivo, o si han adoptado las medidas técnicas y organizativas adecuadas para garantizar que los datos se hacen anónimos y se agregan de forma irreversible en el propio dispositivo, antes de extraerlos del mismo.

En cualquier caso, si los desarrolladores de aplicaciones acceden a información almacenada en el dispositivo, la Directiva sobre la privacidad electrónica electrónica también es aplicable, por lo que los desarrolladores deben cumplir el requisito del consentimiento establecido en el artículo 5, apartado 3, de dicha Directiva.

Los desarrolladores de aplicaciones deben cumplir todas las obligaciones relacionadas con el recurso a un encargado del tratamiento de datos en la medida en que hayan externalizado parte o la totalidad del tratamiento real de los datos a un tercero y este asuma el papel de encargado del tratamiento de datos. Esto incluiría también el recurso a un proveedor de computación en nube (p. ej., para el almacenamiento externo de datos)[21].

Los desarrolladores de aplicaciones, en la medida en que permitan el acceso de terceros a los datos del usuario (como una red publicitaria que acceda a los datos de geolocalización del dispositivo para distribuir publicidad comportamental), deben emplear mecanismos adecuados para cumplir los requisitos aplicables con arreglo al marco jurídico de la UE. Si el tercero accede a datos almacenados en el dispositivo, es aplicable la obligación de obtener el consentimiento informado fijado en el artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica electrónica. Además, si el tercero trata datos personales para sus propios fines, también puede tratarse de un responsable del tratamiento de datos en conjunción con el desarrollador de aplicaciones y debe, por tanto, garantizar el respeto del principio de limitación de la finalidad y las obligaciones en materia de seguridad[22] en relación con la parte del tratamiento para la que determina los fines y medios. Dado que entre los desarrolladores de aplicaciones y las terceras partes pueden existir diversos tipos de vínculos (tanto comerciales como técnicos), las respectivas responsabilidades de cada una de las partes

---

[21] Véase el Dictamen 05/2012 de este grupo de trabajo sobre la computación en nube, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf (julio de 2012).

[22] Véase el dictamen 2/2010 de este grupo de trabajo sobre publicidad comportamental en línea de junio de 2010 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf) y el dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» de febrero de 2010 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf).

deben establecerse caso por caso, teniendo en cuenta las circunstancias específicas del tratamiento en cuestión.

Los desarrolladores de aplicaciones pueden utilizar bibliotecas de terceros con programas que proporcionan funciones comunes, como, por ejemplo, la biblioteca de una plataforma de juegos sociales. Los desarrolladores de aplicaciones deben garantizar que los usuarios sean conscientes de toda operación de tratamiento de datos realizada por esas bibliotecas y, si ese es el caso, que ese tratamiento se ajuste al marco jurídico de la UE, incluyendo, si procede, la obtención del consentimiento del usuario. En ese sentido, los desarrolladores de aplicaciones deben evitar el uso de funciones que se ocultan al usuario.

3.3.2 Fabricantes de sistemas operativos y de dispositivos

Los fabricantes de sistemas operativos y de dispositivos también deben considerarse responsables del tratamiento de datos (y, cuando proceda, responsables conjuntos) respecto a todo dato personal procesado para fines propios como el buen funcionamiento del dispositivo, motivos de seguridad, etc. Esto incluiría los datos generados por el usuario (p. ej., los datos del usuario en la fase de registro), los datos generados automáticamente por el dispositivo (p. ej., si el dispositivo cuenta con una función de llamada a casa) o datos personales tratados por el fabricante del dispositivo o el sistema operativo derivados de la instalación o el uso de las aplicaciones. Cuando el fabricante del sistema operativo o del dispositivo proporcione funciones adicionales como copia de seguridad o localización a distancia, será también el responsable del tratamiento de los datos en cuanto a los datos personales tratados a tal efecto.

Las aplicaciones que requieren acceso a la geolocalización deben usar los servicios de localización del sistema operativo. Cuando una aplicación use la geolocalización, el sistema operativo puede recoger datos personales para transmitir datos de geolocalización a las aplicaciones y también puede considerar el uso de los datos para mejorar sus propios servicios de localización. A tal efecto, se considera que el sistema operativo es el responsable del tratamiento.

Los fabricantes de sistemas operativos y de dispositivos son también responsables de la API que permite el tratamiento de datos personales por las aplicaciones de los dispositivos inteligentes. Los desarrolladores de aplicaciones podrán acceder a estas características y funciones que los fabricantes de sistemas operativos y de dispositivos ponen a disposición a través de la API. Dado que los fabricantes de sistemas operativos y de dispositivos determinan los medios (y el grado) de acceso a los datos personales, deben asegurarse de que se ofrece a los desarrolladores de aplicaciones un control suficientemente diferenciado o «granulado», de modo que se dé acceso solo a los datos necesarios para el funcionamiento de la aplicación. Los fabricantes de sistemas operativos y de dispositivos también deben garantizar que este acceso pueda revocarse de forma sencilla y eficaz.

El concepto de «privacidad desde el diseño» es un principio importante al que ya se hace referencia indirectamente en la Directiva sobre protección de datos[23] y que, junto con el concepto de «protección de la intimidad por defecto», se desprende más claramente de la

[23] Véase el considerando 46 y el artículo 17.

Directiva sobre la privacidad electrónica electrónica[24]. Este concepto exige que los fabricantes de dispositivos o de aplicaciones incorporen la protección de datos desde el inicio de su diseño. La protección de la intimidad desde el diseño se exige explícitamente en el diseño de equipos de telecomunicaciones, con arreglo a lo dispuesto en la Directiva sobre equipos radioeléctricos y equipos terminales de telecomunicación[25]. Por tanto, los fabricantes de sistemas operativos y de dispositivos, junto con la las tiendas de aplicaciones tienen la importante responsabilidad de ofrecer salvaguardas para la protección de los datos personales y de la intimidad de los usuarios de aplicaciones. Esto incluye garantizar la disponibilidad de mecanismos apropiados para informar y educar al usuario final sobre lo que las aplicaciones pueden hacer y los datos a que pueden aaceder, así como proporcionar configuraciones adecuadas para que los usuarios de aplicaciones modifiquen los parámetros del tratamiento[26].

3.3.3 Tiendas de aplicaciones

Cada uno de los dispositivos inteligentes más utilizados tiene su propia tienda de aplicaciones y generalmente un sistema operativo determinado está profundamente integrado con una tienda de aplicaciones determinada. Las tiendas de aplicaciones suelen procesar pagos por adelantado por las aplicaciones y también 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 (directamente) identificables pueden combinarse con los datos sobre el comportamiento de compra y uso y con datos leídos en el dispositivo o generados por el mismo (p. ej., los identificadores únicos). Para el tratamiento de dichos datos personales, es probable que las tiendas de aplicaciones sean el responsable del tratamiento de los datos, en particular si facilitan esa información a los desarrolladores de aplicaciones. Cuando las tiendas de aplicaciones procesan la descarga de una aplicación por un usuario final o el historial de uso o un mecanismo similar para restablecer aplicaciones descargadas anteriormente, también serían el responsable del tratamiento de datos personales procesados a tal efecto.

Las tiendas de aplicaciones registran los datos de inicio de sesión y el historial de aplicaciones compradas previamente. También piden al usuario que facilite un número de tarjeta de crédito que se almacenará con la cuenta del usuario. La tienda de aplicaciones es el responsable del tratamiento en lo que respecta a estas operaciones.

Por el contrario, los sitios web que permiten la descarga de aplicaciones para instalarse en el dispositivo sin autenticación alguna podrían no estar procesando datos personales.

---

[24] Véase el artículo 14, apartado 3.

[25] Directiva 1999/5/CE de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad. Diario Oficial de las Comunidades Europeas L 91/10 de 7.4.1999. El artículo 3, apartado 3, letra c), establece que la Comisión puede decidir que «los aparatos incluidos en determinadas categorías de equipo se construyan de forma que contengan salvaguardias que garanticen la protección de los datos personales y de la intimidad del usuario y del abonado».

[26] El grupo de trabajo acoge con satisfacción las recomendaciones que la *Federal Trade Commission* (FTC) hace a este respecto en su informe *Mobile Privacy Disclosures*, mencionado en la nota 6; así, por ejemplo en la página 15 se señala: «(…) las plataformas están en perfecta disposición para suministrar información coherente en todas las aplicaciones y se les anima a que así lo hagan. De acuerdo con los comentarios recogidos en los seminarios, también podrían suministrar información en diversas fases (…)».

Las tiendas de aplicaciones ocupan una posición importante para permitir a los desarrolladores de aplicaciones entregar información adecuada sobre las aplicaciones, incluidos los tipos de datos que la aplicación puede procesar y para qué fines. Las tiendas de aplicaciones pueden hacer cumplir esas normas mediante su política de admisión (basándose en controles *ex ante* o *ex post*). Las tiendas de aplicaciones 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 (como símbolos que representen determinados tipos de acceso a datos sensoriales) y presentarlos de forma destacada en el catálogo de la tienda.

3.3.4 Terceras partes

En el tratamiento de los datos a través del uso de aplicaciones participan numerosos tipos de terceras partes.

