

Apps para móviles: ¿somos conscientes de los datos personales que manejan y con qué fin?

"Las apps que más datos recopilan son Facebook e Instagram"



(Foto: E&J)

En la actualidad, prácticamente todas las empresas tratan a diario, datos de carácter personal; de tal manera que, la actividad propia de toda compañía exige la utilización y el tratamiento de **datos personales** (desde la información de sus empleados, hasta la de sus propios clientes y proveedores).

Lo anterior determina la necesidad ineludible de adecuar, adaptar y revisar el funcionamiento de la empresa en cuestión, a la normativa vigente en materia de protección de datos.

Esa última, como bien es sabido, consiste en el conjunto de **medidas** para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de esos datos por los sectores público y privado. Ello, a los efectos de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

El Reglamento Europeo (UE) 2016/679 del Parlamento Europeo y del Consejo, de 17 de abril de 2016, de Protección de Datos Personales y la Ley Orgánica 3/2018 de 5 de diciembre, de **Protección de Datos** Personales y garantía de los derechos digitales, conforman, entre otros textos normativos, el marco de las obligaciones que debe cumplir cualquier empresa o profesional que trate datos de carácter personal en el desempeño de su actividad profesional.

Para la debida y oportuna protección de datos, la **Agencia Española de Protección de Datos**, establece una serie de principios: información al interesado, calidad de los datos, consentimiento del interesado, datos especialmente protegidos, deber de secreto, seguridad de los datos, datos relativos a la salud, comunicación de datos. Y acceso a los datos por cuenta de terceros.



Sede de la Agencia Española de Protección de Datos. (Foto: AEPD)

Pues bien, quería centrarme en esta tribuna, en un ámbito omnipresente en nuestro día a día: **las aplicaciones de los dispositivos móviles que utilizamos** y la necesaria protección de datos que, las compañías del sector están obligadas a llevar a cabo.

Es evidente que, cuando instalamos una determinada app (aplicación informática diseñada para ser ejecutada en teléfonos inteligentes y tablets), vamos a ceder datos de carácter personal, por ello, las citadas compañías deben ocuparse en el momento de la descarga e instalación en nuestro dispositivo móvil de lo siguiente: recabar el **consentimiento** informado y previo del cliente; indicar el propósito para el que se recoge la información; e informar a los clientes de los **derechos y plazos de conservación** de sus datos.

La mayoría de aplicaciones, sin embargo, ofrecen **muy poca información** de por qué recopilan datos de naturaleza personal y para qué la utilizan, o no han adaptado la política de protección de datos para ser leídas en pequeña pantalla, e incluyen **extensas políticas** que obligan a desplazar el texto o a hacer “clic” en varias páginas; lo que al final acaba provocando que el usuario por defecto, **acepte todo cuanto se le plantea**. Y lo que es peor: en prácticamente la totalidad de ocasiones, para poder usar la aplicación, no habrá más opción que conceder los permisos solicitados. **Son cláusulas de adhesión**, donde no admiten la aclaración o reserva del usuario. En términos generales, son confusas, tediosas, **de letra pequeña** y de muy difícil lectura.

Resulta que los datos personales que más recaban y guardan las apps de nosotros son la edad, el sexo, la orientación sexual, la raza, la ubicación, la dirección del domicilio, el número de teléfono móvil, el número de teléfono fijo, el tipo de dispositivo, los datos bancarios, el idioma y los contactos.

Debemos prestar especial atención y cuidado al descargar y utilizar aplicaciones móviles

Y me asalta, entonces, la siguiente cuestión: **¿para qué recopilan estos datos las aplicaciones?** Pues algunas de ellas necesitan dicha información para funcionar: pensemos en un comercio electrónico que precisa de nuestros datos bancarios para proceder al pago; o en las aplicaciones de **TikTok** o **Instagram**, que necesitan acceder a la cámara e incluso galería del móvil para tomar fotos o hacer videos y subirlos a sendas plataformas. **¿Pero es necesario que la aplicación de la calculadora tenga que acceder a nuestros contactos?**, ¿o que al descargar una app de linterna nos solicite acceder a la galería de fotos? Evidentemente no.

