# Replanteando la Conversación: Sumergiéndose a profundidad en el debate sobre cifrado

***Para los gobiernos, el cifrado impide a las fuerzas de seguridad hacer su trabajo, pero la tecnología nos protege a todos, incluidos los niños y otras poblaciones vulnerables.***

**Febrero 2024**


Recopilado por:
Heather West | Director Senior
+1 202.344.4597
HEWest@Venable.com

Zack Martin | Asesor Político Senior
+1 202.344.4393
ZPMartin@Venable.com

Ivy Orecchio | Jefe de Proyecto
+1 202.344.4277
IDOrecchio@Venable.com


CENTER FOR CYBERSECURITY POLICY AND LAW

# Tabla de Contenidos

# Resumen Ejecutivo

El cifrado desempeña un papel fundamental en la confidencialidad y protección de los datos al salvaguardar las comunicaciones en línea, permitir la libertad de expresión, proteger las transacciones financieras, entre otras cosas. El Center for Cybersecurity Policy & Law, junto con la gran mayoría de los que conforman la comunidad especializada en ciberseguridad, cree que debilitar el cifrado pondría en peligro la seguridad, la privacidad, las libertades civiles y los intereses sociales vitales de todas las organizaciones e individuos.

Mientras que el cifrado protege a las personas contra delitos como el robo de identidad o la vigilancia ilegal, las fuerzas del orden y las agencias de seguridad nacional argumentan que éste dificulta o imposibilita la investigación de delitos y amenazas a la seguridad pública. Algunos argumentan que, en la era digital, la investigación requiere necesariamente pruebas digitales, incluidas las comunicaciones interceptadas y descifradas relacionadas con la seguridad pública, el terrorismo y el material de abuso sexual infantil (CSAM, por sus siglas en inglés).

Los que se oponen a la cifrado han enmarcado esto como un debate con dos bandos opuestos, cuando en realidad estamos unidos por una causa común contra los mismos adversarios. La cifrado protege a todos, incluidos los niños y otras poblaciones vulnerables.

Las empresas tecnológicas, incluidos los sitios de redes sociales y las aplicaciones de mensajería, no quieren ser espacios en los que se puedan conducir actividades delictivas ni tener material ilícito en sus plataformas.

Los autores de este documento creen que ha llegado el momento de replantear la conversación. Como tal, el gobierno y las fuerzas del orden deben adoptar un enfoque práctico y gradual de las políticas y la legislación que afectan a la aplicación de la ley y la seguridad en línea, en lugar de imponer una vigilancia omnipresente que pueda eludir la cifrado.

En este documento:

- Se examinará el debate histórico y los argumentos en torno a la política de cifrado;
- Se revisarán los temas recurrentes entre las propuestas en el contexto de las políticas y la legislación actuales;
- Se establecerá cómo debería desarrollarse el debate moderno sobre la cifrado; y
- Se abordarán los retos potenciales en caso de que el discurso permanezca inalterado.

## Sobre el *Center for Cybersecurity Policy & Law*

El *Center for Cybersecurity Policy & Law* es una organización independiente dedicada a mejorar la ciberseguridad en todo el mundo proporcionando a los gobiernos, la industria privada y la sociedad civil prácticas y políticas para gestionar mejor las amenazas a la seguridad. Establecido en 2017 como una organización sin fines de lucro 501 (c) (6) dentro del grupo de Servicios de Ciberseguridad de Venable LLP, el Centro combina la experiencia política con el poder de convocatoria a nivel mundial, nacional y local para reunir a los líderes de la industria con los responsables políticos a fin de formar coaliciones y lanzar iniciativas que produzcan resultados en el mundo real. Aplicando un enfoque orientado al consenso y basado en la gestión de riesgos, el Centro trata de desmitificar las complejidades y disipar la confusión en torno a la ciberseguridad mediante la promoción de soluciones pragmáticas y recomendaciones políticas extraídas de las perspectivas y prácticas de quienes están en primera línea en temas de seguridad de las infraestructuras digitales y los sistemas de información.

