>> Jorge Dávila

La eterna y falsa disyuntiva

Una vez más se oyen lamentos de que con un buen cifrado de las comunicaciones de todo tipo lo que hacemos es beneficiar al crimen organizado, y no se recuerda que ese mismo cifrado, esa misma protección de cualquier comunicación, es la base de la libertad de operación en nuestras sociedades. No es la primera vez que las fuerzas de seguridad del estado quieren acercar el áscua a su sardina, pero no por ello debemos dejar de prestar atención a qué significa realmente lo que están planteando. Quizás descubramos que su versión de los hechos está claramente sesgada y esconde riesgos no calculados.

Aunque no es nada nuevo eso de **ir en contra del uso civil de la criptografía** [1] por parte de los estados y las distintas administraciones con responsabilidades en temas de seguridad, la entrega que nos ocupa –la solicitud en el pasado mes de abril de este año–, en la que la Europol pide a los gobiernos europeos **que se prohíba el cifrado de las comunicaciones** [2], quizás tiene su origen en el 2 de julio de 2021, día en el que **Europol** [3] y **Eurojust** [4] publican el "***Third report of the Joint Observatory Function on encryption***" [5].

Este informe anual es parte de las seis medidas prácticas que la UE anunció en su undécimo informe de progreso hacia una efectiva y genuina "*Security Union*" [6], y en él se anima a las Fuerzas de Seguridad del Estado y a la Justicia que superen los retos que a ellos les plantea el uso de la criptografía, en concreto del cifrado, en el contexto de las investigaciones y persecuciones criminales

El tercer informe sobre criptografía presenta por primera vez los desarrollos clave que sobre el cifrado se están haciendo en distintas regiones y países del mundo para intentar aclarar las interacciones entre los desarrollos técnicos, legislativos y políticos en esta área.

En particular, el tercer informe resalta los retos que afrontan las fuerzas de seguridad del estado para legalmente interceptar las comunicaciones y obtener así evidencias, pruebas, para sus investigaciones criminales. Así mismo, ese informe también plantea qué desarrollos políticos que están influyendo y dando forma al debate público sobre el cifrado en Europa.

En lugar de hacer un discurso general sobre el uso del cifrado por parte de cualquiera, las autoridades europeas prefieren centrar su tiro en las empresas que puedan optar por el uso del cifrado en sus productos.

El acceso en claro a 1) todas las **comunicaciones cifradas** y 2) todo **dato almacenado cifrado** presenta aspectos difíciles y muy controvertidos entre los **custodios de las claves**, las **fuerzas policiales** y las **judiciales**, por una parte y las **Organizaciones por los Derechos Civiles** por otra.

Lo curioso es que las autoridades europeas parten de la premisa de que hay que encontrar un equilibrio entre la seguridad de las comunicaciones y su capacidad para intervenirlas. Y quizás sea tiempo de negar la existencia de ese posible equilibrio.

UN EQUILIBRIO POLÉMICO E INVIABLE

Lo curioso es que las autoridades europeas parten de la premisa de que hay que encontrar un equilibrio entre la seguridad de las comunicaciones y su capacidad para intervenirlas. Y quizás sea tiempo de negar la existencia de ese posible equilibrio.

Las autoridades suelen partir sus discursos pidiendo que se ingenien **soluciones técnicas** que hagan posible reconciliar ambos intereses (Seguridad y Privacidad). En concreto mencionan como ámbitos de trabajo los **servicios de comunicación** electrónicas (**VPNs** [7], **MIs** [8] y aplicaciones como **Signal** [9] y **Telegram** [10] principalmente), los **espacios de almacenamiento** de datos online (*Cloud Storage*), los servidores de **correo electrónico y Redes Sociales**, etc., ya que son estos los escenarios donde el cifrado supone una barrera más insalvable para sus pretensiones de interceptar secretamente todo lo que se comunica.

