EL DEBER DE INFORMAR Y OTRAS MEDIDAS DE RESPONSABILIDAD PROACTIVA EN APPS PARA DISPOSITIVOS MÓVILES

I. INTRODUCCIÓN

Esta nota técnica está orientada a las entidades involucradas en el desarrollo, distribución y explotación de apps para dispositivos móviles, en particular a aquellas que desempeñen el rol de responsables de tratamiento o corresponsable en cada una de sus áreas de competencia, así como otros agentes que intervienen en el ecosistema de apps para dispositivos móviles, como pueden ser, entre otros, desarrolladores de aplicaciones y desarrolladores de librerías.

De forma general, la Agencia Española de Protección de Datos (AEPD) tienen diversos recursos publicados para orientar en el cumplimiento de las obligaciones en materia de protección de datos como son la "Guía para el cumplimiento del deber de informar", el "Decálogo para la adaptación al RGPD de las políticas de privacidad en internet", la "Guía del RGPD para responsables de tratamiento" y las "Directrices para elaborar contratos entre responsables y encargados de tratamiento". El entonces Grupo del Artículo 29 publicó también un "Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes". La presente nota técnica viene a ampliar y completar estos recursos estableciendo unas directrices específicas en el caso de las apps para dispositivos móviles, desarrollando algunos aspectos específicos con relación al deber de informar y otras medidas de responsabilidad proactiva.

Estas directrices se obtienen a partir de las conclusiones de los trabajos llevados a cabo en un marco de colaboración entre la Universidad Politécnica de Madrid (UPM) y la AEPD sobre apps para dispositivos móviles en los ámbitos educativo y de bienestar, que se describen en el Anexo I.

II. DIRECTRICES ESPECÍFICAS PARA APPS PARA DISPOSITIVOS MÓVILES

En cuanto al deber de información, del análisis de las apps para dispositivos móviles estudiadas se concluye que hay ciertos aspectos de cumplimiento que requieren de una especial atención por parte de los responsables de tratamiento:

1. La información proporcionada a los usuarios sobre el tratamiento de sus datos personales debe cumplir los requisitos establecidos en los artículos 13 y 14 del RGPD y el artículo 11 de la LOPDGDD, en particular con respecto a la información por capas, en los términos señalados en la "Guía para el cumplimiento del deber de informar" y el "Decálogo para la adaptación al RGPD de las políticas de privacidad en internet".
2. Dicha información, en forma de política de privacidad, debe estar disponible tanto en la propia aplicación como en la tienda de aplicaciones. De esta forma, el usuario podrá consultarla antes de instalar la aplicación o en cualquier momento durante su uso.
3. El acceso a la política de privacidad debe poder hacerse de forma sencilla desde la aplicación, y requerir del usuario un número de interacciones

reducido, a ser posible a un máximo de dos clics como recomienda el GT29 en sus directrices sobre la transparencia.