# Introducción

La tecnología está arraigada en nuestra vida cotidiana. Internet está literalmente al alcance de la mano, los teléfonos fijos han dado paso a las llamadas por FaceTime y las reuniones a través de Zoom, las cartas se han transformado en mensajes de texto y correos electrónicos, y los dispositivos portátiles ofrecen información en tiempo real sobre nuestra salud, con seguimiento de la frecuencia cardíaca, los niveles de azúcar en sangre y otros parámetros. Las tecnologías de la comunicación y la Internet de las cosas han ampliado nuestra realidad y nos mantienen conectados con nuestros amigos, familiares y comunidades, independientemente del lugar del mundo en el que nos encontremos. A medida que ampliamos el uso de estas tecnologías digitales, las empresas se esfuerzan por mantenerse impenetrables recurriendo normalmente a la cifrado o cifrado para proteger nuestros datos.

Junto a estos notables avances en nuestro panorama digital, los delincuentes y los actores malintencionados también utilizan estas tecnologías. Las instituciones responsables de proteger a la sociedad -las fuerzas del orden y los organismos de seguridad nacional- llevan décadas preocupadas porque los mecanismos de seguridad y cifrado de estas tecnologías les impiden hacer su trabajo, y culpan a las empresas tecnológicas.

Esto puede ser fácil de hacer: la privacidad y la seguridad están integradas en nuestras tecnologías, y cada vez se dan más por sentadas. El cifrado es fundamental para la protección de datos personales importantes. La propuesta de las fuerzas de seguridad ha sido sencilla: crear un sistema que permita acceder al material cifrado y escanear los mensajes para identificar el material dañino. Los funcionarios afirman que sus propuestas ayudarían a proteger a los niños, a mantener las drogas ilegales fuera de las calles, a prevenir la corrupción y, potencialmente, a disminuir  los delitos violentos. Sin embargo, estas soluciones excesivamente simplificadas podrían ser bastante peligrosas, al degradar la privacidad y exponer potencialmente a las personas a agentes malintencionados y curiosos. En cualquier caso, las fuerzas del orden y los responsables políticos siguen creando excepciones a medida que las plataformas avanzan hacia la incorporación del cifrado de extremo a extremo en la mensajería y el cifrado de datos en los dispositivos, pero esas propuestas no tienen debidamente en cuenta el importante papel que desempeña el cifrado en la seguridad de la vida digital de todos.

El cifrado es fundamental para mantener segura la información. Las empresas han estado utilizando el cifrado desde hace cincuenta años para proteger sus datos de filtraciones, así como para salvaguardar sus comunicaciones y operaciones, y muchos sectores (como la sanidad, los servicios financieros y la educación) tienen requisitos propios que cumplir para cifrar sus datos, ya sea por ley o a través de buenas prácticas y normas. Las fuerzas de seguridad, los militares y los funcionarios públicos también están de acuerdo en la importancia del cifrado y emplean las mismas herramientas y tecnologías para proteger sus propios sistemas y datos. Sin embargo, muchas de estas instituciones públicas quieren eludir el cifrado con el pretexto de proteger a los niños y la seguridad pública. Desgraciadamente, romper el cifrado para uno la rompería casi con toda seguridad para todos, incluidas las personas a las que ellos pretenden proteger.

Caracterizar el "debate sobre el cifrado" o la "la encriptoguerra" como un enfrentamiento de fuerzas opuestas no le hace justicia a los objetivos compartidos y a los intereses mutuos que lo sustentan. Las cuestiones clave de este polémico debate, en particular la lucha contra los abusos sexuales a menores y el asesinato de niños, así como los esfuerzos antiterroristas, persisten independientemente de los avances tecnológicos. Las actividades delictivas no son algo nuevo, son anteriores a Internet y al cifrado. Las empresas tecnológicas que gestionan plataformas de redes sociales y aplicaciones de mensajería no quieren que este tipo de material aparezca en sus plataformas y dedican considerables recursos a impedirlo[1]. Más allá de la

[1] https://www.thorn.org/blog/new-report-shows-an-increased-effort-by-tech-companies-to-detect-csam-on-the-internet/

superficie, una causa común une a estos bandos aparentemente opuestos: impedir que estos delitos se produzcan en primer lugar para proteger a los niños y al público.