[1] Ver https://en.wikipedia.org/wiki/Crypto_Wars

[2] Ver https://es.wired.com/articulos/europol-exige-eliminar-el-cifrado-de-extremo-a-extremo-en-whatsapp

[3] Ver https://en.wikipedia.org/wiki/Europol

[4] Ver https://en.wikipedia.org/wiki/Eurojust

[5] Ver https://www.europol.europa.eu/publications-events/publications/third-report-of-observatory-function-encryption

[6] Ver https://home-affairs.ec.europa.eu/system/files/2020-09/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

[7] Ver https://en.wikipedia.org/wiki/Virtual_private_network

[8] Ver https://en.wikipedia.org/wiki/Instant_messaging

[9] Ver https://en.wikipedia.org/wiki/Signal_(messaging_app)

[10] Ver https://en.wikipedia.org/wiki/Telegram_(software)

En este escenario, las autoridades europeas vuelven a plantear que hay dos posibles enfoques: por una parte se desarrollan herramientas que directamente **'*debilitan*' pública o privadamente el cifrado utilizado** y otra en la que se proporcionan herramientas de **depósito forzoso de claves** (***Key escrow*** [11]) que permitan tener acceso al contenido del mensaje siempre que se tenga acceso al criptograma, o incluso soluciones (***backdoors*** [12]) que permitirían tener acceso a la versión en claro del mensaje antes de que se cifre o después de que se descifre el mensaje.

Todas estas posibilidades, de facto, son lo mismo que aceptar que, para algunos (**¿Para quiénes exactamente y en concreto?**), se omita o se elimine completamente las virtudes que proporciona el cifrado y que no son otras que las de "**hacer accesible sólo a los autorizados por parte del emisor** (y no del juez de turno) **al contenido del mensaje**".

Los temas más concretos que preocupan a la Policía son **1)** aquellos escenarios en los que el cifrado es la opción por defecto para muchos usuarios del sistema. El tercer informe también menciona **2)** la proliferación del **cifrado basado en hardware** [13] y no en software. En concreto menciona las dificultades que impone aumentar el número de iteraciones en el cálculo de la función *hash* dependiente de una clave o **Funciones de Derivación de Claves** [14] como es el caso de **Bcrypt** [15], lo cual tiene efectos muy perniciosos en la implementación de ataques por fuerza bruta o de diccionario. También se lamentan de la mayor robustez en los mecanismos de generación de contraseñas empleados por algunas compañías para ayudar a sus usuarios a generar y utilizar contraseñas más seguras que todavía hoy podrían considerarse seguras *online*.

Otra bestia negra mencionada sería el concepto de **oblivious DNS** [16], donde las consultas del Domain Name System se realizan a través de canales volátiles y cifrados HTTPs, de modo que separa la obtención de direcciones IP concretas de las consultas de búsqueda que las invocan. Esto se consigue añadiendo y una capa de cifrado sobre la consulta DNS antes de mandársela al servidor intermediario que, en ese caso, actúa como mero intermediario ciego entre el usuario de internet y la web que quiere visitar. Esta tecnología desacopla la consulta del usuario del servidor DNS que tiene que resolverla.

Las acciones criminales no se distinguen de las no criminales más que en lo que diga el correspondiente Código Penal o la legislación de cada país. Las dos posibilidades clásicas mencionadas (debilitamiento del cifrado o deposito obligatorio de las claves) no han tenido mucho éxito porque, ambas, ponen en claro peligro la privacidad de los ciudadanos y conculcan directa o indirectamente muchos otros derechos fundamentales.

CRECIENTE DEPENDENCIA DEL CIFRADO

Todos estos desarrollos reflejan la creciente dependencia del cifrado en lo que se refiere a la protección de la ciberseguridad, la protección de los datos y la privacidad de las comunicaciones. Aunque todos corren a declarar públicamente su beneplácito y necesidad de estas nuevas protecciones, muchos no tardan en mencionar que esta misma tecnología **puede ser utilizada con fines criminales** (¿y cuáles no?), además de complicar seriamente la investigación digital de los crímenes que se cometen continuamente y que son una amenaza para la paz social tal y como la conocemos.