Así, por ejemplo, muchas aplicaciones gratuitas se costean mediante publicidad que puede ser, aunque no exclusivamente, contextual o personalizada, facilitada mediante un sistema de seguimiento como *cookies* u otros identificadores del dispositivo. La publicidad puede consistir en un *banner* dentro de la aplicación o en anuncios fuera de la misma, presentados mediante la modificación de los parámetros del navegador o la colocación de iconos en el escritorio del dispositivo móvil o mediante una organización personalizada del contenido de la aplicación (p. ej, resultados de búsqueda patrocinados).

La publicidad de las aplicaciones suele ser suministrada por redes publicitarias e intermediarios similares que pueden estar vinculados con el fabricante del sistema operativo o la tienda de aplicaciones o ser la misma entidad. Tal como se señala en el dictamen 2/2010 de este grupo de trabajo[27], la publicidad en línea suele implicar el tratamiento de datos personales como se define en el artículo 2 de la Directiva sobre protección de datos y lo interpreta el grupo de trabajo del artículo 29[28].

Otros ejemplos de terceras partes son los proveedores de análisis y los prestadores de servicios de comunicaciones. Los proveedores de análisis permiten a los desarrolladores comprender el uso, la popularidad y la facilidad de uso de sus aplicaciones. Los proveedores de servicios de comunicaciones[29] también pueden desempeñar un papel importante al determinar los parámetros por defecto y las actualizaciones de seguridad de muchos dispositivos y pueden tratar datos sobre el uso de las aplicaciones. Su personalización («*branding*») podría tener consecuencias para las posibles medidas técnicas y funcionales que el usuario puede aplicar para proteger sus datos personales.

Con respecto a los desarrolladores de aplicaciones, las terceras partes pueden tener dos tipos de funciones. La primera consiste en realizar operaciones para el propietario de la aplicación como, por ejemplo, proporcionar análisis dentro de la aplicación. En ese caso, cuando actúan

---

[27] Dictamen 2/2010 sobre publicidad comportamental en línea, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf (junio de 2010).

[28] Véase también la interpretación del concepto de datos personales en el dictamen 4/2007 de este grupo de trabajo sobre ese tema (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf).

[29] Los proveedores de servicios de comunicaciones también están sujetos a obligaciones en materia de protección de datos que están fuera del ámbito de aplicación del presente dictamen.

exclusivamente en nombre del desarrollador de aplicaciones y no procesan datos para sus propios fines y/o comparten datos con los desarrolladores, es probable que actúen como encargados del tratamiento.

La segunda función consiste en recoger información de las aplicaciones para prestar servicios adicionales: proporcionar cifras para análisis a gran escala (popularidad de las aplicaciones, recomendación personalizada) o evitar la presentación del mismo anuncio a un mismo usuario. Cuando las terceras partes tratan datos personales para sus propios fines, actúan como responsables del tratamiento de datos y, por tanto, deben cumplir todas las disposiciones aplicables de la Directiva sobre protección de datos[30]. En el caso de la publicidad comportamental, el responsable del tratamiento debe obtener el consentimiento válido del usuario para la recogida y el tratamiento de datos personales, consistente, por ejemplo, en el análisis y la combinación de datos personales, y la creación y/o la aplicación de perfiles. Como ya se indicó en el dictamen 2/2012 sobre publicidad comportamental en línea, la mejor forma de anunciar dicho consentimiento es utilizar mecanismos de aceptación previa.

Una empresa proporciona datos métricos para los propietarios de aplicaciones y los anunciantes mediante el uso de rastreadores (*trackers*) incorporados a las aplicaciones por los desarrolladores de aplicaciones. Los rastreadores de la empresa pueden, por tanto, instalarse en numerosas aplicaciones y dispositivos. Uno de sus servicios es informar a los desarrolladores de qué otras aplicaciones utiliza un usuario, mediante la recogida de un identificador único. La empresa define los medios (es decir, los rastreadores) y los objetivos de sus herramientas antes de ofrecérselos a los desarrolladores, los anunciantes y otras partes y, por tanto, actúa como responsable del tratamiento de datos.

Las terceras partes deben cumplir, en la medida en que acceden o almacenan información en el dispositivo inteligente, el requisito de consentimiento del artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica electrónica.

En este contexto, es importante señalar que, en los dispositivos inteligentes, los usuarios suelen tener limitadas las posibilidades de instalar programas que puedan controlar el tratamiento de los datos personales, como es habitual en el entorno web del escritorio. Como alternativa al uso de *cookies* http, las terceras partes suelen acceder a identificadores únicos para singularizar a (grupos de) usuarios y proveerles servicios personalizados, incluida la publicidad. Dado que los usuarios no pueden borrar ni modificar muchos de esos datos (como el IMEI, el IIAM, el MSISDN[31] o identificadores específicos únicos del dispositivo añadidos por el sistema operativo), estas terceras partes tienen potencial para tratar importantes cantidades de datos personales sin el control del usuario final.

[30] Dictamen 2/2010 sobre publicidad comportamental en línea, p. 10-11.
[31] Iniciales inglesas del Número de Abonado Móvil de la Red Digital de Servicios Integrados.

3.4 Fundamento jurídico

Para tratar datos personales, se requiere un fundamento jurídico, según lo enumerado en el artículo 7 de la Directiva sobre protección de datos, que distingue seis condiciones para el tratamiento de datos personales: el consentimiento inequívoco del interesado; la necesidad para la ejecución de un contrato con el interesado; la protección de los intereses vitales del interesado; la necesidad del cumplimiento de una obligación jurídica; la realización (en el caso de las autoridades públicas) de cumplir una misión de interés público; y la necesidad (en el caso de las empresas) de satisfacer intereses legítimos.

En lo que respecta al almacenamiento de la información o la obtención del acceso a información ya almacenada en dispositivos inteligentes, el artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica (es decir, el requisito del consentimiento para la instalación y la extracción de datos de un dispositivo) establece una limitación o restricción más detallada de los fundamentos jurídicos que pueden tomarse en consideración.

3.4.1 Consentimiento previo a la instalación y tratamiento de datos personales

En el caso de las aplicaciones, el principal fundamento jurídico aplicable es el consentimiento. Al instalar una aplicación, se introduce información en el dispositivo del usuario final. Muchas aplicaciones también acceden a los datos almacenados en el dispositivo, la lista de contactos, las fotografías, los vídeos y otra documentación personal. En todos estos casos, el artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica exige el consentimiento del usuario tras habérsele facilitado información clara y completa, antes de la introducción y la extracción de datos del dispositivo.

Conviene observar la distinción entre el consentimiento requerido para introducir o leer información en el dispositivo y el consentimiento necesario para tener un fundamento jurídico para el tratamiento de los distintos tipos de datos personales. Aunque ambos requisitos de consentimiento son simultáneamente aplicables, cada uno de ellos a partir de un fundamento jurídico distinto, ambos están sujetos a las condiciones de ser libre, específico e informado (tal como se define en el artículo 2, letra h], de la Directiva sobre protección de datos). Por tanto, ambos tipos de consentimiento pueden unificarse en la práctica, ya sea durante la instalación o antes de que la aplicación comience a recoger datos personales del dispositivo, siempre que se informe al usuario de forma inequívoca de aquello a lo que está dando su acuerdo.

Muchas tiendas de aplicaciones ofrecen a los desarrolladores de aplicaciones la oportunidad de informar a los usuarios finales sobre las características fundamentales de una aplicación antes de la instalación y requieren una acción positiva del usuario antes de que la aplicación se descargue y se instale (p. ej., pulsar el botón «instalar»). Aunque, en algunas circunstancias, tal acción cumple el requisito de consentimiento del artículo 5, apartado 3, es improbable que aporte suficiente información para servir como consentimiento válido para el

tratamiento de datos personales. Este tema ya fue debatido por el grupo de trabajo en su dictamen 15/2011 sobre la definición del consentimiento[32].

En el contexto de los dispositivos inteligentes, el término «[manifestación de voluntad] libre» significa que el usuario debe tener la opción de aceptar o rechazar al tratamiento de sus datos personales. Por tanto, si una aplicación debe tratar datos personales, el usuario debe tener la libertad de aceptarlo o rechazarlo. El usuario no debería verse ante una pantalla que contenga una opción única «Sí, acepto» para completar la instalación, sino que debe disponer de una opción «Cancelar» o poder detener la instalación de otra forma.

El término «[manifestación de voluntad] informada» significa que el interesado dispone de los datos necesarios para formarse una opinión precisa[33]. Para evitar ambigüedades, la información debe estar disponible antes de que se produzca cualquier tratamiento de datos personales. Esto incluye los tratamientos de datos que puedan tener lugar durante la instalación, por ejemplo, para fines de seguimiento o depuración. El contenido y la forma de esa información se detallan en el apartado 3.7 del presente dictamen.

El término «[manifestación de voluntad] específica» significa que la manifestación de voluntad debe referirse al tratamiento de un dato o un tipo de datos concreto. Es por ello por lo 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. En algunos casos, el usuario puede dar un consentimiento diferenciado o «granular» cuando el consentimiento se requiere para cada tipo de datos a que la aplicación pretende acceder[34]. Este planteamiento permite satisfacer dos importantes requisitos legales: en primer lugar, el de informar al usuario sobre elementos importantes del servicio; y, en segundo lugar, el de solicitar el consentimiento específico para cada uno de ellos[35]. El planteamiento alternativo de que los desarrolladores de aplicaciones pidan a sus usuarios la aceptación de una larga serie de términos y condiciones y/o de su política de privacidad no constituye autorización específica[36].

