Por qué los cifrados de Facebook o de Whatsapp no sirven para nada

DIEGO HERCHHOREN :: 27/08/2015

Los cifrados de Facebook o de cualquier otra red social siguen estando sometidos al imperativo de entregar los algoritmos a las autoridades. El caso Blackberry en Reino Unido

Al menos en Europa. Ampliemos esto a cualquier otra aplicación corporativa que presuma de proteger nuestras conversaciones. Las filtraciones de la NSA y todo lo que tiene que ver con la vigilancia masiva en muchos países del mundo ha desatado una carrera publicitaria entre los pesos pesados de las redes sociales y la mensajería, con el fin de revertir la mala imagen adquirida por su colaboración con estos programas de vigilancia.

Pero lo cierto es que las funcionalidades añadidas en muchas de ellas no sirven para nada, y la explicación no es técnica, sino jurídica. Las normativas europea y española establecen tres aspectos para los operadores que presten servicios de comunicaciones electrónicas disponibles al público: que los datos generados sean retenidos, que el almacenamiento y entrega a las autoridades sea libre de cualquier cifrado y que los organismos reguladores tengan acceso a los dispositivos de cifra utilizados en esas redes.

La Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, imponía a las empresas operadoras el deber de conservación y en su caso, de entrega, de los metadatos relativos al tráfico de sus redes. Y por operadores no solo debe entenderse a las empresas proveedoras de la infraestructura comunicacional, sino también a las empresas que proveen servicios de mensajería instantánea, correo electrónico o mensajería privada.

Y decimos imponía porque una reciente sentencia del Tribunal de Justicia de las Comunidades Europeas ha anulado la norma por considerarla intrusiva de la vida privada.

Un conjunto de normas habilitantes de la vigilancia masiva

La ley española que desarrolla esta Directiva comunitaria (que todavía sigue en vigor), y de la que hablamos en un post anterior, establece el catálogo de datos que deberán ser almacenados obligatoriamente, entre los que están las identidades de los intervinientes, la hora, el lugar, las características técnicas de las terminales, la identificación de éstas, etc.

También afirma que "*ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley*". Sin embargo, la norma española de protección de datos y los dictámenes del GT29, que también afecta a los operadores como Facebook o Whatsapp, identifica a éstas como auténticos ficheros de datos personales donde se almacenan los contenidos producto de las comunicaciones electrónicas de sus usuarios.

Pero además, la Ley General de Telecomunicaciones impone a los operadores que utilicen

las redes de acceso público "*facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control*".

Resumiendo:

- El Estado es el titular de la infraestructura de redes para las comunicaciones electrónicas, y otorga los derechos de explotación a los operadores.
- Los operadores, por definición, almacenan y conservan los datos de carácter personal, entre los que se incluye el contenido de las comunicaciones electrónicas.
- Los operadores pueden proveer mecanismos de cifrado a los usuarios de esas comunicaciones, pero deben facilitar al Estado los algoritmos y aparatos de cifra.
- En cualquier caso, los operadores deben conservar todos los datos relativos a la identidad de los intervinientes en la comunicación, dispositivos empleados, identidad de los aparatos, etc.

¿Por qué entonces los cifrados no sirven?

Porque si bien nacieron para evitar la vigilancia masiva de nuestras comunicaciones, existe todo un conjunto de normas que permite a las agencias estatales habilitadas a capturar todos esos datos, disponiendo además de mecanismos útiles para romper la protección que se le pudiera aplicar, ya que el Estado es el titular de la infraestructura.

Por otro lado, se trata de mecanismos de cifrado cuyo código fuente no se encuentra a disposición del público; esto supone la imposibilidad de comprobar la existencia de "puertas traseras" en estas herramientas, quedando la facultad de hacer esta comprobación limitada a dos actores: el creador del programa, y la agencia gubernamental que tenga acceso a la misma por imperativo legal. Y es que ambos se necesitan: los operadores necesitan la venia legal y el Estado necesita a los operadores.

Por poner un ejemplo, Whatsapp anunció en noviembre de 2014 el lanzamiento de una función de cifrado*end-to-end*, tras desvelarse varios problemas de seguridad en la aplicación. No sabemos si ha ocurrido ya, pero acorde a la normativa española, la Comisión del Mercado de las Telecomunicaciones está facultada para requerir a Whatsapp Inc. los algoritmos de cifra, situación que tiene precedentes en Europa. Recordemos que Blackberry hizo lo propio con las autoridades británicas durante las revueltas callejeras del verano de 2011.

El caso de Facebook y PGP

Quien ha ido más lejos en este tema ha sido Facebook. La red social de Mark Zuckerberg ha implementado, en fase beta, la funcionalidad de OpenPGP, un sistema de cifrado de código abierto que parece ser el que más problemas ha traído a la NSA. Pero esto debe ser motivo de desconfianza.

Facebook es un operador imprescindible del programa de vigilancia PRISM, siendo además una empresa caracterizada por el almacenamiento masivo de datos de usuarios y que vive de la transferencia comercial a terceros de sus gustos y opiniones. La funcionalidad de

PGP implementada no tiene como finalidad evitar esta transferencia de datos, sino que afecta sólo a las comunicaciones entre usuarios, estando esta función además en fase de desarrollo. Esto quiere decir que nada impide a Facebook recomponer la confianza de los usuarios para hacer cambios posteriores introduciendo un cifrado con algoritmo secreto.

De momento, la función de la red social puede traer controversias legales a la compañía, que no tiene buenas relaciones con la normativa europea de protección de datos. Y es que la solución a estas intromisiones sigue pasando por aplicaciones que permitan la auditoría pública de su código fuente; podemos ver muchas de ellas aquí.

www.buenjuicio.com

---

https://www.lahaine.org/est_espanol.php/por-que-los-cifrados-de