4. El responsable de tratamiento tiene que identificarse claramente en la política de privacidad, y en aquellos casos de responsables de tratamiento establecidos fuera de la UE y que ofrecen sus aplicaciones para usuarios en Europa, deben haber designado un representante en la UE e identificarlo igualmente en la política de privacidad.
5. La información sobre el tratamiento debe ser completa y consistente tanto en la tienda de aplicaciones, en su caso, como en la propia aplicación. No puede haber discrepancias entre ambas y por tanto también es aplicable en el caso de aplicaciones preinstaladas en los dispositivos que se comercialicen.
6. El lenguaje en el que se describen las políticas de privacidad debe ser adecuado para el usuario objetivo de la aplicación teniendo en cuenta su edad y su nivel de conocimiento, además, también se tendrá en cuenta el idioma empleado, por ejemplo, aplicaciones disponibles en castellano y destinadas por tanto a usuarios hispanohablantes, deben proporcionar la política de privacidad en castellano sin perjuicio de que pueda mostrarse en otros idiomas. Estos aspectos son especialmente relevantes en el caso de aplicaciones destinadas a menores.
7. Las políticas de privacidad deben ser concretas y específicas sobre el tratamiento de datos personales que se lleva a cabo. Para evitar la "fatiga informativa" se debe evitar proporcionar información de carácter genérico, no específica de la aplicación. La política de privacidad ha de evitar, por ejemplo, describir un conjunto de aplicaciones u otros servicios de la organización como su página web.
8. En la política de privacidad de la app debe proporcionarse al usuario toda la información sobre el tratamiento de los datos personales que pretende realizar, información precisa sobre qué datos y tratamientos son necesarios para el funcionamiento básico de la aplicación, cuáles son opcionales, y toda la información adicional relevante del tratamiento que se va a realizar con los datos. Además, en la política de privacidad, se deberían indicar los permisos que puede solicitar la aplicación (directamente o a través de bibliotecas de terceros) para el acceso a datos y recursos, para qué tratamientos y finalidad se solicitan esos permisos y con qué extensión (lectura, escritura, …). Por ejemplo, ha de informar si la aplicación tratará los datos únicamente cuando se está ejecutando por acción del usuario en primer plano o necesita acceder también cuando se ejecuta en segundo plano. También se debe facilitar al usuario información relativa a la forma en la que puede gestionar los permisos otorgados a la aplicación de manera que pueda decidir en todo momento si decide otorgar o revocar dichos permisos, o en qué condiciones los otorga.
9. Cuando la legitimación para el tratamiento de los datos personales a través de la app sea el consentimiento, dicho consentimiento tiene que solicitarse de forma granular, es decir, de forma selectiva e independiente para los distintos tratamientos y finalidades. La instalación y utilización de la app no puede estar condicionada a la obtención de un consentimiento para un tratamiento no necesario para proporcionar el servicio definido en la misma.
10. No hay que utilizar cláusulas ambiguas o vacías como, por ejemplo, "cualquier dato puede ser recolectado o difundido, o retenido indefinidamente" o "recopilamos sus datos con el fin de mejorar su experiencia de usuario".

11. Hay que incluir información concreta sobre los periodos de retención de los datos y el destino final de los mismos finalizados dichos periodos.
12. En el mismo sentido, hay que incluir información concreta relativa a la lógica aplicada en la elaboración de perfiles y toma de decisiones automatizadas, o un enlace para consultar dicha información, como la utilizada para personalizar los anuncios.
13. La definición de las finalidades del tratamiento y sus bases legales ha de ser clara y precisa, así como los datos personales que se recopilan para cada una de esas finalidades.
14. No hay que olvidar el proporcionar a los usuarios información sobre sus derechos en materia de protección de datos y proporcionar mecanismos y procedimientos para ejercerlos de forma efectiva.
15. En su caso, hay que informar de la existencia de transferencias internacionales de datos de forma concreta y específica.

Los responsables de tratamiento que encarguen el desarrollo, puesta en producción y/o explotación de aplicaciones a terceras partes con acceso a datos personales, deben asegurarse de cumplir los requisitos establecidos en el RGPD para cada una de las partes. Para estos casos son particularmente útiles la "Guía del RGPD para responsables de tratamiento" y "Directrices para elaborar contratos entre responsables y encargados de tratamiento".

Cabe destacar los siguientes requisitos:

16. El tratamiento debe estar regulado por un contrato o vínculo legal que establezca el objeto, la duración, la naturaleza, la finalidad del tratamiento, el tipo de datos personales, las categorías de interesados, y las obligaciones y derechos del responsable.
17. En el contrato de encargo se estipulará específicamente que el encargado tratará los datos personales únicamente siguiendo las instrucciones documentadas del responsable, por lo que el encargado de tratamiento no debe introducir en la aplicación otros tratamientos de datos personales que el responsable pueda desconocer, como aquellos que se pueden introducir al incluir en la aplicación librerías de terceras partes con fines publicitarios, analíticas, u otros.
18. El contrato de encargo estipulará que el encargado de tratamiento tomará las medidas indicadas por el responsable relativas a la seguridad del tratamiento, incluyendo específicamente buenas prácticas de desarrollo y teniendo en cuenta la privacidad desde el diseño y por defecto desde la concepción misma de la aplicación.

En particular, se deben tener en cuenta con especial consideración las siguientes prácticas:

19. Proporcionar granularidad en la gestión de permisos de acceso a recursos protegidos del sistema de acuerdo con lo establecido en la política de privacidad. Un ejemplo es limitar los permisos de acceso a un recurso, como podría ser la carpeta de imágenes en lugar de otorgar un permiso genérico de acceso al almacenamiento del dispositivo.