El término «específico» también se refiere a la práctica del seguimiento del comportamiento de los usuarios por parte de anunciantes y otras terceras partes. Los parámetros por defecto que proporcionan los sistemas operativos y las aplicaciones deben evitar todo seguimiento, para permitir que los usuarios puedan dar consentimiento específico a ese tipo de tratamiento

---

[32] Dictamen 15/2011 sobre la definición del consentimiento de julio de 2011 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf).

[33] Ídem, p. 19.

[34] «Consentimiento diferenciado» significa que los usuarios pueden controlar en detalle (específicamente) las funciones de tratamiento de datos personales que ofrece la aplicación que ellos desean activar.

[35] La necesidad de tal consentimiento diferenciado también recibe el apoyo expreso de la FTC en su último informe (nota a pie de página nº 6), en cuyas páginas 15 y 16 se indica: «(...) las plataformas deben considerar la posibilidad de ofrecer información tipo 'justo a tiempo' y de obtener consentimiento expreso para la recogida de otros contenidos que muchos consumidores considerarían sensibles en muchos contextos como fotografías, contactos, entradas de agendas o grabaciones de audio o vídeo.».

[36] Ídem, p 34 y 35: «El consentimiento general sin una indicación exacta del objetivo del tratamiento que el interesado acepta no cumple ese requisito. Esto significa que la información sobre el objetivo del tratamiento no debe incluirse en las disposiciones generales, sino en la cláusula de consentimiento.».

de datos. Estos parámetros por defecto no pueden ser eludidos por terceras partes, como suele ocurrir actualmente con los mecanismos «Evitar seguimiento» aplicados en los navegadores.

Ejemplos de consentimiento específico

Una aplicación ofrece información sobre restaurantes cercanos. Para instalarla, el desarrollador debe obtener el consentimiento. Para acceder a los datos de geolocalización, el desarrollador de aplicaciones debe pedir el consentimiento por separado, por ejemplo, durante la instalación o antes de acceder a la geolocalización.
«Específico» significa que el consentimiento debe limitarse al objetivo concreto de informar al usuario sobre restaurantes próximos. Por tanto, solo puede accederse a los datos de localización del dispositivo cuando el usuario utiliza la aplicación a tal efecto. El consentimiento del usuario para procesar datos de geolocalización no permite a la aplicación la recogida continua de datos de localización del dispositivo. Este tratamiento adicional requeriría información adicional y un consentimiento por separado.

Del mismo modo, para que una aplicación de comunicaciones acceda a la lista de contactos, el usuario debe poder seleccionar los contactos con que desea comunicarse, en lugar de tener que dar acceso a toda la lista de contactos (incluidos los datos de contacto de quienes no son usuarios de ese servicio, que no pueden haber dado su consentimiento al tratamiento de los datos que les afectan).

No obstante, es importante señalar que incluso si el consentimiento cumple los tres elementos mencionados, esto no permite tratamientos ilícitos o desleales. Si la finalidad del tratamiento es excesiva y/o desproporcionada, incluso cuando el usuario haya dado su consentimiento, el desarrollador de aplicaciones no tendrá un fundamento jurídico válido y es probable que esté infringiendo la Directiva sobre protección de datos.

Ejemplo de tratamiento de datos excesivo e ilícito

Una aplicación de reloj despertador ofrece una función opcional para que el usuario pueda dar una orden verbal para detener la alarma o activar la función «snooze» (dormitar). En este ejemplo, el consentimiento de registro se limitaría al tiempo en que la alarma esté sonando. Todo seguimiento, registro o audio mientras la alarma no esté sonando se consideraría probablemente excesivo e ilícito.

En el caso de las aplicaciones instaladas en el dispositivo por defecto (antes de su adquisición por el usuario final) u otros tratamientos realizados por el sistema operativo que dependen del fundamento jurídico del consentimiento, los responsables del tratamiento deben estudiar cuidadosamente si dicho consentimiento es o no verdaderamente válido. En muchos casos, debería considerarse un mecanismo de consentimiento por separado, quizá cuando la aplicación se usa por primera vez, para ofrecer al responsable del tratamiento de datos la oportunidad de informar plenamente al usuario final. Cuando se trate de categorías especiales de datos, como se define en el artículo 8 de la Directiva sobre protección de datos, el consentimiento debe ser explícito.

Por último, pero no por ello menos importante, los usuarios deben tener la posibilidad de retirar su consentimiento de forma sencilla y eficaz, tema que se aborda en la sección 3.8 del presente dictamen.

3.4.2 Fundamento jurídico del tratamiento de datos durante el uso de la aplicación

Como se ha indicado anteriormente, el consentimiento es el fundamento jurídico necesario para permitir que los desarrolladores de aplicaciones lean y/o escriban datos legalmente y, por consiguiente, procesen datos personales. En una fase posterior, durante la utilización de la aplicación, el desarrollador puede invocar otros fundamentos jurídicos para otros tipos de tratamiento de datos, siempre que ello no implique el tratamiento de datos sensibles de carácter personal.

Estos fundamentos jurídicos pueden consistir en la necesidad para la ejecución de un contrato con el interesado o en la necesidad para la satisfacción de intereses (empresariales) legítimos, artículo 7, letras b) y f), de la Directiva sobre protección de datos.

Estos fundamentos jurídicos se limitan al tratamiento de datos personales no sensibles de un usuario concreto, y solo pueden invocarse en la medida en que determinado tratamiento de datos sea estrictamente necesario para realizar el servicio deseado o, en el caso del artículo 7, letra f), solo si el interés de los derechos y libertades fundamentales del interesado no prevalecen sobre tales intereses.

Ejemplos de fundamento jurídico contractual

Un usuario da su consentimiento a la instalación de una aplicación de banca móvil. Para atender una solicitud de pago, el banco no tiene que solicitar el consentimiento separado del usuario para revelar su nombre y número de cuenta bancaria al beneficiario del pago. Esa información es estrictamente necesaria para ejecutar el contrato con ese usuario concreto y, por tanto, el banco tiene un fundamento jurídico en el artículo 7, letra b), de la Directiva sobre protección de datos. El mismo razonamiento es aplicable a las aplicaciones de comunicaciones: cuando se proporciona información esencial como el nombre de una cuenta, una dirección de correo electrónico o un número de teléfono a otra persona con la que el usuario desea comunicarse, es evidente que la información es necesaria para la ejecución del contrato.

3.5 Limitación de la finalidad y minimización de datos

Los principios fundamentales de la Directiva sobre protección de datos son la limitación de la finalidad y la minimización de datos. La limitación de la finalidad permite a los usuarios optar deliberadamente por confiar a una de las partes sus datos personales, dado que sabrán cómo se usan esos datos y podrán confiar en la descripción de la finalidad limitada para comprender los fines para los que se utilizarán los mismos. Por tanto, la finalidad del tratamiento de datos debe estar bien definida y ser comprensible para un usuario medio sin conocimientos jurídicos o técnicos especiales.

Al mismo tiempo, la limitación de la finalidad exige a los desarrolladores de aplicaciones tener una visión correcta de sus argumentos comerciales, antes de comenzar a recoger datos personales de los usuarios. Los datos personales solo pueden tratarse con una finalidad leal y lícita (artículo 6, apartado 1, letra a], de la Directiva sobre protección de datos) y esa finalidad debe definirse antes de realizar el tratamiento.

El principio de limitación de la finalidad excluye los cambios súbitos de las condiciones clave del tratamiento.

Por ejemplo, si el objetivo original de una aplicación es permitir a los usuarios enviarse correos electrónicos entre sí, pero el desarrollador decide cambiar su modelo empresarial y fusiona las direcciones de correo electrónico de los usuarios con los números de teléfono de los usuarios de otra aplicación, los respectivos responsables del tratamiento de datos tendrían que dirigirse a todos los usuarios individualmente y solicitar su consentimiento previo e inequívoco para esa nueva finalidad del tratamiento de los datos personales.

La limitación de la finalidad va unida al principio de minimización de datos. Para evitar el tratamiento de datos innecesario y potencialmente ilícito, los desarrolladores de aplicaciones deben considerar atentamente los datos que son estrictamente necesarios para realizar la función deseada.

Las aplicaciones pueden acceder a muchas funciones del dispositivo y, por tanto, son capaces de hacer muchas cosas, como enviar SMS furtivos o acceder a imágenes y a la lista de contactos. Muchas tiendas de aplicaciones soportan actualizaciones (semi)automáticas en las que los desarrolladores de aplicaciones pueden integrar nuevas características y hacer accesibles dichos archivos con poca o ninguna intervención del usuario final.

