Obra Social "la Caixa"

eduCaixa

Bloque 3 • Las *apps* que usamos

Unidad 2 • Píldora 3

PROTEGIENDO MIS DATOS: CÓMO MANTENER A RAYA A LAS *APPS*

BIGDATA

LA INTELIGENCIA DE LOS DATOS

PROTEGIENDO MIS DATOS: CÓMO MANTENER A RAYA A LAS APPS

Las *apps* están **obligadas a cumplir con la normativa de *cookies* y avisar al usuario**. Por otro lado, las *apps* también tienen que avisar, en las políticas de privacidad, de que esos datos pueden cederse, dando la opción al usuario de no prestarlos para esa finalidad en concreto, ya que es secundaria a la función que ofrece la *app*. En el caso de que las cookies sean estrictamente necesarias para prestar el servicio solicitado por el usuario, no tendrán por qué pedir su consentimiento, aunque sí deberá figurar el uso de estas *cookies* en el aviso legal de la *app*.

Es cierto que la gran mayoría de las aplicaciones van a utilizar los permisos de acceso que les otorgamos para una finalidad legítima y no van a hacer un uso indebido de la información que puedan manejar. Además, las aplicaciones que podemos encontrar en las tiendas de *apps* han sido revisadas y validadas desde el punto de vista de la seguridad.

Pero también es cierto que en el mercado pueden "colarse" *apps* poco fiables, que pueden hacer un mal uso de nuestra información. En algunas ocasiones los datos pueden ser destinados a usos adicionales a los previstos para la aplicación, sin que el usuario sea consciente de ello, y normalmente con el objetivo de generar ingresos por otras vías.

Por este motivo, cuando estemos descargando una *app* en nuestro *smartphone* o en nuestra tableta, **es conveniente que prestemos atención al paso en el que se aceptan los permisos de acceso que la aplicación solicita.**

Los propios consumidores facilitan el seguimiento que las *apps* hacen de ellos cuando no prestan atención a las condiciones de uso de los servicios y de las aplicaciones que utilizan. **Es responsabilidad del usuario informarse de las implicaciones que tiene el uso de estos productos**. Pero lo habitual es hacer clic en el botón "Aceptar" sin haberlo hecho, también en el caso de las cada vez más frecuentes aplicaciones de geolocalización a través del *smartphone*.

Si nos descargamos una nueva *app* es recomendable que llevemos a cabo las siguientes comprobaciones:

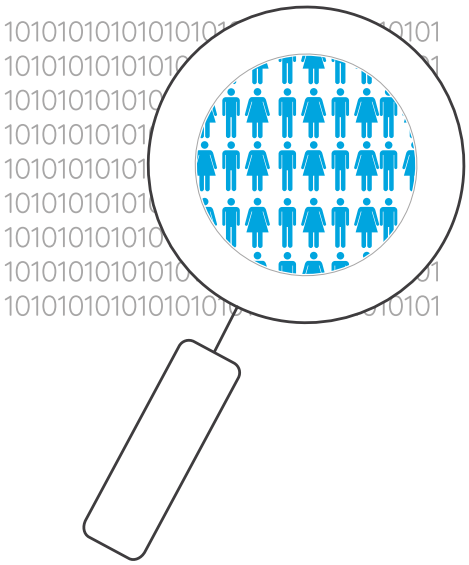
- **Leer atentamente los permisos que solicita la *app***. Verificar los permisos de uso que solicita cada *app*. Acceso a la lista de contactos, agenda, fotos y vídeos, sms, etc. Si no crees que para el funcionamiento sea necesario aceptar tantos permisos, sencillamente desinstala la *app*.

- **Revisar la antigüedad de la *app* en el mercado**. Una simple consulta de su fecha de aparición o del número de descargas que tiene puede resultar muy significativa.

- **Revisar los comentarios y las opiniones de las *apps*.** Echar un vistazo a las opiniones de las personas que ya se la han descargado nos puede dar información muy importante.

MÉTODOS DE CONTROL DE NUESTROS DATOS

En Europa y Estados Unidos ya se han puesto manos a la obra para proteger la intimidad de los usuarios, si es que se pudiera ver comprometida. En España, la Agencia Española de Protección de Datos (AEPD) está examinando las condiciones de privacidad que existen en torno a las aplicaciones móviles más populares conjuntamente con autoridades italianas, inglesas, francesas y alemanas.



Pero se pueden utilizar otros recursos para proteger nuestra privacidad. Hay aplicaciones que sirven para limitar los permisos de uso de otras aplicaciones. Un ejemplo es App Ops, para controlar las aplicaciones Android de un modo fácil y sencillo.

Además de *apps* existen múltiples maneras de controlar la información que cedemos a las *apps*, determinadas por el sistema operativo que tenga nuestro dispositivo móvil. Generalmente se puede gestionar a través del Market Place o los Ajustes del móvil.

CONCLUSIÓN

La conclusión para el Pew Research Center, que ha analizado los datos de la Universidad de Georgetown, es clara: las aplicaciones recopilan demasiada información de los usuarios a partir de una variedad de permisos demasiado amplia.

La protección de la información privada se ha convertido en una preocupación de los usuarios, cada vez más concienciados sobre los perjuicios a los que se verían expuestos si alguien malintencionado accediera a sus datos. El almacenamiento de información puede suponer un riesgo para la privacidad de los usuarios.

Las grandes compañías de diseño de aplicaciones para los dispositivos que tenemos al alcance de la mano durante las 24 horas de los siete días de la semana lo saben casi todo de nosotros: dónde estamos en cada momento, qué estamos haciendo y con quién, en qué gastamos nuestro dinero e incluso dónde nos iremos de vacaciones el próximo verano.

Debemos prestar atención a las condiciones que nos imponen las *apps* y conocer los mecanismos para preservar nuestra intimidad.

Se pueden utilizar los servicios que internet nos ofrece, ya que son muy útiles, pero sabiendo qué obtienen ellos de nosotros a cambio, cuáles son nuestros derechos y qué deben respetar