

FaceApp, un “cambio de sexo” con una peligrosa letra pequeña.

Por: José Mendiola Zuriarrain. El País. 19/06/2020

La popular aplicación rusa, de nuevo en el punto de mira por su política de privacidad.

¿Quién no ha visto el rostro de un político transformado en el sexo opuesto? Estas divertidas estampas están invadiendo las redes sociales y aligerando los ánimos, precisamente cuando la crispación en el terreno político marca máximos. Cómo no sonreír ante una escena tan informal cuya autoría se debe reconocer a FaceApp, la popular app de la empresa rusa Wireless Lab. Ha sido una reciente actualización en la que, empleando magistralmente técnicas de deepfake, permite transformar con un sorprendente realismo el género de un rostro. Sí, se puede ver qué aspecto tendrían los políticos españoles si fueran del sexo opuesto y un hilo en Twitter viralizado al extremo lo demuestra.

Sin embargo, los expertos han alertado sobre la controvertida política de privacidad de la aplicación: se debe aceptar como requisito imprescindible para utilizar la aplicación y esconde algunas inquietantes sorpresas. De esta manera, y tras instalar la aplicación en el móvil, de debe aceptar una política de privacidad que fue actualizada el pasado 4 de junio y que contiene unos requisitos de los que no todo el mundo es consciente. Entre ellos, el usuario deberá aceptar que el sistema registre la IP del dispositivo y lo que resulta más preocupante, la página web que se ha visitado antes de utilizar su sistema.

El momento de ocio y chanzas disfrutando de los cambios en las fotos paga su peaje también cuando descubrimos que se acepta tácitamente que FaceApp registre buena parte de nuestra “actividad online”. En un apartado al efecto, el servicio advierte que registrará “las páginas visitadas, tiempo y duración de los accesos”, y lo peor del asunto es que se acepta que esta información sea cedida a “terceras partes”. No puede decirse que las cláusulas de privacidad de FaceApp sean confusas, sino que explican claramente que se comercia con los datos, siempre anonimizados, según explican y que posteriormente son vendidos a terceros.

Los expertos recomiendan revisar las cláusulas antes de instalar las apps.

No es la primera vez que FaceApp se sitúa en el disparadero por este motivo y ya en 2019 sus creadores se vieron envueltos en una polémica similar tras la cual se vieron desbordados ante el aluvión de usuarios que demandaba borrar su rastro de los servidores. El principal problema de este tipo de aplicaciones gratuitas es doble: por un lado y al ser gratuitas, la práctica totalidad de ellas obtiene un rendimiento de explotar los datos del usuario; por otro lado, quien quiera disfrutar de este tipo de apps debe aceptar, casi a ciegas, sus políticas de privacidad. Una vez que se aceptan, ya no hay vuelta atrás salvo que se ejerzan los derechos en materia de privacidad.

“Se puede comprobar el nivel de privacidad de una aplicación antes de instalarla”, explica a EL PAÍS Daniel Creus, analista de seguridad de Kaspersky, que recomienda visitar servicios que recopilan las políticas de privacidad como AppCensus. En cualquier caso, debe asumirse que un servicio gratuito —pese a que FaceApp cuenta con una opción de pago— obtendrá rendimiento de los datos del usuario, algo que “de por sí, no tiene por qué ser negativo siempre y cuando seamos conscientes de ello y la política de privacidad sea transparente”, explica Creus.

Más preocupado se muestra Fernando Suárez, presidente del Consejo General de Colegios de Ingeniería Informática, que advierte que ceder estos datos a ciegas es como “vender el alma al diablo”. Este experto advierte además de la gravedad en la falta de concienciación general sobre la privacidad de los datos y recuerda que “al publicar datos en internet, perdemos por completo el control sobre los mismos”. Pero las redes sociales y triunfar con contenido atractivo y diferente es una tentación demasiado irresistible para muchos que minimizan los riesgos. “Nuestra vanidad supera nuestro sentido común y cedemos nuestra imagen, ya no solo en redes sociales, sino a empresas que usan técnicas de inteligencia artificial para su procesamiento y asociado a incontables datos sobre nuestra privacidad”.

[LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ](#)

Fotografía: El Confidencial.

Fecha de creación

2020/06/19