En este punto, el grupo de trabajo desea subrayar que las terceras partes que pueden acceder a los datos del usuario a través de las aplicaciones deben respetar los principios de limitación de la finalidad y minimización de datos. Los identificadores únicos, a menudo no modificables, no deben utilizarse para fines publicitarios y/o analíticos basados en intereses, debido a la incapacidad de los usuarios para revocar la autorización. Los desarrolladores de aplicaciones deben garantizar que se impide la desvirtuación de funciones evitando el cambio del tratamiento que efectúa una versión de una aplicación por el que hace otra sin enviar a los usuarios finales anuncios informativos y darles la oportunidad de renunciar al tratamiento o al conjunto del servicio. También deben ofrecerse a los usuarios medios técnicos para verificar las declaraciones sobre objetivos predeterminados, dándoles acceso a información sobre los flujos de tráfico saliente por aplicación, en relación con el tráfico iniciado por ellos mismos.

La información y la supervisión por el usuario son aspectos fundamentales para garantizar el respeto de los principios de la minimización de datos y la limitación de la finalidad.

El acceso a los datos subyacentes del dispositivo a través de las aplicaciones da a los fabricantes de sistemas operativos y dispositivos y a las tiendas de aplicaciones la oportunidad de hacer cumplir normas específicas y ofrecer información adecuada a los usuarios finales. Por ejemplo, los fabricantes de sistemas operativos y dispositivos deben ofrecer una aplicación con controles precisos para diferenciar cada tipo de esos datos y garantizar que los desarrolladores de aplicaciones pueden solicitar acceso solo a los datos estrictamente necesarios para el funcionamiento (lícito) de sus aplicaciones. Los tipos de datos solicitados por los desarrolladores de aplicaciones pueden, entonces, mostrarse claramente en las tiendas de aplicaciones para informar al usuario antes de la instalación.

A este respecto, el control del acceso a los datos almacenados en el dispositivo se basa en diversos mecanismos:

a. Los fabricantes de sistemas operativos y dispositivos y las tiendas de aplicaciones definen **las normas** vigentes para presentar aplicaciones en su tienda: los desarrolladores de aplicaciones deben respetar esas normas o correr el riesgo de no estar disponibles en esas tiendas[37].
b. Las **API** de los sistemas operativos establecen métodos normalizados para acceder a los datos almacenados en el teléfono al que tienen acceso las aplicaciones. Además, también influyen en la recogida de datos desde el lado del servidor.
c. **Controles *ex ante***: controles aplicados antes de instalar una aplicación[38].
d. **Controles *ex post***: controles aplicados tras haber instalado una aplicación.

3.6 Seguridad

De acuerdo con el artículo 17 de la Directiva sobre protección de datos, los responsables y los encargados del tratamiento deben adoptar las medidas técnicas y organizativas necesarias para garantizar la protección de los datos personales que traten. Como consecuencia de ello, todos los agentes indicados en la sección 3.3 deben adoptar medidas, cada uno de ellos según su papel y sus responsabilidades.

El objetivo del cumplimiento de las obligaciones en materia de seguridad es doble: permitir a los usuarios controlar sus datos con más rigor y aumentar el grado de confianza en las entidades que realmente procesan datos de los usuarios.

A fin de cumplir con sus respectivas obligaciones en materia de seguridad como responsables del tratamiento de datos, los desarrolladores de aplicaciones, las tiendas de aplicaciones, los fabricantes de sistemas operativos y dispositivos, y las terceras partes deben tener en cuenta los principios de protección de la intimidad desde el diseño y por defecto, lo cual exige una evaluación continua de los riesgos actuales y futuros para la protección de los datos, y la aplicación y la evaluación de medidas correctoras eficaces, incluida la minimización de datos.

Desarrolladores de aplicaciones

Los fabricantes de sistemas operativos y dispositivos y terceras partes como ENISA[39] han publicado numerosas directrices relativas a la seguridad de las aplicaciones para dispositivos móviles.

La revisión de todas las mejores prácticas en materia de seguridad en el desarrollo de aplicaciones queda fuera del ámbito del presente dictamen; sin embargo, el grupo de trabajo aprovecha esta oportunidad para examinar las que pueden llegar a repercutir gravemente en los derechos fundamentales de los usuarios de aplicaciones.

---

[37] Los dispositivos «liberados» o «desprotegidos» (*jailbroken*) permiten la instalación de aplicaciones al margen de las tiendas oficiales; los dispositivos Android también permiten la instalación de aplicaciones de otras fuentes.

[38] Con el caso particular de las aplicaciones preinstaladas.

[39] *Smartphone Secure Development Guideline* de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA): http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

Una decisión importante antes de diseñar una aplicación es la de dónde se almacenarán los datos. En algunos casos los datos de usuario se almacenan en el dispositivo, pero los desarrolladores de aplicaciones también pueden utilizar una arquitectura cliente-servidor. Esto significa que los datos personales se transfieren a los sistemas del proveedor de servicios o se copian en ellos. El almacenamiento y el tratamiento de datos en el dispositivo da a los usuarios finales el máximo control sobre esos datos al permitirles, por ejemplo, suprimir los datos si retiran su consentimiento a su tratamiento. Sin embargo, el almacenamiento de datos a distancia puede ayudar a su recuperación en caso de pérdida o robo del dispositivo. También son posibles métodos intermedios.

Los desarrolladores de aplicaciones deben indicar unas políticas claramente definidas sobre cómo se elaboran y se distribuyen sus programas. También los fabricantes de sistemas operativos y dispositivos desempeñan un papel en el fomento de tratamientos seguros por parte de las aplicaciones, en el que se abundará más abajo. En segundo lugar, los desarrolladores de aplicaciones y las tiendas de aplicaciones deben diseñar y aplicar un entorno favorable a la seguridad, con herramientas que impidan la propagación de aplicaciones maliciosas y permitan la instalación y desinstalación sencillas de cada aplicación.

Algunas buenas prácticas que pueden aplicarse durante el diseño de una aplicación son la minimización de las líneas y la complejidad del código, y la aplicación de controles para excluir que los datos puedan transferirse o comprometerse involuntariamente. Además, deberían validarse todas las entradas para evitar desbordamientos de búfer o ataques de inyección. Otros mecanismos de seguridad que cabe destacar son la adecuación de las estrategias de gestión de los parches de seguridad y la realización de auditorías independientes de seguridad del sistema. Además, los criterios de diseño de aplicaciones deberían incluir la aplicación del principio del mínimo privilegio por defecto, según el cual las aplicaciones pueden acceder únicamente a los datos que realmente necesitan para poner una función a disposición del usuario. Los desarrolladores de aplicaciones y las tiendas de aplicaciones también deben alentar a los usuarios, mediante advertencias, a complementar esas buenas prácticas de diseño con prácticas de usuario adecuadas como la actualización de sus aplicaciones con las últimas versiones disponibles, y recordatorios para evitar el uso repetido de contraseñas en los distintos servicios.

Durante la fase de diseño de la aplicación, los desarrolladores también deben tomar medidas para evitar el acceso no autorizado a datos personales, garantizando la protección de datos tanto en tránsito como, en su caso, almacenados.

Las aplicaciones móviles deben funcionar en puntos específicos de la memoria de los dispositivos (separados por «aislamiento de procesos»[40]), con objeto de reducir las consecuencias de los programas y las aplicaciones maliciosas. Los desarrolladores de aplicaciones deben utilizar, en estrecha colaboración con los fabricantes de sistemas operativos y las tiendas de aplicaciones, los mecanismos disponibles que permitan a los usuarios ver qué datos se están tratando en qué aplicaciones, y permitirles activar o desactivar

[40] Se trata de mecanismos de seguridad para separar los programas en funcionamiento.

de manera selectiva los correspondientes permisos. El uso de funciones ocultas no debe estar autorizado.

Los desarrolladores de aplicaciones deben considerar atentamente sus métodos de identificación y acreditación del usuario. No deben utilizar identificadores persistentes (específicos de los dispositivos) sino, por el contrario, usar identificadores de baja entropía específicos de cada aplicación o identificadores temporales del dispositivo, con objeto de evitar el seguimiento de usuarios a lo largo del tiempo. Debería considerarse el uso de mecanismos de autenticación más respetuosos de la intimidad. Al autenticar a los usuarios, los desarrolladores de aplicaciones deben prestar especial atención a la gestión de los códigos de identificación y las contraseñas de los usuarios. Estas últimas deben almacenarse cifradas y de forma segura, como un valor criptográfico de comprobación aleatoria cifrado. Poner a disposición de los usuarios un test de solidez de las contraseñas que eligen, también es una técnica útil para promover mejores contraseñas (comprobación de entropía). Asimismo, podría contemplarse la autenticación repetida (o reautenticación) cuando corresponda (acceso a datos sensibles y acceso a recursos de pago), también por medio de factores múltiples y canales diversos (por ejemplo, código de acceso enviado por SMS) y/o el uso de datos de autentificación vinculados al usuario final (en lugar del dispositivo). Además, al seleccionar identificadores de sesión, deben utilizarse series imprevisibles, posiblemente en combinación con información contextual como la fecha y la hora, además de la dirección IP o los datos de geolocalización.

Los desarrolladores de aplicaciones también deberían tener 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. Aunque estos requisitos actualmente solo se aplican a los proveedores de servicios de comunicaciones electrónicas disponibles públicamente, es de esperar que la obligación se extienda a todos los responsables (y los encargados) del tratamiento mediante el futuro Reglamento sobre protección de datos, según las propuestas de la Comisión (COM 2012/0011/COD). Esto subraya la necesidad de disponer de un «plan de seguridad» detallado continuamente evaluado, que cubra la recogida, el almacenamiento y el tratamiento de datos personales, a fin de impedir las infracciones y evitar incurrir en las fuertes sanciones económicas previstas en tales casos. El plan de seguridad debe prever, entre otras cosas, la gestión de la vulnerabilidad y la divulgación oportuna y segura de soluciones fiables a los problemas.

