OPINIÓN / DESPUÉS DE LA PANDEMIA

El error de pretender prohibir el cifrado

por Enrique Dans

24 mayo, 2023 - 02:37

GUARDAR

Un documento filtrado y obtenido por Wired revela que los planes de España, a las puertas de comenzar sus seis meses de presidencia de la Unión Europea, son los de tratar de liderar la prohibición de un elemento fundamental de toda sociedad digital y democrática: **el cifrado de extremo a extremo.**

Aplicaciones de mensajería como Signal, Telegram o WhatsApp utilizan el cifrado extremo a extremo como una **garantía de la privacidad de las comunicaciones** entre sus usuarios. En realidad, cuando WhatsApp comenzó su andadura siguiendo la visión de sus fundadores, Jan Koum y Brian Acton, como un "SMS con esteroides", carecía completamente de cifrado: recuerdo perfectamente un ejercicio en clase que permitía rápidamente acceder a todos los mensajes que fluían por la red del IE, y hasta qué punto les parecía demencial a mis alumnos que algo así pudiese ser tan sencillo.

Cuando el mercado comenzó a criticar a WhatsApp, en su momento de popularización masiva, por carecer de cifrado, la compañía, tras algunas pruebas, terminó adoptando la tecnología de Signal, de código abierto, e implementando gracias a ello un cifrado robusto y con garantías: algunos episodios, como el de los jueces brasileños que llegaron a cerrar WhatsApp en todo el país porque sus responsables se negaban a descifrar presuntas conversaciones entre narcotraficantes mientras la compañía se hacía cruces intentando explicarles que eso no era técnicamente posible, permitieron comprobar que **la promesa de comunicaciones verdaderamente protegidas era real.**

Con la tecnología de cifrado de extremo a extremo, solo el emisor y el receptor pueden ver el contenido de un mensaje. En cada conversación

receptor pueden ver el contenido de un mensaje. En cada conversación, cada uno de los mensajes que se cruzan se cifra con una clave única que impide descifrarlo a nadie que no sea el dispositivo de su receptor, incluida la compañía propietaria de la herramienta. La única manera de ver ese mensaje sería teniendo acceso al propio dispositivo del emisor, o instalando en él algún programa que lo reenvíe una vez descifrado (como se ha hecho en algunos casos conocidos de espionaje de alto nivel).

El cifrado es una herramienta básica que defiende un derecho fundamental: el de las comunicaciones privadas. Por supuesto, ese derecho tiene lo que tienen todos los derechos: que todos lo pueden ejercer, y eso incluye no solo a los ciudadanos y a sus comunicaciones cotidianas, sino también a **terroristas, narcotraficantes o pedófilos de todo tip**o, algo que los gobiernos, obviamente, pretenden impedir.

El cifrado es una herramienta básica que defiende un derecho fundamental: el de las comunicaciones privadas

Ahora bien: ¿es eso técnicamente posible? En principio, si un canal deja de ofrecer una garantía de cifrado de extremo a extremo, ¿qué hacen aquellos que pretendían utilizarlo para ocultar actividades ilegales? Lógicamente, **cambiarse a otro canal que permita ese cifrado**, algo que puede, hoy en día, crearse de manera relativamente sencilla, y el Gobierno en cuestión se quedaría simplemente espiando las comunicaciones de los ciudadanos que no intentan llevar a cabo nada ilegal, sino simplemente ejercer su derecho a una comunicación privada.

Algunas cuestiones, como el anonimato o el cifrado, parecen ofender a muchos políticos: en realidad, esa pretendida ofensa no es nada más que incultura digital, carencia de una formación adecuada. Y pretender, a partir

de una carencia en tu formación, legislar en contra de un derecho fundamental es un error**. Un error enorme, que España nunca debería asumir.** Sobre todo, porque nuestro país, con algunos episodios en su historia reciente como la expulsión de Google News, se ha ganado cierta mala fama de anti-tecnológico, y eso es algo muy peligroso en los tiempos que vivimos, susceptible de alejar inversiones y de convertirse en un cliché.

En algunos casos, como la persecución de compañías como Uber o Deliveroo, o **el intento de freír a impuestos a las compañías tecnológicas,** los intentos de España se convirtieron, al cabo de un tiempo, en iniciativas que otros países también han seguido, y que han terminado demostrando ser razonablemente equilibradas. Pero en otros, como el caso del cifrado extremo a extremo, ni va a ser así, ni deberías ser así, ni lo será nunca.

Algunas cuestiones, como el anonimato o el cifrado, parecen ofender a muchos políticos

Hablamos de un error tecnológico conceptual que supondría un atentado contra un derecho fundamental, pero que, sobre todo, sería preocupante porque no serviría para absolutamente nada: simplemente, la tecnología de cifrado extremo a extremo no se puede "desinventar", y los que pretenden ocultar sus comunicaciones con el propósito de llevar a cabo actividades ilegales siempre la van a tener a su disposición, hagan lo que hagan los gobiernos de turno. Pretender, por tanto, que las compañías descifren las comunicaciones de los ciudadanos a petición del gobierno correspondiente es, simplemente, un liberticidio con tintes dictatoriales, algo que sería esperable de un gobierno como China, pero que nunca debería serlo en un país democrático.

España nunca debería liderar iniciativas en contra del cifrado extremo a extremo, y si lo hace, será un grave error que perjudicará su reputación y su capacidad de liderazgo, Nada desgasta más a un gobierno que la promulgación de medidas que no sirven para nada. **Es fundamental explicar a los políticos que esa iniciativa es como darse cabezazos contra una pared**, algo que nadie con un mínimo de inteligencia debería hacer. Y menos, en un país que pretende que todos lo vean como una democracia madura.

******Enrique Dans es Profesor de Innovación en IE University.***