La protección de datos en las aplicaciones de los dispositivos inteligentes

Juan José Marín López
Catedrático de Derecho Civil de la Universidad de Castilla-La Mancha
Consejero Académico de Gómez-Acebo & Pombo

El Grupo del 29 ha publicado su Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, adoptado el 27 de febrero de 2013 (00461/13/ES; WP 202). El Dictamen finaliza con unas conclusiones muy detalladas y recomendaciones dirigidas tanto a los fabricantes de las aplicaciones, comúnmente conocidos como desarrolladores, a los vendedores o distribuidores de las mismas y a los fabricantes de los sistemas operativos y los dispositivos en los que se descargan esas aplicaciones. El Grupo advierte que 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 (abreviatura inglesa de interfaces de programación de aplicaciones), 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.