20. Respetar las preferencias del usuario en cuanto a privacidad, por ejemplo, en cuanto a la personalización de anuncios, evitando, en su caso, el acceso incluso a identificadores de publicidad.
21. Evitar el acceso a identificadores globales únicos junto al identificador de publicidad del dispositivo, lo que permitiría hacer asignaciones que permiten dejar sin efecto medidas de protección del usuario como cambiar su identificador de publicidad.
22. Evitar la difusión de datos personales hacia servicios de analítica y publicidad desde el mismo momento en que se inicia la aplicación, sin que el usuario mismo haya podido hacer ningún uso o ajuste.
23. Comprobar que no hay difusión de datos personales sin conocimiento del responsable de tratamiento, al tratarse de comunicaciones iniciadas desde librerías de terceros utilizadas por el desarrollador para ampliar la funcionalidad de la aplicación o rentabilizarla económicamente.
24. Evitar la cesión de datos personales hacia destinatarios no especificados o informados en la política de privacidad, que tengan el rol de responsables de tratamiento o corresponsables.
25. Evitar transferencias internacionales de datos no declaradas en la política de privacidad.
26. Utilizar métodos avanzados para el cifrado de las comunicaciones (ej: *certificate-pinning*[1]) supone una garantía adicional para la privacidad de los usuarios a considerar dependiendo de las características del tratamiento de datos.

III. CONCLUSIONES

La transparencia en el tratamiento de datos personales por parte de las apps para dispositivos móviles es un aspecto capital para el cumplimiento la normativa de protección de datos, es decir, para la protección de los derechos y libertades de los ciudadanos.

La AEPD ha puesto a disposición de los responsables de tratamiento dos recursos para facilitar a los responsables el cumplimiento de los requisitos de transparencia e información del RGPD, uno genérico como es la "Guía para el cumplimiento del deber de informar" y uno específica para aplicaciones en Internet: el "Decálogo para la adaptación al RGPD de las políticas de privacidad en internet".

La presente nota técnica extiende las guías anteriores y se dirige a atender aspectos específicos del entorno de apps para dispositivos móviles en los que se ha detectado que es necesario un especial cuidado.

Para ello, hay que subrayar que la información al usuario debe proporcionarse con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible, de fácil acceso y adaptada al interesado o usuario potencial de la aplicación. Es por ello, que se debe tener muy en cuenta el público al cual va dirigida la aplicación para elaborar las cláusulas informativas de la política de privacidad.

Ciertos sensores y almacenes de datos del terminal móvil son una fuente potencial de datos personales a las que pueden acceder las aplicaciones o bibliotecas de terceros

[1]Técnica para prevenir la intercepción de comunicaciones cifradas mediante ataques MITM: Certificate Pinning Symantec

incluidas en las aplicaciones. El sistema operativo del dispositivo móvil protege los accesos a estos recursos a través de permisos con diferentes niveles de protección.

Si bien el dispositivo muestra al usuario una notificación solicitando su autorización para acceder a dichos recursos, en muchos casos, la información mostrada no es suficiente en el contexto del RGPD, ni la granularidad del permiso se precisa de forma correcta, ya que, entre otra información, debe incluir la finalidad del tratamiento de esos datos. La necesidad de acceder a dichos recursos debe informarse apropiadamente en la política de privacidad de la aplicación, para que el usuario pueda decidir la conveniencia o no de otorgar autorización a la aplicación para acceder a dichos recursos.

En segundo lugar, se desarrollan también directrices para responsables de tratamiento que encarguen el desarrollo, puesta en producción y/o explotación de aplicaciones a terceras partes, con acceso a datos personales, deben asegurarse de cumplir los requisitos establecidos en el RGPD para cada una de las partes. Estas directrices vienen a complementar la "Guía del RGPD para responsables de tratamiento" y "Directrices para elaborar contratos entre responsables y encargados de tratamiento". El responsable de tratamiento debe asegurarse de cumplir con todos los requisitos de responsabilidad activa recogidos en el RGPD, asegurándose además que el encargado de tratamiento únicamente trata los datos de acuerdo con sus instrucciones y tomando medidas para asegurarse de que así sea.

