Publicado en Madrid el 23/01/2020

Panda Security aconseja qué hacer con las apps que no cumplen la ley de protección de datos

Hace unos días Twitter suspendió a la app Grindr de su plataforma publicitaria, porque un estudio de la asociación de consumidores de Noruega indica que la aplicación de citas entre gays no cumple con la normativa de protección de datos

En concreto, el homónimo de la OCU española en Noruega asegura que la plataforma de citas Grindr pasa “cantidades significativas de información privada a anunciantes, sin el consentimiento explícito de los usuarios”, lo cual choca frontalmente con el Reglamento General de Protección de Datos de la Unión Europea (por sus siglas en inglés GDPR).

Poco después de que Twitter vetara de su plataforma publicitaria a Grindr, un portavoz de la compañía que rige la app de citas gay comentó que “la privacidad de sus usuarios, así como la seguridad de sus datos es prioritaria” a lo que añadió que la empresa “está implementando una plataforma de gestión de consentimiento mejorada para proporcionar a sus usuarios un control adicional en la aplicación con respecto a sus datos personales”.

Sin embargo, Grindr no es la única app que fue criticada por ‘la OCU’ noruega. Según su informe, publicado hace unos días, otras dos aplicaciones de citas como Happn, OkCupid y Tinder también podrían estar difundiendo información privada y personal de los usuarios a empresas publicitarias, como sus preferencias sexuales, ciertos datos de comportamiento y la ubicación precisa. De ser así, estas apps para ligar estarían violando las leyes de privacidad.

“Al descargar una app en el móvil, aceptamos tantos términos y condiciones legales que, en ocasiones, la mera aceptación de los Términos de Servicio ha sido considerada como una confirmación de que se desea recibir publicidad”, advierte Hervé Lambert, Global Consumer Operations Manager de Panda Security. Sin embargo, "el GDPR exige que los consumidores den un consentimiento explícito e informado para que sus datos personales puedan ser utilizados para su comercialización” añade.

Por ello, es importante saber qué se está haciendo con los datos y quién puede tener acceso a ellos. En este sentido es aconsejable contar con medidas de seguridad que encripten todas las comunicaciones que salen de todos los dispositivos, ya sean móviles, ordenadores o wearables. Porque, además del uso comercial que le puedan dar terceros a la información, también existirá siempre el riesgo de que algún ciberdelincuente se haga con la base de datos de usuarios de una de estas apps y haga un uso ilegal de ella.

Aunque las compañías tienen la obligación de notificar cualquier incidente de seguridad sobre los datos personales, la mitad de las empresas reconoce haber sufrido alguna fuga de datos en los últimos años, según la encuesta Intangible Assets Financial Statement Impact Comparison Report de 2019 del Ponemon Institute.

“Es decir, si nuestra información no queda encriptada desde el momento en el que sale de nuestros dispositivos, hay muchas papeletas de que algún dato sensible pueda filtrarse en internet tarde o temprano” apunta Hervé Lambert.

Por ello, se recomienda tener cuidado al descargar apps en el móvil y solo hacerlo cuando provienen de fuentes fiables. Al igual que no se debe comprar medicinas a un desconocido por la calle, tampoco se debe descargar jamás una aplicación que no provenga de Google Play o de Apple Store. Por sentido común, jamás hay que descargarla.

Aun así, sigue habiendo muchas aplicaciones que, al inciarlas, envían innumerables ventanas emergentes en las que se pide acceso a ciertas funcionalidades del dispositivo en cuestión. Cuando esto ocurra, lo acertado es dudar de por qué necesitan usar esas operativas y si la información que recojan pueda ser tratada con la intención de generar un perfil a partir de la actividad diaria del móvil del usuario.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Derecho Marketing E-Commerce Ciberseguridad Dispositivos móviles