A pesar de este compromiso compartido, los avances significativos hacia una solución común han seguido siendo esquivos. Es esencial reconocer que no existe una solución universal, una bala de plata ni una varita mágica capaz de erradicar estos problemas de la sociedad y, en algunos casos, las soluciones propuestas serían un arma de doble filo muy peligrosa.

Por ejemplo, una campaña reciente hace un llamamiento específico a los esfuerzos de Apple en torno a la detección de CSAM en iCloud, una plataforma de almacenamiento en la nube en línea. El anuncio de la valla publicitaria mostraba una imagen generada por inteligencia artificial de una niña con la cara disfrazada junto con el texto "El abuso sexual infantil se almacena en iCloud. Apple lo permite". Esto responde a la decisión de Apple de dejar de intentar desarrollar un sistema de protección de la privacidad y la seguridad para escanear las imágenes almacenadas en iCloud, estén o no cifradas de extremo a extremo, en busca de CSAM, pero no es exactamente la verdad del asunto.[2] Tras años de investigación, Apple determinó que "escanear los datos de iCloud almacenados de forma privada de cada usuario crearía nuevos vectores de amenaza que los ladrones de datos podrían encontrar y explotar. También crearía la posibilidad de una pendiente resbaladiza de consecuencias imprevistas. El escaneo de un tipo de contenido, por ejemplo, abre la puerta a la vigilancia masiva y podría crear el deseo de buscar en otros sistemas de mensajería cifrada a través de tipos de contenido".[3]

Y así, el debate sobre el cifrado persiste, plagado de complejidades y retos, con todas las partes buscando soluciones sencillas. No nos malinterpreten: el *Center for Cybersecurity Policy & Law* cree que la seguridad de los niños y del público es primordial, pero hay formas eficaces de combatir la delincuencia sin poner en peligro la privacidad y la seguridad de todas las demás organizaciones e individuos de los sectores público y privado. Sin embargo, no podemos permitir que lo perfecto se convierta en enemigo del progreso. Mientras debatimos posibles soluciones, no debemos perder de vista los pasos graduales que pueden mejorar la privacidad y la seguridad y salvaguardar nuestras comunidades. Las soluciones alternativas al cifrado están plagadas de problemas técnicos y políticos que harían muy difícil o aún imposible, su despliegue seguro. Creemos firmemente que hay formas de proteger la seguridad pública y la de los niños sin socavar la seguridad que protege todo el ecosistema digital y a todos los que lo utilizan.

## Los argumentos históricos en torno al cifrado

En la película *Sneakers* (1992), protagonizada por Robert Redford y Sidney Poitier, un criptógrafo construye un dispositivo capaz de romper cualquier esquema de cifrado y exponer a la vista cualquier cosa que estuviera oculta. Robert Redford, que había asumido una nueva identidad después de entrar en conflicto con la ley tras un incidente con el gobierno y ciertos temas de piratería informática, y su equipo son contratados para un trabajo que les lleva hasta aquel dispositivo y se les plantea entonces un dilema ético. Tienen en sus manos el poder de acceder a la información de cualquier sistema del mundo, pero ¿no es demasiado? Al final, el equipo de Redford decide que sí, y destruye el dispositivo, frustrando tanto a los malos como a los agentes de la ley que lo querían.

---

[2] "Apple's Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy", https://www.wired.com/story/apple-csam-scanning-heat-initiative-letter/

[3] Ibid.

La película ha entretenido al público durante más de 30 años, pero el enigma en el que se basa se ha debatido durante siglos, ya que la criptografía se ha empleado para la diplomacia, el espionaje y las guerras. A lo largo de la historia, el uso de códigos secretos y cifras ha sido esencial para mantener la seguridad de las comunicaciones y preservar la información sensible. Se han ganado y perdido guerras y se han evitado crímenes. Sin embargo, su uso pone de relieve la necesidad de impedir que las amenazas o adversarios potenciales exploten las mismas herramientas y tecnologías para actividades ilícitas.