Por si el escenario no fuese suficientemente confuso, el adviento de lo denominado como **Quantum computing** se presenta como "*santo grial*" [17] que vendría a devolver a la Policía y los Jueces (¿Y a quién más?) la posibilidad de terminar venciendo al cifrado de cualquiera y así mitigar sus actuales dificultades. Mientras los apóstoles de este nuevo Mesías tecnológico tengan éxito en sus campañas de adviento, más probable es que los jueces y policías sigan "*Going Dark*" [18].

Aunque el escenario es complejo e insoluble porque las acciones criminales no se distinguen de las no criminales más que en lo que diga el correspondiente Código Penal o la legislación de cada país, las dos posibilidades clásicas que se han mencionado (debilitamiento del cifrado [19] o depósito obligatorio de las claves [20]) no han tenido mucho éxito porque, ambas, ponen en claro peligro la privacidad de los ciudadanos y conculcan directa o indirectamente muchos otros derechos fundamentales de los ciudadanos y de las personas. Por ello, este escenario no se ha quedado asi y en los últimos años han ocurrido cosas interesantes.

EL CASO ENCROCHAT: INCORRECCIÓN EN DISEÑO

Un elemento muy importante en este caso es el de los teléfonos y el servicio **EncroChat** [21]. Este es un ejemplo

[11] Ver https://en.wikipedia.org/wiki/Key_escrow

[12] Ver https://en.wikipedia.org/wiki/Backdoor_(computing)

[13] Ver https://en.wikipedia.org/wiki/Hardware-based_encryption

[14] Ver https://en.wikipedia.org/wiki/Key_derivation_function

[15] Ver https://en.wikipedia.org/wiki/Bcrypt

[16] Ver https://en.wikipedia.org/wiki/DNS_over_HTTPS

[17] Ver https://en.wikipedia.org/wiki/Holy_Grail

[18] Going Dark es, en la jerga militar, la terminación repentina de una comunicación. Es el término utilizado para describir un escenario en el que la comunicación parece haber cesado, pero en realidad acaba de pasar de un canal de comunicación público, donde podría ser monitoreado, a un canal de comunicación privado que evita su intercepción (espionaje).

[19] Ver https://en.wikipedia.org/wiki/Bullrun_(decryption_program)

[20] Ver https://en.wikipedia.org/wiki/Bullrun_(decryption_program)

[21] Ver https://en.wikipedia.org/wiki/EncroChat

en el que se ve lo potente que ha sido el uso de las medidas técnicas necesarias (no conocidas públicamente del todo) y elementos legislativos que harán evolucionar los casos criminales creados a partir del desastre (para sus clientes) de EncroChat.

Las identidades de los que operaban EncroChat actualmente siguen siendo desconocidas y la justicia no ha decidido imputarlas en ninguno de los casos que tiene abiertos con esta Fuente como origen.

Lo teléfonos EncroChat eran dispositivos Android, muchos de ellos, en concreto basados en el modelo **BQ Aquaris X2** [22] fabricado por la extinta empresa Española BQ en 2018. A los teléfonos originales se le quitaban la cámara, el micrófono, el receptor GPS y las puertas USB, para asegurarse de que estuviesen **lo más aislados y ciegos posibles** y **sólo ejecutasen** el sistema operativo y las aplicaciones que sus promotores han elegido. Además de ello, se les dotó con "***botón del pánico***" consistente en un código PIN que, una vez invocado, borrara todos los mensajes que pudiera haber en el dispositivo

Este sistema de mensajería cifrada llamó la atención de la gendarmería francesa en 2017 por el número de esos dispositivos que se encontraban en registros habituales contra bandas criminales de todo tipo. Pronto se dieron cuenta de que los servidores que conformaban el servicio EncroChat estaban operando desde suelo francés y gracias a la legislación francesa al respecto y a la colaboración de un Juez de las ciudad de Lille, los franceses pudieron infiltrase en la organización y "*plantar*" un dispositivo técnico que les permitió, durante dos meses de autorización judicial (hasta el 12-13 de junio de 2020), acceder en claro a **todos los mensajes** que fueron tratados por la red de esa compañía.