ANEXO I: ORIGEN Y METODOLOGÍA

Esta nota técnica se ha desarrollado en el marco los trabajos sobre privacidad y protección de datos en el marco del Plan Estratégico de la Agencia Española de Protección de Datos para el periodo 2015-2019. El primero orientado a los tratamientos de datos personales que se llevan a cabo en apps para dispositivos móviles de uso en entornos de educación obligatoria, mientras que el segundo se focaliza en apps para dispositivos móviles para la monitorización de la actividad física, el bienestar y la salud. Estos trabajos se han realizado por la Universidad Politécnica de Madrid, bajo la dirección y coordinación de esta Agencia.

El Plan Estratégico de la Agencia Española de Protección de datos 2015-2019 fija en su eje estratégico número 2 “Innovación y protección de datos: factor de confianza y garantía de calidad” una línea de actuación por la que se crea la Unidad de Evaluación y Estudios Tecnológicos, entre cuyos objetivos se encuentra la elaboración de estudios e informes sobre iniciativas y proyectos de carácter tecnológico (punto 2.5 del mencionado plan).

En este sentido la AEPD se plantea la necesidad de llevar a cabo una labor proactiva entre los responsables de productos y servicios en los que se traten datos personales, en especial se plantea la necesidad de llevar a cabo estudios sobre servicios de la denominada sociedad conectada entre los que se encuentran los trabajos objeto de esta memoria, en los que los datos utilizados son especialmente sensibles por el sujeto fuente, ya que se trata de menores en el estudio dirigido a las aplicaciones de uso en entorno de educación obligatoria y, de otra parte, por la naturaleza de los datos ya que en el estudio sobre aplicaciones para la monitorización de la actividad física se trata de datos con un enfoque próximo al de la salud.

Al mismo tiempo se pretende fomentar la colaboración entre esta Agencia y el entorno universitario-investigador para promover la investigación técnica orientada a fomentar la privacidad y protección de datos.

Los trabajos han supuesto la realización de tareas de investigación técnicas destinadas a:

- Detectar flujos de información en apps para dispositivos móviles en general,
- Diseño de procedimientos estándar que permitan realizar evaluaciones de privacidad en aplicaciones de forma sistemática, ordenada y comparable,
- Evaluación de un subconjunto representativo de aplicaciones de utilidad en el entorno educativo y relativas a salud y bienestar,
- Evaluación de políticas de privacidad de aplicaciones respecto al decálogo de adaptación al RGPD publicado por la Agencia.

El objetivo último es detectar aquellas prácticas más lesivas con la privacidad de los usuarios de ambos grupos de aplicaciones, a fin de aportar soluciones o alternativas para desarrolladores, promotores y usuarios de dichas aplicaciones.

En este informe pretende destacar las principales conclusiones obtenidas a partir de ambos estudios, conclusiones que bien podrían hacerse extensivas a otros tipos de apps para dispositivos móviles.

En el marco de estos trabajos se han analizado un total de 20 apps para dispositivos móviles para terminales Android, 10 aplicaciones de cada uno de los dominios de interés, educación y bienestar.

Los criterios aplicados para la selección de las aplicaciones han sido:

- Aplicaciones con mayor número de descargas en Play Store de Google dentro de cada uno de los dominios de estudio, destinadas a público en español.
- Asegurar distribución homogénea de aplicaciones desarrolladas y publicadas por pequeños desarrolladores, pero que tienen gran acogida entre los usuarios, y aplicaciones desarrolladas y publicadas por grandes tecnológicas.
- Asegurar una distribución homogénea entre aplicaciones de pago y aplicaciones gratuitas.

En el caso de aplicaciones de monitorización de actividad física que funcionen con un dispositivo externo tipo pulsera de actividad, se realizó el análisis de la aplicación conectada a la pulsera de actividad.

La metodología de estos trabajos incluye un análisis técnico de los flujos de información de cada aplicación empleando técnicas de análisis estático y dinámico en contraste con un análisis de las políticas de privacidad de la aplicación. Por tanto, para cada aplicación se ha realizado un doble análisis, por un lado, se contrastan las políticas de privacidad de cada aplicación con el decálogo de políticas de privacidad publicado por la Agencia, y por otro lado se contrastan las discrepancias que pueden aparecer entre lo declarado en las políticas de privacidad y lo observado en el análisis estático y dinámico.