LA POLÉMICA CON FACEAPP REABRE EL DEBATE SOBRE LA SEGURIDAD DE LOS DATOS PERSONALES

La popular «app» que envejece el rostro no es inofensiva: vulnera la privacidad de quien la descarga. La empresa dueña dice borrar las imágenes a las 48 horas pero, pese a que no es la única que solicita acceso a información personal, la polémica ha servido para recordar la importancia de la protección de datos.

30 de julio de 2019

FaceApp ha reabierto el debate sobre la comercialización de los datos personales de los usuarios por parte de las aplicaciones y los servicios digitales más populares. La «app**» está arrasando en internet** gracias a su filtro de retoque digital, que permite simular el paso del tiempo en una persona: **envejecerla en cuestión de segundos**. Sus resultados son sorprendentes, hasta el punto que es el fenómeno viral del momento, especialmente entre los famosos. Sin embargo, no es oro todo lo que reluce. Y es que el servicio genera numerosas dudas, especialmente en lo que se refiere a su política de privacidad.

Esta, de entrada, no se ajusta al completo a las exigencias vigentes en el **Reglamento General de Protección de Datos.** La letra pequeña de la «app» oculta detalles preocupantes; ya que se reserva el derecho de usar la información personal de los usuarios y las fotos que hagan con fines comerciales, **aunque promete que no los vende a terceros sin el consentimiento del usuario**. A su vez, se garantiza el acceso a dichos datos a todas las firmas del grupo ruso **Wireless Lab**, la propietaria de FaceApp, así como a aquellas compañías desconocidas que se conviertan en «afiliadas».

Las cláusulas de uso de la aplicación establecen, de una manera bastante ambigua y superficial, que **los usuarios otorgan a la empresa una «licencia perpetua, irrevocable, no exclusiva**, sin royalties, totalmente pagada y con licencia transferible» para «usar, reproducir, modificar, adaptar, publicar, traducir, crear trabajos derivados, distribuir, realizar públicamente y mostrar» los resultados obtenidos. La «app» solicita, entre otras cosas, acceso al carrete fotográfico, según apuntario grupos de analistas de seguridad en los primeros días, aunque una investigación posteriormente lo puso en duda: en principio, **solo accede a la imagen que se va a tratar digitalmente. No obstante, el servicio permite utilizarse sin la necesidad de registrarse, aunque ofrece, siendo este su verdadero modelo de negocio, la posibilidad de suscribirse para obtener mejoras.**

Disponible 48 horas

Sin embargo, Wireless Lab ha defendido que **la mayoría de las fotos subidas se eliminan de sus servidores a las 48 horas**. Los expertos creen que el problema adicional de este tipo de aplicaciones es que obligan al usuario a entregar demasiados datos personales. «Los términos de uso son una plantilla que aparece por internet. Lo tienen miles de páginas. **Son términos genéricos que aparecen por la Red**. No incluye nada sobre la normativa de protección de datos actual, recogida por el Reglamento General de Protección de Datos, ni tampoco de lo que obliga la ley a incluir. Fiabilidad no me ofrece ninguna», dice a ABC **Samuel Parra**, jurista digital.

«Cuando los usuarios descargan esta aplicación no tienen un acceso fácil a sus términos y condiciones y a su política de privacidad, la cual no se actualiza desde enero de 2017, tienen que consultarlo en la web. Esto hace que casi nadie se pare a consultar qué información se va a compartir con la aplicación y cuál es el uso que va a hacer de ella», añade a este diario **Sergio Maldonado,** director de la firma de gestión de datos en PrivacyCloud.

Rusia, detrás

Wireless Lab se esconde tras la aplicación. Esta compañía, fundada en 2014 por **Yaroslav Goncharov**, **se ubica en Rusia**, aunque en las tiendas de aplicaciones se presenta con sede en el estado de **Delaware**, Estados Unidos. Esta zona del país norteamericano está considerada en la práctica un «**paraíso fiscal**», motivo que ha llevado al senador del Partido Demócrata de Estados Unidos, **Chuck Schumer**, a solicitar al FBI y a la Comisión Federal de Comercio (FTC) que inicien una investigación sobre la «app» por motivos de seguridad. «La aplicación requiere que los usuarios proporcionen acceso total e irrevocable a sus fotos y datos personales, lo que podría plantear un problema de seguridad nacional y riesgos de privacidad para millones de ciudadanos de los EE.UU.», asegura en una carta enviada al director del FBI, **Christopher Wray**, y al presidente de la FTC, **Joe Simons.**