Aunque hoy sigue sin estar claro de qué se trataba ese "*dispositivo*" tan sigilosamente plantado, los comentarios vienen a sugerir que los investigadores fueron capaces de colarse dentro de la red donde circulaban los mensajes en claro, más que haber sido capaces de romper el cifrado de los mensajes en tránsito.

El resultado fue uno de los más grandes éxitos de las policías europeas. El servicio hackeado tenía 60.000 suscriptores en ese momento. Aunque había usuarios de toda Europa, en el caso de UK la operación la llevó a cabo la National Crime Agency (**NCA**) y dio lugar a 2.600 arrestos y el establecimiento de 1.384 acusaciones criminales firmes.

Las distintas policías fueron capaces de fisgonear entre millones de mensajes de lo más explícitos y conseguir con ello un tesoro de evidencias con las que sustentar los casos criminales posteriores. Nikki Holland [23], director de investigaciones de la NCA, dijo que "*fue como hacerse con las llaves de la cueva de Aladino*", mientras que su segundo, Matt Horne [24], prefirió compararlo a "*cracking the criminals' Enigma code*". Por su parte, Steve Jupp [25], cabeza del National Police Chiefs' Council dijo que fue como "*having an **insider** in every organized crime group in the UK*".

Gracias al incorrecto diseño de seguridad del servicio EncroChat las policías y justicia europea ha desmantelado numerosos grupos criminales muy bien organizados y sólidamente establecidos a la vez que han conseguido evidencias prácticamente irrefutables para condenar a gran número de criminales conocidos por ellos pero que hasta entonces estuvieron siempre fuera de su alcance.

Los riesgos de hacer caso a quien pide prohibir el cifrado en general o el E2E en particular, o los que piden debilitar la resistencia de los métodos permitidos es poner coto a la intimidad y a los derechos ciudadanos y humanos de los usuarios. En el caso de aceptarse esas estrategias, ¿quién vigilaría por su correcta aplicación? ¿Quién vigilaría al vigilante?

MÁS EJEMPLOS DE ÉXITOS SIMILARES

Sin embargo, hay más ejemplos de éxitos similares, como son los casos de hackeo de la aplicación **Sky ECC** [26] (cierre de **Sky Global** en 2008), **Ennetcom** [27], y **Exclu** [28] cerrada en febrero de 2023, o el famoso caso del Caballo de Troya del FBI norteamericano llamada **ANON** [29], impulsada como consecuencia de la detención del CEO Vincent Ramos [30] y el subsecuente cierre de un servicio anterior llamado **Phantom Secure** [31]. Todas ellas eran soluciones que se presentaban frente a sus posibles clientes como mensajería anónima intrazable y completamente confidencial a través del cifrado de los mensajes. Sin embargo, **todas ellas cayeron por errores en su diseño y confección**, y hoy nutren el Honor Hall de muchas policías occidentales.

Podemos decir que, por el momento, el uso del cifrado realmente ha favorecido a las fuerzas de seguridad del estado y a la Justicia occidental ya que ha alimentado **una falsa sensación de seguridad** entre "*los malos*".