La responsabilidad de los desarrolladores de aplicaciones en cuanto a la seguridad de sus productos no termina con la puesta en el mercado de una versión operativa. Las aplicaciones, como cualquier producto de *software*, pueden sufrir deficiencias de seguridad y tener puntos vulnerables, por lo que los desarrolladores deben elaborar soluciones o parches para los mismos y suministrárselos a aquellas partes que pueden ponerlas a disposición de los usuarios o hacerlo ellos mismos.

Tiendas de aplicaciones

Las tiendas de aplicaciones son un importante intermediario entre los usuarios finales y los desarrolladores de aplicaciones, por lo que deben incluir una serie de controles sólidos y eficaces de las aplicaciones antes de admitirlas en el mercado. Dichas tiendas deben proporcionar información sobre los controles que efectúan y sobre los tipos de controles que realizan del cumplimiento de la normativa sobre protección de datos.

Aunque esta medida no sea eficaz al 100 % a la hora de eliminar la diseminación de aplicaciones maliciosas, las estadísticas muestran que esta práctica reduce considerablemente la aparición de funciones maliciosas en las tiendas de aplicaciones «oficiales»[41]. A fin de hacer frente al gran número de aplicaciones que se presentan a diario, este proceso podría beneficiarse de la disponibilidad de herramientas de análisis automático y de la creación de canales de intercambio de información entre los expertos en seguridad y los profesionales de la programación, así como de procedimientos y políticas eficaces que atajen los problemas comunicados.

Además de revisar las aplicaciones antes de admitirlas en las tiendas de aplicaciones, las aplicaciones deben someterse, también, a un mecanismo de evaluación pública. Los usuarios deben calificar las aplicaciones no solo en cuanto a sus aspectos más «actuales» sino también por sus funciones, haciendo especial referencia a los mecanismos de protección de la intimidad y la seguridad. Asimismo, deberían diseñarse mecanismos para evitar falsas calificaciones. Los mecanismos de calificación y evaluación de aplicaciones también pueden resultar eficaces para crear confianza mutua entre las distintas entidades, especialmente si los datos son objeto de intercambio a través de una larga cadena de terceros.

Las tiendas de aplicaciones suelen aplicar un método para desinstalar a distancia aplicaciones malintencionadas o no seguras. Si no se diseña debidamente este mecanismo puede constituir un obstáculo para dar a los usuarios un mayor control de sus datos. Por tanto, una forma de permitir a las tiendas de aplicaciones la desinstalación remota de aplicaciones respetando la intimidad debería basarse en la información y el consentimiento del usuario. Por otra parte, desde un punto de vista más práctico, los usuarios deberían contar con canales de retroalimentación para notificar problemas de seguridad relacionados con sus aplicaciones y la eficacia de todo procedimiento de desinstalación remota.

Al igual que los desarrolladores de aplicaciones, las tiendas de aplicaciones 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.

Fabricantes de sistemas operativos y dispositivos

Los fabricantes de sistemas operativos y dispositivos también desempeñan un papel importante en la fijación de normas mínimas y mejores prácticas entre los desarrolladores de aplicaciones, no solo en cuanto a la seguridad de los programas y las API subyacentes, sino también en lo relativo a las herramientas, las orientaciones y el material de referencia que distribuyen. Los fabricantes de sistemas operativos y dispositivos deben distribuir algoritmos de cifrado fuertes y bien conocidos y soportar longitudes de clave apropiadas. Asimismo, deben poner a disposición de los desarrolladores de aplicaciones mecanismos de autenticación fuertes y seguros (p. ej., el uso de certificados firmados por autoridades de certificación fidedignas para verificar la autorización de una fuente remota). Esto evitaría también la necesidad de que los desarrolladores de aplicaciones trabajen en mecanismos de autenticación

[41] «*Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets*», Y Zhou y otros, Network and Distributed System Security Symposium (NDSS) 2012.

protegidos por derechos de propiedad intelectual. En la práctica, esto suele aplicarse deficientemente y pueden representar una vulnerabilidad grave[42].

El acceso y el tratamiento de datos personales por las aplicaciones deben gestionarse mediante tipos de API integrados y métodos que aporten controles y salvaguardias adecuados. Los fabricantes de sistemas operativos y dispositivos deben garantizar que los métodos y las funciones que permiten acceder a datos personales incluyen características destinadas a aplicar las solicitudes de consentimiento granular. Del mismo modo, deben emprenderse acciones para excluir o limitar el acceso a datos personales utilizando funciones de bajo nivel u otros medios que pudieran eludir los controles y las salvaguardias incorporadas en las API.

Asimismo, los fabricantes de sistemas operativos y dispositivos deben desarrollar líneas de auditoría claras en los dispositivos, de modo que los usuarios finales puedan ver claramente qué aplicaciones han estado accediendo a los datos de sus dispositivos.

Todas las partes deben responder con rapidez a los puntos débiles en materia de seguridad en los plazos adecuados, de forma que los usuarios finales no se vean innecesariamente expuestos a deficiencias de seguridad. Desgraciadamente, algunos fabricantes de sistemas operativos y dispositivos (así como los operadores de telecomunicaciones cuando distribuyen dispositivos de marca) no proporcionan apoyo a largo plazo a las versiones del sistema operativo, lo que deja a los usuarios indefensos contra puntos débiles de la seguridad bien conocidos. Los fabricantes de sistemas operativos y dispositivos, junto con los desarrolladores de aplicaciones, deben proporcionar a los usuarios finales información por adelantado sobre el periodo en el que pueden esperar actualizaciones de seguridad periódicas. Asimismo, deben informar cuanto antes a los usuarios cuando un aspecto de seguridad debe repararse mediante una actualización.

Terceras partes

Las características y consideraciones de seguridad citadas deben ser aplicadas también por las terceras partes al recoger y procesar datos personales para sus propios fines, especialmente los anunciantes y los proveedores de análisis. Esto incluye la transmisión segura y el almacenamiento cifrado de identificadores únicos de dispositivos y aplicaciones y otros datos personales.

3.7 Información

3.7.1 Obligación de informar y contenido requerido

De conformidad con el artículo 10 de la Directiva sobre protección de datos, cada interesado tiene derecho a conocer la identidad del responsable del tratamiento de datos que está tratando

---

[42] Recientemente, también se ha señalado que la falta de indicadores de seguridad visuales para el uso de protocolos SSL/TLS y el uso inadecuado de SSL/TLS pueden aprovecharse para lanzar ataques de los denominados *man-in-the-middle* (MITM o «de intermediario»). Según estudios recientes, la base instalada acumulada de las aplicaciones con vulnerabilidades confirmadas contra ataques MITM incluye varios millones de usuarios. «*Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security*», Bernd Freisleben y Matthew Smith, 19ª Conferencia ACM sobre seguridad informática y de las comunicaciones (ACM CCS 2012).

sus datos personales. Además, en el contexto de las aplicaciones, el usuario final tiene derecho a saber qué tipo de datos personales están siendo tratados y con qué finalidad se quiere usarlos. Si los datos personales del usuario se recogen a partir de otros agentes del ecosistema de las aplicaciones (como se describe en la sección 3.3 del presente dictamen), el usuario final, de conformidad con el artículo 11 de la Directiva sobre protección de datos, tiene, en todo caso, derecho a ser informado de ese tratamiento de datos del modo ya descrito. Por tanto, si se tratan datos personales, el responsable del tratamiento pertinente deberá informar a los usuarios potenciales, como mínimo, de:

- quiénes son (identidad y datos de contacto)
- las categorías exactas de datos personales que el desarrollador de aplicaciones recogerá y tratará
- los objetivos precisos
- si los datos se comunicarán a terceros
- la forma en que los usuarios pueden ejercer sus derechos (retirar el consentimiento y eliminar datos).

La disponibilidad de esta información sobre el tratamiento de datos personales es imprescindible para obtener el consentimiento del usuario para tal tratamiento. El consentimiento solo puede ser válido si la persona ha sido previamente informada sobre los principales elementos del tratamiento de datos. Facilitar dicha información únicamente después de que el tratamiento de datos personales se haya iniciado (que suele comenzar durante la instalación) no se considera suficiente ni tiene validez jurídica. De acuerdo con el informe de la FTC, el grupo de trabajo subraya la necesidad de proporcionar información en el momento en que es importante para los consumidores, justo antes de la recogida de esa información por las aplicaciones. Ser informado de qué datos se están tratando es especialmente importante, habida cuenta del amplio acceso que las aplicaciones suelen tener a sensores y estructuras de datos del dispositivo, donde dicho acceso no es, en muchos casos, obvio. La información adecuada también es de vital importancia cuando las aplicaciones tratan categorías especiales de datos personales como, por ejemplo, el estado de salud, las creencias políticas, la orientación sexual, etc. Por último, los desarrolladores de aplicaciones deben diferenciar claramente la información obligatoria y opcional, y el sistema debe permitir al usuario denegar el acceso a información opcional utilizando por defecto opciones respetuosas de la intimidad.