Los argumentos contra el cifrado digital moderno son anteriores a la existencia de la Internet pública y desempeñaron un papel importante en la Guerra Fría. Tras la Segunda Guerra Mundial, Estados Unidos impuso controles a la exportación de tecnologías de cifrado para la comunicación, prohibiendo la exportación de tecnologías de cifrado muy potentes. Al igual que Estados Unidos, muchos países europeos impusieron inicialmente estrictos controles a la exportación de tecnologías de cifrado más potentes, por considerarlas “armas” de doble uso que podrían tener aplicaciones militares[4]. Esto tuvo cierto éxito, pero en general dio lugar al uso de un cifrado débil en todo el mundo, incluido los Estados Unidos.[5]

En la década de los 90, el debate sobre el cifrado evolucionó. Con el lanzamiento de la Internet comercial y el uso generalizado de los ordenadores personales -especialmente para las transacciones financieras- el cifrado se generalizó. El FBI y la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) empezaron a luchar públicamente contra el uso del cifrado de extremo a extremo en las comunicaciones[6]. En 1993, propusieron un dispositivo que permitía al gobierno acceder a las comunicaciones cifradas, llamado Clipper Chip[7]. El chip utilizaría *key escrow*, un concepto que permite a un tercero -en este caso, el gobierno- acceder a una clave de descifrado para leer ese contenido cifrado. Al final se impuso un diseño deficiente e inseguro, unido a la indignación de los defensores de las libertades civiles y la privacidad, por lo que los teléfonos actuales no llevan ningún chip que permita a las fuerzas de seguridad escuchar las conversaciones.

En 1996, treinta y nueve países firmaron el Arreglo de Wassenaar sobre el control de las exportaciones, incluidas las tecnologías de doble uso; las formas menos seguras de cifrado dejaron entonces de estar controladas de manera previa a su exportación en virtud del acuerdo[8]. En Estados Unidos, la Ley de Seguridad y Libertad mediante el Cifrado (SAFE por sus siglas en inglés) intentó resolver los problemas creados por las políticas de la época de la Guerra Fría. Durante décadas, los productos de cifrado fuerte estuvieron estrictamente regulados, impidiendo su venta en el extranjero o exigiendo la exportación de versiones más débiles "aptas para la exportación". La legislación bipartidista subrayaba la necesidad de equilibrar la seguridad nacional con el avance tecnológico y los derechos individuales. Las empresas de software argumentaban que los controles de exportación existentes ahogaban la innovación, y las pruebas demostraban que las políticas vigentes desde hacía décadas eran ineficaces y tenían un efecto negativo en la economía estadounidense[9]. Aunque la Ley SAFE no se convirtió en ley, en otoño de 1999, la Administración Clinton adoptó una política que aplicaba casi todas las

---

[4] https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220, https://www.sciencedirect.com/science/article/abs/pii/B9780444516084500274?via%3Dihub

[5] “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications”, http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8

[6] “The state of encryption: How the debate has shifted”, https://opensource.com/article/18/6/listening-susan-landau

[7] “The Short Life and Humiliating Death of the Clipper Chip”, https://gizmodo.com/life -and-death-of-clipper-chip-encryption-backdoors-att-1850177832

[8] https://www.armscontrol.org/factsheets/wassenaar

[9] https://slate.com/technology/2015/06/safe-act-the-right-to-strong-encryption-almost-became-law-in-the-90s.html

disposiciones del proyecto de ley, incluida la eliminación de las restricciones a la exportación de productos de cifrado al por menor[10].

En respuesta a estos cambios políticos globales, la NSA comenzó a trabajar en secreto para debilitar los estándares de cifrado que subyacen a un cifrado fuerte, creando una puerta trasera sin escrutinio público[11]. En 2006, la NSA había obtenido acceso a las comunicaciones de tres aerolíneas, un sistema de reservas de viajes, el departamento nuclear de un gobierno extranjero y el servicio de Internet de otro gobierno mediante el crackeo de sus redes privadas virtuales. Esto salió a la luz con las revelaciones de Snowden de 2013, en las que se documentaba cómo la agencia de espionaje había obtenido acceso a comunicaciones cifradas, poniendo en peligro los números aleatorios utilizados para generar claves de cifrado[12].