EL CIFRADO A EXTREMO A EXTREMO

Otra cosa es lo que se conoce como **Cifrado E2E**, **Cifrado Extremo-a-Extremo** [32]; en este caso, **los mensajes no se descifran más que cuando llegan a destino** y **se cifran justo después de**

[22] Ver https://www.xataka.com/moviles/aquaris-x2-y-x2-plus-caracteristicas-precio-ficha-tecnica

[23] Ver https://www.bbc.com/news/uk-wales-67808245

[24] Ver https://www.nationalcybersecurityshow.com/speakers/matt-horne

[25] Ver https://news.npcc.police.uk/releases/new-national-police-lead-for-serious-organised-crime-appointed

[26] Ver https://en.wikipedia.org/wiki/Shutdown_of_Sky_Global

[27] Ver https://en.wikipedia.org/wiki/Ennetcom

[28] Ver https://nltimes.nl/2023/02/03/dutch-police-take-exclu-encrypted-chat-service-42-arrests-eu4-million-seized

[29] Ver https://en.wikipedia.org/wiki/Operation_Trojan_Shield

[30] Ver https://www.unodc.org/unodc/en/untoc20/truecrimestories/phantom-secure.html

[31] Ver https://en.wikipedia.org/wiki/Phantom_Secure

[32] Ver https://en.wikipedia.org/wiki/End-to-end_encryption

En ALSO estamos contigo para ayudarte a crecer en tu negocio

NUESTRA PROPUESTA DE VALOR

¿Cómo ayudamos a desarrollar tu negocio en Ciberseguridad?

- Formación y capacitación
- Desarrollo de negocio
- Generación de demanda
- Servicios profesionales

Porque somos expertos en desarrollar el negocio de ciberseguridad de nuestros partners

ALSO TE OFRECE:

- Marcas líderes del mercado
- Migración de solución a Cloud
- Expertos en Ciberseguridad
- Automatización de la gestión de tu negocio con ALSO Cloud Marketplace
- Soluciones que se adaptan al mercado
- Consultoría adaptada a tus clientes

Contacta con un especialista de ALSO

comercial.es@also.com | +34-697172423

ser compuestos, por lo que el acceso a servidores intermedios de cualquier índole, no proporciona ningún tipo de ventaja al atacante (en este caso, la policía).

El único ataque útil conocido en los escenarios del E2EE es, en lugar de intentar romper el cifrado (cosa que puede ser imposible, pero seguro que es tremendamente cara), el atacante intentará colarse en medio de la comunicación (**MitM** o **Man-in-the-middle attach** [33]) suplantando al destinatario del mensaje durante la fase de negociación de claves (key exchange) o poniendo su clave pública sustituyendo a la del destinatario legítimo, de modo que los mensajes terminen cifrados con una clave conocida (también) por el atacante.

En y entre los gobiernos está de moda echarle la culpa a la necesaria adopción de las técnicas del E2EE por parte de los servicios digitales para proteger el secreto y privacidad de las comunicaciones de sus clientes, a una pretendida pérdida de posibilidades de investigación criminal, lo cual no es necesariamente cierto.

Solo Dinamarca, Francia, Alemania, Polonia, Suecia, Suiza y Holanda tienen en su legislación artículos que habilitan a su policía a utilizar herramientas técnicas para atacar el cifrado. En los demás países de la Unión, cada caso se trata utilizando principios generales de sus legislaciones. Sin embargo, en el análisis legal del problema hay que tener muy en cuenta que, en todos los casos, la ley distingue lo que es atacar al contenido cifrado de lo que son herramientas para tener acceso al contenido antes de ser cifrado y después de ser descifrado.

La verdad es que el avance de las técnicas de cifrado E2E lo único que hace es llevar el ataque a los extremos de la comunicación, y ello lo puede hacer siguiendo varios enfoques. Por una parte, **1)** puede interceptar en los extremos los mensajes justo antes de ser cifrados, y/o justo después de haber sido descifrados (estrategias de los **RATs** [34] como **Pegasus** [35] o **Imminent Monitor** [36]), o **2)** alterar de alguna manera en la autenticación de los comunicantes y montar un ataque MitM -persona interpuesta-, o **3)** participar imperceptiblemente en la **negociación de las claves de cifrado** de modo que el atacante pueda conocerla también (aunque no tenga ningún poder sobre cuál sea la clave utilizada) o, incluso, **4)** que, de alguna manera, el atacante **pueda "*forzar*" que la clave secreta negociada esté dentro de un conjunto** suficientemente pequeño para poder montar ataques por fuerza bruta [37].