Por lo que se refiere a la identidad del responsable del tratamiento de los datos, los usuarios deben saber quién es legalmente responsable del tratamiento de sus datos personales y cómo puede ponerse en contacto con él, ya que en caso contrario, no pueden ejercer derechos como el de acceder a los datos almacenados (a distancia) sobre ellos. Dado el carácter fragmentario del entorno de las aplicaciones, es fundamental que cada aplicación tenga un punto de contacto único, donde se asuma la responsabilidad de todo tratamiento de datos que tenga lugar a través de la aplicación. No debe dejarse al usuario final la investigación de las relaciones entre los desarrolladores de aplicaciones y otras partes relacionadas con el tratamiento de datos personales a través de la aplicación.

Por lo que se refiere a los objetivos, los usuarios finales deben estar adecuadamente informados sobre los datos que se recogen sobre ellos y por qué. Asimismo, los usuarios deben ser informados en un lenguaje claro y sencillo de si los datos pueden ser reutilizados por otras partes y, en caso afirmativo, con qué fines. Conceptos elásticos como «innovación

de productos» no resultan adecuados para informar a los usuarios. Debe indicarse claramente si se pedirá el consentimiento de los usuarios para compartir datos con terceros para fines de publicidad o análisis. Las tiendas de aplicaciones tienen la importante responsabilidad de garantizar que esa información se encuentra disponible y fácilmente accesible en el caso de cada aplicación.

Además, también tienen la responsabilidad de garantizar una información adecuada. Se recomienda vivamente el uso de significadores visuales o iconos relativos al uso de los datos para informar a los usuarios de los tipos de tratamiento de datos.

Además de mantener la información mínima necesaria para obtener el consentimiento del usuario de las aplicaciones, el grupo de trabajo aconseja encarecidamente, en aras del tratamiento leal de los datos personales, que los responsables del tratamiento de datos transmitan a los usuarios también la siguiente información:

- consideraciones de proporcionalidad en cuanto a los tipos de datos recogidos o a que se ha accedido en el dispositivo
- periodos de conservación de los datos
- las medidas de seguridad aplicadas por el responsable del tratamiento de datos.

El grupo de trabajo también recomienda que los desarrolladores de aplicaciones incluyan en su política de privacidad dedicada a los usuarios europeos información sobre cómo se ajusta la aplicación a la normativa europea de protección de datos, incluidas las posibles transferencias de datos personales desde Europa a, por ejemplo, Estados Unidos, y, en tal caso, si la aplicación se ajusta al denominado «marco de puerto seguro» y de qué manera.

3.7.2 Forma de la información

La información esencial sobre el tratamiento de datos debe estar a disposición de los usuarios antes de instalar la aplicación a través de la tienda de aplicaciones. En segundo lugar, la información pertinente sobre el tratamiento de datos debe ser accesible desde dentro de la aplicación, tras su instalación.

Como responsables, junto con los desarrolladores de aplicaciones, en cuanto a la información, las tiendas de aplicaciones deben garantizar que cada aplicación ofrece la información esencial sobre el tratamiento de datos personales. Deben comprobar que los hiperenlaces incluyen páginas de información sobre la privacidad y eliminar las aplicaciones con enlaces inactivos o información inaccesible por otras razones sobre el tratamiento de datos.

El grupo de trabajo recomienda que la información sobre el tratamiento de datos personales esté también disponible y fácilmente localizable, por ejemplo dentro de la tienda de aplicaciones y, preferiblemente, en los sitios web del desarrollador responsable de la aplicación. Es inaceptable que los usuarios se vean en una situación en la que tendrían que buscar en la web información sobre las políticas de tratamiento de datos de la aplicación en lugar de ser informados directamente por el desarrollador de la misma u otro responsable del tratamiento de los datos.

Como mínimo, cada aplicación debería contar con una política de privacidad legible, comprensible y fácilmente accesible, donde se incluya toda la información antes mencionada. Muchas aplicaciones no cumplen este requisito mínimo de transparencia. Según el informe

del foro FPF de junio de 2012, el 56 % de la las aplicaciones de pago y cerca del 30 % de las aplicaciones gratuitas carecen de política de privacidad.

Las aplicaciones que no tratan datos personales (o no están destinadas a ello) deben indicarlo claramente en su política de privacidad.

Lógicamente existen limitaciones en cuanto a la cantidad de información que puede presentarse en una pantalla pequeña, pero esto no debe servir de excusa para no informar adecuadamente a los usuarios finales, ya que pueden aplicarse diversas estrategias para garantizar que se informa de los elementos fundamentales del servicio. El grupo de trabajo considera beneficioso el uso de los avisos breves como se detalla en su dictamen 10/2004[43], según el cual el primer aviso destinado al usuario contiene la información mínima exigida en el marco jurídico de la UE y se pone a su disposición información complementaria a través de enlaces al conjunto de la política de privacidad. La información debe presentarse directamente en la pantalla, ser de fácil acceso y tener gran visibilidad. Además de información completa y adecuada para la pantalla pequeña de los dispositivos móviles, los usuarios deben poder acceder mediante enlaces a explicaciones más detalladas, por ejemplo, en la política de privacidad sobre el modo en que la aplicación utiliza los datos personales, quién es el responsable del tratamiento de los datos y dónde puede un usuario hacer valer sus derechos.

Este planteamiento puede combinarse con el uso de iconos, imágenes, vídeo y audio, y hacer uso de notificaciones contextuales en tiempo real cuando una aplicación accede a la lista de contactos o a fotografías[44]. Estos iconos deben ser significativos, es decir, claros, autoexplicativos y sin ambigüedades. Evidentemente, los fabricantes de sistemas operativos tienen una importante responsabilidad en la facilitación del uso de dichos iconos.

De hecho, los desarrolladores de aplicaciones son brillantes al programar y diseñar interfaces complejas para las pequeñas pantallas, por lo que el grupo de trabajo pide al sector que utilice ese talento creativo para ofrecer soluciones más innovadoras, con objeto de informar de manera eficaz a los usuarios mediante los dispositivos móviles. A fin de garantizar que la información es realmente comprensible para los usuarios sin conocimientos técnicos o jurídicos, el grupo de trabajo (en consonancia con el informe de la FTC) recomienda encarecidamente someter las estrategias de información elegidas a encuestas entre los consumidores[45].

3.8 Derechos del interesado

Según los artículos 12 y 14 de la Directiva sobre protección de datos, los desarrolladores de aplicaciones y otros responsables del tratamiento de datos del ecosistema de las aplicaciones móviles deben permitir a los usuarios ejercer sus derechos de acceso, rectificación, supresión y bloqueo del tratamiento de datos. Si un usuario ejerce el derecho de acceso, el responsable

---

[43] Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información, de julio de 2004 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_es.pdf).

[44] Por ejemplo, el icono de advertencia para el tratamiento de geolocalización utilizado en el iPhone.

[45] Informe de la FTC indicado en la nota 6, p. 16.

del tratamiento debe proporcionarle información sobre los datos que se están tratando y la fuente de esos datos. Si el responsable del tratamiento toma decisiones automatizadas sobre los datos recogidos, también debe informar al usuario sobre la lógica de esas decisiones. Este podría ser el caso cuando se evalúa la actuación o la conducta de los usuarios basándose, por ejemplo, en datos financieros, sanitarios u otros datos del perfil. Sujeto a la solicitud del usuario, el responsable del tratamiento de datos de la aplicación debe permitir también la rectificación, la supresión o el bloqueo de datos personales si son incompletos, inexactos o tratados de forma ilícita.

Para que los usuarios puedan controlar el tratamiento de sus datos personales, las aplicaciones deben informarles de forma clara y visible de la existencia de dichos mecanismos de acceso y corrección. El grupo de trabajo recomienda el diseño y la aplicación de herramientas de acceso en línea simples pero seguras. Las herramientas de acceso deben estar accesibles preferiblemente dentro de cada aplicación o a través de un enlace a un mecanismo en línea mediante el que los usuarios puedan acceder inmediatamente a todos los datos objeto de tratamiento y a las explicaciones correspondientes. Los proveedores de servicios en línea han utilizado iniciativas similares, como pueden ser distintos cuadros de instrumentos y otros mecanismos de acceso.

La necesidad de fácil acceso en línea es especialmente marcada en el caso de las aplicaciones que tratan perfiles de usuario ricos en información como los de creación de redes, las aplicaciones sociales y de mensajería o las aplicaciones que tratan datos sensibles o financieros. Lógicamente, el acceso debe concederse únicamente si se ha comprobado la identidad del interesado, a fin de evitar la filtración de datos a terceros. No obstante, esta obligación de verificar la identidad correcta no debe dar lugar a una recogida adicional y excesiva de datos personales sobre el interesado. En muchos casos, podría bastar con la autenticación, en lugar de la identificación (completa).