Más allá de los datos que necesitan para funcionar de manera correcta, la gran mayoría de las aplicaciones utilizan la **información personal** que recaban de los clientes para crear perfiles de los usuarios y **ofrecerles publicidad personalizada** e incluso para otras finalidades completamente desconocidas.

Es curioso que sean gratuitas. ¿Imaginamos la ingente riqueza que cosecharía, WhatsApp, por ejemplo, simplemente con un 1 euro/mes por usuario? ¿Y quién no pagaría dicho importe con la dependencia que todos tenemos hacia dicha aplicación? Claro está, que quieren datos, información, no dinero de los usuarios.

Pensemos, por ejemplo, cuando nos encontramos inmersos en una red social y **nos aparecen anuncios de artículos que hemos buscado o queremos comprar** (o incluso, en atención simplemente a lo que hemos conversado, pues la mayoría también tienen acceso al micrófono).

Precisamente las dos aplicaciones que más datos recopilan son **Facebook** e **Instagram** (en torno al 70%), frente a **YouTube** o **WhatsApp** (sobre el 20%). Y son las dos primeras las que mayor cantidad de publicidad inserta también en sus propias aplicaciones, que es personalizada sobre nuestros intereses personales.



«Esa información sobre el tratamiento de datos debe encontrarse disponible para el usuario antes de instalar la aplicación». (Foto: E&J)

Pese a que buena parte de los usuarios son conscientes de las amenazas de seguridad debido al uso de apps y a la cesión de datos que realizamos, es evidente que es necesaria una mayor concienciación sobre los peligros y para ello, **es ineludible proporcionar más información a los ciudadanos acerca de los derechos que les asisten** en este ámbito y que suelen ser conculcados de forma flagrante en buena parte de las ocasiones.

Así, por ejemplo, el usuario tiene derecho a ser informado de la identidad del encargado del tratamiento de sus datos personales en la concreta aplicación, de qué tipo de datos están siendo tratados y con qué finalidad.

El responsable del tratamiento correspondiente deberá comunicar a los usuarios potenciales, como mínimo: quiénes son (identidad y datos de contacto); las categorías concretas de datos personales que el desarrollador solicitará y tratará; los objetivos precisos de ese tratamiento; si los datos se comunicarán a terceros; y los medios que tienen los usuarios para ejercer sus derechos.

Esa información sobre el tratamiento de datos debe encontrarse **disponible** para el usuario antes de instalar la aplicación y debe ser accesible desde dentro de la aplicación, una vez instalada.

Dicho lo anterior, es cierto que, en ocasiones, en muchas aplicaciones, **la publicidad acaba siendo invasiva en nuestros terminales, y el ciudadano se encuentra indefenso** sobre el modo de hacer efectivo su deseo de no recibir más publicidad y/o de ejercer sus derechos de acceso y rectificación.

En definitiva, debemos prestar especial atención y cuidado al descargar y utilizar aplicaciones móviles, y especialmente, con la cesión de datos de carácter personal que realizamos y los consentimientos que prestamos para que accedan a nuestra información personal: **la publicidad mueve miles de millones de euros**, y disponer de perfiles individualizados hace que la mayoría de las aplicaciones recaben el mayor número de datos posible de sus usuarios para sí mismos o para su cesión.

Y, aunque la actual normativa permite luchar contra las actuaciones publicitarias que no respeten los necesarios ámbitos de privacidad, existe aún, en el **Derecho Administrativo**, una importante ausencia de control efectivo de los problemas que dicha publicidad sin límites acarrea, así como la utilización de los datos personales que se recaban de forma masiva, incontrolada e indiscriminada.



TEMAS RELACIONADOS: #APLICACIÓN #APP #CONSENTIMIENTO #DATOS PERSONALES #FACEBOOK #INSTAGRAM #PRIVACIDAD #PUBLICIDAD #WHATSAPP #YOUTUBE ¿Asesinato u homicidio imprudente?: el caso de un hijo que atropelló a su padre tras una discusión en un bar de Ciudad Real El Supremo establece que la custodia compartida se puede acordar solo si la solicitan las partes Las hijas de un abogado fallecido pagarán por las difamaciones de su padre a un fiscal (vendercoche.es)

Recomendado por