Los riesgos de hacer caso a esas voces que piden prohibir el cifrado en general o el cifrado E2E en particular, o los que piden debilitar intencionadamente la resistencia de los métodos permitidos es poner coto a la intimidad y a los derechos ciudadanos y humanos de los usuarios.

No solo hay que defender la libertad individual como hacen algunos 'anarco-liberales de motosierra' y alguna 'Lady Machetes', también hay que defender la libertad colectiva de las mayorías y minorías sociales si queremos vivir en paz, por lo que la comunicación entre ciudadanos debe seguir siendo secreta y sagrada.

En el caso de que se aceptasen esas estrategias, ¿quién vigilaría por su correcta aplicación? ¿Quién vigilaría al vigilante?

En un país como el nuestro en el que la sombra del **lawfare** [38] hace que un 70% de los ciudadanos no se fíe de sus jueces [39] y el resultado depende del juez que te toque [40], y que haya ejemplos sobrados de prácticas de vigilancia policial ilegales [41] al servicio del Ministro del Interior de turno, facilitar la interpretación de las comunicaciones **no va a protegernos del crimen organizado** (que siempre seguirá siendo ilegal en sus usos) y **sí nos va dejar desprotegidos** de las **cloacas del estado** [42], de las **cloacas del Ibex35** [43], y del **espionaje sicario** [44] de quien pueda pagarlo.

No solo hay que defender la libertad individual como hacen algunos "anarco-liberales de motosierra" y alguna "Lady Machetes" [45], también hay que defender la libertad colectiva de las mayorías y minorías sociales si queremos vivir en paz, por lo que la comunicación entre ciudadanos **debe seguir siendo secreta y sagrada**. Quien no lo entienda, que se vaya al prefacio de un libro de códigos [46] para la Correspondencia Telegráfica de los ferroviarios de Galesburg en 1892:

> *… is intended more especially for Telegraphic Correspondence **in time of trouble, when it is desirable or necessary to send telegrams that can not be read by any but those for whom they are intended**, as is the case in time of strikes or other important moves on the part of an Organization…*

Sin más, sólo puedo pedir ¡Larga vida al buen cifrado! ■

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[33] Ver https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[34] Ver https://en.wikipedia.org/wiki/RATS_(software), y/o https://en.wikipedia.org/wiki/Remote_desktop_software

[35] Ver https://en.wikipedia.org/wiki/Pegasus_(spyware)

[36] Ver https://www.pcrisk.es/guias-de-desinfeccion/9105-imminent-monitor-rat

[37] Ver https://en.wikipedia.org/wiki/Brute-force_attack

[38] Ver https://en.wikipedia.org/wiki/Lawfare

[39] Ver https://www.lavanguardia.com/politica/20240630/9765353/confia-justicia-espana.html

[40] Ver https://www.publico.es/politica/fiscalia-recurre-absolucion-hombre-amenazo-heterosexual-hostias.html

[41] Ver https://elpais.com/espana/2024-07-12/radiografia-de-la-guerra-sucia-del-pp-y-su-policia-politica-contra-podemos.html

[42] Ver https://es.wikipedia.org/wiki/Estado_profundo

[43] Ver https://www.infolibre.es/politica/espionajes-luchas-acceso-informacion-privilegiada-caso-villarejo-saca-luz-verguenzas-grandes-empresas-ibex-35_1_1191466.html

[44] Ver https://www.clarin.com/mundo/sombrias-operaciones-wetwork-trabajo-sucio-espias-sicarios_0_HyRckilbG.html

[45] Ver https://www.eldiario.es/rastreador/lady-machetes-apodo-vox-ayuso-echarle-cara-ataques-menas-convierte-tt_132_8740395.html

[46] Ver https://telegrafie.cz/files/cipher-code-1892.pdf