Por su parte, la compañía ha tratado de dar carpetazo a la polémica suscitada por su política de privacidad. De este modo, **ha negado que las imágenes procesadas sirvan para «entrenar» sistemas de inteligencia artificial rusos.** «No usamos fotos para el entrenamiento de reconocimiento facial», explicó Goncharov, que añadió que la «app» está pensada exclusivamente para «editar y mejorar las imágenes». Al mismo tiempo, la firma ha enviado un comunicado en el que sostiene que su principal motivación a la hora de guardar las imágenes de los usuarios es la de «asegurar que el usuario no cargue una foto repetidamente cada vez que quiera realizar una edición». **La empresa también niega cualquier relación con el gobierno ruso**: «Aunque el equipo central de I + D se encuentra en Rusia, los datos del usuario no se transfieren a Rusia».

A pesar de las **crecientes dudas acerca de sus políticas,** parece que la compañía no está perdiendo el apoyo de los usuarios. Así lo demuestra el que la aplicación cuente con más de 80 millones de usuarios en todo el mundo y haya escalado

rápidamente en España hasta convertirse en **la aplicación más descargada en los móviles Android**. Pese a que no es la única que solicita acceso a información personal, la polémica ha servido para recordar la importancia de la protección de datos

El hermetismo y las dudas acerca del tráfico de datos se han convertido en un problema recurrente entre los servicios digitales, que suelen solicitar más información de la necesaria. Además, lo hacen saltándose las leyes de privacidad y aprovechándose, en muchas ocasiones, de los usuarios con menos conocimientos en la materia. Es algo que motivó el escándalo de **Cambridge Analytica**, que ha provocado las dudas y pérdida de confianza sobre Facebook.

Miles de apps recaban información sin permiso

Una investigación del Instituto Internacional de Ciencias de la Computación, entre los que se encuentra un investigador español, detectó recientemente la presencia en la tienda Google Play, en Android, de más de mil aplicaciones que recopilan datos personales de sus usuarios incluso después de haber desactivado los permisos. De esas **1.325 aplicaciones que violaban los permisos en Android**, la mayoría usaban técnicas ocultas en su código que les permitía consultadas datos personales de fuentes, como las redes Wi-Fi conectadas y los metadatos almacenados en las fotografías.

Tras analizar unas 88.000 aplicaciones, los investigadores hallaron pruebas que demuestran que **muchos servicios digitales tienen restricciones limitadas**, lo que les permite recopilar información precisa de los usuarios, acceder a su ubicación, así como consultar datos del teléfono. Y lo hacen a espaldas del afectado, sin recibir el necesario consentimiento expreso que exige el marco legal. Pese a la incapacidad de acceder a información como la ubicación por GPS, los investigadores explican que estas «apps» pueden consultar otros apartados ocultos donde se almacenan estos detalles, con lo que pueden explotarlo para beneficio propio.

Respuestas para iniciados

¿Qué es FaceApp?

No es una aplicación nueva. Saltó a la palestra en el año 2017 debido a su polémico «filtro de etnicidad», que tuvo que ser retirado al poco tiempo debido a numerosas acusaciones de racismo. Desde entonces, la «app» se ha limitado a ofrecer la posibilidad al usuario de envejecer sus fotografías y de transformar las expresiones. La empresa detrás del desarrollo de su desarrollo es Wireless Lab, una compañía de origen ruso dirigida por el ingeniero Yaroslav Goncharov desde 2014. A pesar de ello, la firma se ubica en la localidad de Wilminton, perteneciente a Delaware, Estados Unidos.

¿Por qué tanta polémica?

FaceApp, así como el resto de empresas del grupo Wireless Lab y sus afiliados, se reserva el derecho de emplear la información que le otorga el usuario, así como las fotos que edita. Todo ello con fines netamente comerciales, aunque desde la aplicación se comprometen a no vender este contenido a terceros siempre que no se cuente con permiso, lo que ha originado una gran tormenta social, incluso política.

¿Cómo funciona la «app»?

Durante los últimos días ha crecido el temor de que FaceApp tuviese como finalidad emplear las imágenes de los usuarios para mejorar los algoritmos de reconocimiento facial. Sin embargo, desde la empresa propietaria desmienten que se esté trabajando en ello. «No, no usamos fotos para el entrenamiento de reconocimiento facial. Solo para editar imágenes», dijo a la BBC el director ejecutivo de la compañía, Yaroslav Goncharov. El servicio, aunque de procedencia rusa, emplea servidores de Google y Amazon para procesar las imágenes, según confirmó «Forbes». De ser así, los riesgos de privacidad que plantea pueden no ser muy diferentes de los planteados por muchas otras aplicaciones o por el uso extenso de Facebook.

Fuente: www.abc.es