Por otro lado, los usuarios deben disponer siempre de la posibilidad de retirar su consentimiento de manera simple y cómoda. Los interesados deben poder retirar su consentimiento al tratamiento de datos de diversas maneras y por motivos diferentes. Sería preferible que la opción de retirada del consentimiento estuviera disponible a través de los mecanismos de fácil acceso arriba mencionados. Debe ser posible desinstalar aplicaciones y, con ello, eliminar todos los datos personales, incluidos aquellos almacenados en los servidores de los responsables del tratamiento de datos. Para permitir que los usuarios puedan pedir a los desarrolladores de aplicaciones la eliminación de sus datos, los fabricantes de sistemas operativos podrían enviar a los primeros una señal cuando el usuario desinstala una aplicación. Dicha señal podría enviarse mediante la API. En principio, una vez que el usuario ha desinstalado la aplicación, el desarrollador carece de fundamento jurídico para continuar tratando los datos personales relativos al usuario y debe, por tanto, eliminar todos sus datos. Los desarrolladores de aplicaciones que deseen conservar determinados datos para, por ejemplo, facilitar la reinstalación de la aplicación, deben solicitar por separado el consentimiento durante el proceso de desinstalación, pidiendo al usuario su acuerdo durante un determinado periodo de conservación añadido. La única excepción a esta norma es la

posible existencia de la obligación legal de conservar algunos datos para fines concretos como, por ejemplo, las obligaciones fiscales relativas a transacciones financieras[46].

3.9 Periodos de conservación

Los desarrolladores de aplicaciones deben considerar la conservación de datos recogidos con la aplicación y los riesgos para la protección de datos que se plantean. Los plazos concretos dependerán de la finalidad de la aplicación y de la relevancia de los datos para el usuario final. Así, por ejemplo, una aplicación para compartir agendas, diarios o fotos pondría el plazo de conservación bajo el control del usuario final mientras que en el caso de una aplicación de navegación puede bastar con almacenar solo las últimas diez visitas hechas recientemente. Los desarrolladores de aplicaciones también deben tener en cuenta los datos de los usuarios que no hayan utilizado la aplicación durante un periodo prolongado. Estos usuarios pueden haber perdido su dispositivo móvil o haberlo cambiado por otro dispositivo sin haber desinstalado activamente todas las aplicaciones del primero. Por tanto, los desarrolladores de aplicaciones deben fijar previamente un periodo de inactividad tras el cual la cuenta se considerará expirada y garantizar que se informa al usuario de ese plazo. Expirado ese plazo, el responsable del tratamiento deberá alertar al usuario y darle la posibilidad de recuperar sus datos personales. Si el usuario no responde al aviso, sus datos personales o los relativos al uso de la aplicación deben hacerse anónimos o suprimirse de forma irreversible. El periodo de validez del recordatorio dependerá del propósito de la aplicación y del lugar en que se almacenen los datos. Si se trata de datos almacenados en el propio dispositivo como, por ejemplo, una puntuación alta en un juego, los datos pueden conservarse mientras la aplicación permanezca instalada. Si se trata de datos que se utilizan únicamente una vez al año como, por ejemplo, la información sobre una estación de esquí, el periodo de validez del recordatorio podría ser de 15 meses.

3.10 Niños

Los niños son ávidos usuarios de aplicaciones, ya sea en dispositivos propios o en dispositivos compartidos (con sus padres, sus hermanos o en un centro educativo), y existe claramente un gran mercado de aplicaciones diversas destinadas a ellos. Pero, al mismo tiempo, los niños apenas comprenden o conocen, si es que lo hacen en absoluto, el alcance y la sensibilidad de los datos a que las aplicaciones pueden acceder, o el alcance de los datos compartidos con terceros para fines publicitarios.

El grupo de trabajo ha abordado ampliamente la cuestión del tratamiento de datos sobre niños en su dictamen 2/2009 sobre la protección de los datos personales de los niños, por lo que en

---

[46] El grupo de trabajo recuerda a todos los servicios de la sociedad de la información, como las aplicaciones, que la obligación de conservación de datos (Directiva 2006/24/CE) 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. El grupo de trabajo aprovecha esta oportunidad para subrayar el carácter especialmente peligroso del tráfico de datos, que merece precauciones y salvaguardias especiales *per se*, como ya se señaló en el informe de este grupo de trabajo sobre la aplicación de la Directiva de conservación de datos (GT172), donde se llamaba a todas las partes interesadas a aplicar medidas de seguridad apropiadas.

este apartado solo se aborda una serie de riesgos y recomendaciones específicos de las aplicaciones[47].

Los desarrolladores de aplicaciones y otros responsables del tratamiento de datos deben prestar atención al límite de edad que define a los niños y los menores de edad en las legislaciones nacionales, donde el consentimiento parental al tratamiento de datos es una condición previa para que las aplicaciones traten datos de forma lícita[48].

Cuando el consentimiento puedan darlo legalmente los menores y la aplicación esté destinada a niños o menores, el responsable del tratamiento de datos debe prestar atención a las posibles limitaciones de comprensión y atención de los menores sobre dicho tratamiento. Debido a su vulnerabilidad general, y teniendo en cuenta que los datos personales deben tratarse de manera justa y lícita, los responsables del tratamiento de datos sobre niños deben respetar de forma aún más rigurosa el principio de minimización de datos y limitación de la finalidad. Concretamente, los responsables del tratamiento no deben procesar los datos sobre niños con fines de publicidad comportamental, ni directa ni indirectamente, por quedar esto fuera del ámbito de comprensión del niño y, por tanto, exceder de los límites de tratamiento lícito.

El grupo de trabajo comparte las preocupaciones expresadas por la Comisión Federal de Comercio en su informe sobre las aplicaciones móviles para niños[49].

Los desarrolladores de aplicaciones, en colaboración con las tiendas de aplicaciones y los fabricantes de sistemas operativos y dispositivos, deben presentar la información pertinente de manera sencilla y con un lenguaje propio de las edades en cuestión. Asimismo, los responsables del tratamiento de datos deben abstenerse específicamente de toda recogida de datos sobre los padres o familiares del niño usuario, como información financiera o de categorías especiales de información como los datos médicos.

4 Conclusiones y recomendaciones

Gran parte de los tipos de datos disponibles en un dispositivo móvil inteligente son de carácter personal. El marco jurídico pertinente es la Directiva sobre protección de datos, en combinación con el requisito del consentimiento específico contenido en el artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica. Estas normas se aplican a las aplicaciones destinadas a usuarios dentro de la UE, independientemente del lugar de establecimiento de los desarrolladores o la tienda de las aplicaciones.

---

47 Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas), de 11 de febrero de 2009 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_es.pdf).

48 En los Estados miembros de la UE los límites de edad van de los 12 a los 18 años.

49 Informe de la FTC «*Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*» de febrero de 2012 (http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf): «Aunque los servicios de la FTC encontraron un amplio abanico de aplicaciones para niños, creadas por cientos de desarrolladores, hallaron escasa, o ninguna, información en las tiendas de aplicaciones sobre las prácticas de recogida y distribución de datos de esas aplicaciones.».

El carácter fragmentario del ecosistema de las aplicaciones, la amplia gama de posibilidades técnicas de acceso a los datos conservados o generados en dispositivos móviles y la falta de concienciación jurídica entre los desarrolladores crean una serie de riesgos graves para la protección de los datos de los usuarios de aplicaciones. Estos riesgos van desde la falta de transparencia y de sensibilización de los usuarios de aplicaciones hasta medidas de seguridad insuficientes, mecanismos de consentimiento inválidos, una tendencia a maximizar los datos y la elasticidad de los fines del tratamiento.

Existe un solapamiento de responsabilidades en la protección de datos entre las diferentes partes que participan en el desarrollo, la distribución y la capacidad técnica de las aplicaciones. La mayoría de las conclusiones y recomendaciones se dirigen a los desarrolladores de aplicaciones (ellos son los que mayor control tienen sobre la forma precisa en que se realiza el tratamiento o en que se presenta la información dentro de la aplicación), pero, para alcanzar el máximo nivel de protección de la intimidad y protección de datos, deben colaborar con otras partes del ecosistema de las aplicaciones, como los fabricantes de sistemas operativos y dispositivos, las tiendas de aplicaciones y terceras partes como los proveedores de análisis y las redes publicitarias.

Los desarrolladores de aplicaciones deben:

- Conocer y cumplir sus obligaciones como responsables del tratamiento de datos cuando procesen datos a partir de usuarios y sobre ellos.
- Conocer y cumplir sus obligaciones como responsables del tratamiento de los datos cuando realicen contratos con encargados de tratamientos de datos, así como cuando externalizan la recogida y el tratamiento de datos personales a desarrolladores, programadores y, por ejemplo, proveedores de almacenamiento en nube.
- Solicitar el consentimiento antes de que las aplicaciones comiencen a recoger información del dispositivo o instalarla en el mismo, es decir, antes de instalar la aplicación. Dicho consentimiento debe ser libre, específico e informado.
- Solicitar el consentimiento diferenciado o «granular» para cada tipo de datos a que accederá la aplicación, es decir, al menos para las categorías siguientes: localización, contactos, identificador único del dispositivo, identidad del interesado, identidad del teléfono, datos de la tarjeta de crédito y de pago, historial de telefonía y SMS, historial de navegación, correo electrónico, credenciales de redes sociales y biometría.
- Ser conscientes de que el consentimiento no legitima el tratamiento de datos excesivo o desproporcionado.
- Informar sobre los fines del tratamiento de datos, que deben estar bien definidos y ser comprensibles, antes de instalar la aplicación, y no cambiar esos fines sin renovar la autorización; facilitar información completa si los datos van a utilizarse para fines relacionados con terceras partes (como publicidad o análisis).
- Permitir a los usuarios revocar la autorización y desinstalar la aplicación, y, en su caso, suprimir los datos.
- Respetar el principio de minimización de datos y recoger solo los datos estrictamente necesarios para realizar la función deseada.
- Tomar las medidas técnicas y organizativas necesarias para garantizar la protección de los datos personales que tratan, en todas las fases del diseño y la puesta en práctica de la aplicación (privacidad desde el diseño), como se indica en el apartado 3.6 del presente dictamen.
- Ofrecer un punto de contacto único a los usuarios de la aplicación.

- Proporcionar una política de privacidad legible, comprensible y fácilmente accesible, que informe a los consumidores, como mínimo, sobre:
  - quiénes son (identidad y datos de contacto)
  - qué categorías precisas de datos personales recopilará y tratará la aplicación
  - por qué es necesario el tratamiento de datos (para qué objetivos precisos)
  - si los datos se comunicarán a terceros (dando no una mera descripción genérica, sino una descripción concreta de a quiénes se comunicarán los datos)
  - qué derechos tienen los usuarios para retirar el consentimiento y suprimir los datos.
- Permitir a los usuarios de aplicaciones ejercer sus derechos de acceso, rectificación, supresión y oposición al tratamiento de los datos, e informarles de la existencia de dichos mecanismos.
- Definir un periodo razonable de conservación de los datos recabados con la aplicación y fijar previamente un periodo de inactividad tras el cual la cuenta se considerará expirada.
- Por lo que se refiere a las aplicaciones destinadas a niños: prestar atención al límite de edad que define a los niños o los menores de edad en las legislaciones nacionales; escoger el enfoque más restrictivo del tratamiento de datos respetando íntegramente los principios de la minimización de datos y de limitación de la finalidad; abstenerse de tratar datos de niños para fines de publicidad comportamental, directa o indirectamente; y abstenerse de recoger a través de los niños datos de sus familiares o amigos.

El grupo de trabajo recomienda a los desarrolladores de aplicaciones:

- Estudiar las directrices pertinentes sobre los riesgos y medidas de seguridad específicos.
- Trabajar activamente para informar a los usuarios sobre las violaciones de datos personales conforme a los requisitos de la Directiva sobre la privacidad electrónica.
- Informar a los usuarios sobre sus 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 y la aplicación de las medidas de protección.
- Elaborar herramientas para que los usuarios puedan adaptar sus periodos de conservación de datos personales en función de contextos y preferencias específicas en lugar de ofrecer plazos de conservación preestablecidos.
- Incluir en su política de privacidad información destinada a los usuarios europeos.
- Elaborar y aplicar herramientas de acceso en línea sencillas y seguras para los usuarios, sin recoger datos personales adicionales en exceso.
- Utilizar, en colaboración con los desarrolladores de aplicaciones y las tiendas de aplicaciones, su talento creativo para desarrollar soluciones innovadoras para informar adecuadamente a los usuarios de dispositivos móviles, por ejemplo mediante un sistema de anuncios informativos estratificados combinado con iconos significativos.

Las tiendas de aplicaciones deben:

- Conocer y cumplir sus obligaciones como responsables del tratamiento de datos cuando procesen datos a partir de usuarios y sobre ellos.
- Hacer cumplir la obligación de los desarrolladores de aplicaciones de informar, incluyendo los tipos de datos a que la aplicación puede acceder y con qué fines, y si los datos se intercambian con terceros.
- Prestar especial atención a las aplicaciones dirigidas a los niños para protegerles contra el tratamiento ilícito de sus datos y, en particular, hacer cumplir la información pertinente de manera sencilla y con un lenguaje propio de las edades en cuestión.
- Informar en detalle sobre los controles que realizan de las solicitudes de la aplicación, incluidos los destinados a evaluar cuestiones de protección de datos y de la intimidad.

El grupo de trabajo recomienda a las tiendas de aplicaciones:

- Elaborar, en colaboración con los fabricantes de sistemas operativos y dispositivos, herramientas de control para los usuarios, como símbolos que representen el acceso a los datos del dispositivo móvil o generados por el mismo.
- Someter todas las aplicaciones a un mecanismo de evaluación pública.
- Aplicar un mecanismo de desinstalación a distancia respetuoso de la intimidad.
- Proporcionar a los usuarios canales de retroalimentación para notificar problemas de intimidad y/o seguridad.
- Colaborar con los desarrolladores de aplicaciones para informar activamente a los usuarios sobre las violaciones de datos personales.
- Advertir a los desarrolladores de aplicaciones sobre las especificidades de la legislación europea antes de presentar la aplicación en Europa como, por ejemplo, el requisito del consentimiento y en caso de transferencia de datos personales a terceros países.

Los fabricantes de sistemas operativos y dispositivos deben:

- Actualizar sus API, normas de almacenamiento e interfaces de usuario para ofrecer a los usuarios un control suficiente para dar un consentimiento válido en cuanto a los datos tratados por las aplicaciones.
- Aplicar mecanismos de consentimiento a la recogida de datos en sus sistemas operativos al lanzar por primera vez la aplicación o la primera vez que la aplicación trata de acceder a una de las categorías de datos con repercusiones significativas para la intimidad.
- Emplear los principios de privacidad desde el diseño para evitar el seguimiento secreto de los usuarios.
- Garantizar la seguridad del tratamiento.
- Garantizar que (los parámetros por defecto de) las aplicaciones preinstaladas son conformes con la normativa europea de protección de datos.
- Ofrecer acceso granular a los datos, los sensores y los servicios, a fin de garantizar que los desarrolladores de aplicaciones pueden acceder solo a los datos necesarios para su aplicación.
- Ofrecer medios eficaces y de uso sencillo para evitar ser objeto de seguimiento por parte de anunciantes y otras terceras partes. Los parámetros por defecto deben imposibilitar todo seguimiento.
- Garantizar la disponibilidad de mecanismos apropiados que permitan informar y educar al usuario final sobre lo que pueden hacer las aplicaciones y los datos a que pueden acceder.
- Garantizar que todo acceso a una categoría de datos se refleja en la información del usuario antes de instalar la aplicación: las categorías presentadas deben ser claras y comprensibles.
- Aplicar un entorno favorable a la seguridad, con herramientas que eviten la propagación de aplicaciones maliciosas y permitan la instalación y desinstalación sencilla de cada función.

El grupo de trabajo recomienda a los fabricantes de sistemas operativos y dispositivos:

- Permitir a los usuarios desinstalar las aplicaciones y enviar una señal (por ejemplo, mediante la API) a los desarrolladores de aplicaciones para permitir la supresión de los datos de usuario pertinentes.
- Ofrecer y facilitar sistemáticamente actualizaciones periódicas de seguridad.
- Garantizar que los métodos y las funciones que permiten acceder a los datos personales incluyen medidas para aplicar el consentimiento granular.

- Colaborar activamente para desarrollar y facilitar iconos que alerten a los usuarios del uso de los distintos datos por las aplicaciones.
- Desarrollar rastros de auditoría claros en los dispositivos de forma que los usuarios finales puedan ver claramente qué aplicaciones han accedido a los datos de sus dispositivos y los flujos del tráfico saliente por aplicación en relación con el tráfico iniciado por el usuario.

Las terceras partes deben:

- Conocer y cumplir sus obligaciones como responsables del tratamiento de datos cuando procesen datos personales sobre usuarios.
- Cumplir el requisito del consentimiento de conformidad con el artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica cuando lean o inscriban datos en los dispositivos móviles en cooperación con los desarrolladores de aplicaciones y/o las tiendas de aplicaciones, esencialmente informando al usuario sobre los fines del tratamiento de datos.
- No eludir los mecanismos diseñados para evitar el seguimiento, como suele ocurrir actualmente con los mecanismos «Evitar seguimiento» aplicados en los navegadores.
- Los proveedores de servicios de comunicaciones, cuando emiten productos de marca, deben garantizar el consentimiento válido de los usuarios de aplicaciones preinstaladas y asumir las responsabilidades correspondientes al contribuir a determinar ciertas características del dispositivo y del sistema operativo, por ejemplo, al limitar el acceso del usuario a determinados parámetros de configuración o al filtrar los lanzamientos de reparación (de seguridad y funcionales) facilitados por los fabricantes de sistemas operativos y dispositivos.
- Las partes relacionadas con la publicidad deben evitar específicamente lanzar anuncios fuera del contexto de la aplicación, como, por ejemplo, los anuncios lanzados mediante la modificación de los parámetros del navegador o la colocación de iconos en el escritorio del dispositivo móvil; y abstenerse de recurrir a los identificadores únicos o de abonado a efectos de seguimiento.
- Abstenerse de tratar datos de niños para fines de publicidad comportamental, directa o indirectamente; y aplicar medidas de seguridad adecuadas. Esto incluye la transmisión segura y el almacenamiento cifrado de los identificadores únicos de dispositivo y de usuario, y otros datos personales.

El grupo de trabajo recomienda a las terceras partes:

- Elaborar y aplicar herramientas de acceso en línea sencillas y seguras para los usuarios, sin recoger datos personales adicionales en exceso.
- Recoger y procesar solo datos que sean coherentes con el contexto en que el usuario debe proporcionarlos.