Un informe técnico de 2015 del Instituto Tecnológico de Massachusetts (MIT por sus siglas en inglés) dejó en claro que permitir este acceso a contenidos cifrados a principios de la década de 2000 fue problemático, y que sería significativamente peor en la actualidad debido a cómo ha evolucionado y crecido la importancia de la Internet[13]. "La complejidad del entorno actual de Internet, con millones de aplicaciones y servicios conectados globalmente podría demandar nuevos requisitos establecidos por ley que introduzcan fallos de seguridad imprevistos y difíciles de detectar", afirma el informe. "Más allá de estas y otras vulnerabilidades técnicas, la perspectiva de sistemas de acceso excepcional desplegados a escala mundial plantea problemas difíciles sobre cómo se gobernaría ese entorno y cómo garantizar que esos sistemas respeten los derechos humanos y el Estado de Derecho."

Mientras la NSA pasaba a explotar las vulnerabilidades de la red como medio para acceder a la información, el FBI se mantenía al frente de la siguiente lucha contra el cifrado. En 2015, líderes políticos y de las fuerzas de seguridad del Reino Unido y Estados Unidos volvieron a manifestarse en contra del cifrado, alegando que amenazaba la capacidad de las fuerzas de seguridad para investigar delitos[14].

El argumento volvió a la palestra tras el tiroteo masivo de San Bernardino (California). El FBI pidió a los tribunales que obligaran a Apple a descifrar el PIN del iPhone del autor del tiroteo -que descifra el dispositivo- para seguir pistas adicionales, pero la empresa tecnológica se negó[15]. Al final, el FBI encontró una tercera empresa que pudo desbloquear el dispositivo, lo que volvió a plantear la idea de los gobiernos utilizando “puertas traseras” para acceder a mensajes y dispositivos. En su momento se propuso legislación al respecto, pero ninguna avanzó. Este tal vez fue el caso más sonado en el que se intentó obligar a Apple a descifrar un dispositivo, pero no fue el único: hubo al menos cinco intentos señalados por Apple, ninguno de los cuales prosperó[16],[17]. Cuando el FBI consiguió acceder al dispositivo, no encontró ninguna información nueva[18].

---

[10] https://www.govinfo.gov/content/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2399.pdf

[11] https://www.brookings.edu/articles/a-brief-history-of-u-s-encryption-policy/

[12] https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2&_r=2

[13] “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications,” http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8

[14] Ibid

[15] “A Year After San Bernardino And Apple-FBI, Where Are We On Encryption?” https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption

[16] https://www.justsecurity.org/wp-content/uploads/2016/03/Apple-All-Writs-Apple-Requests-Received-Letter.pdf

[17] https://www.theguardian.com/technology/2016/feb/23/apple-new-iphone-models-san-bernardino-shooter-all-writs-act-department-of-justice

[18] https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads

## Temas recurrentes y política y legislación actuales

A lo largo de los debates sobre temas de cifrado, han surgido varias propuestas sobre puertas traseras y puertas delanteras en los algoritmos de cifrado, y sobre considerar ilegal el uso de un cifrado fuerte.

| Propuesta | Retos |
|---|---|
| **Acceso Mediado (Key Escrow):** Método en el que las claves de cifrado son custodiadas por un tercero de confianza, lo que permite a las fuerzas de seguridad acceder a los datos cifrados cuando se cumplen determinadas condiciones. | La seguridad y fiabilidad de terceros podría generar riesgos innecesarios (por ejemplo, uso indebido, acceso no autorizado).<br>Los poseedores de claves podrían convertirse en objetivos de ataques eventualmente catastróficos.<br>El acceso rápido a los datos es difícil cuando las claves deben recomponerse o transferirse. |
| **Acceso no Mediado:** El despliegue de herramientas y técnicas por parte de las fuerzas de seguridad para acceder a datos cifrados sin la participación de los propietarios o procesadores de datos. | Las puertas traseras utilizadas por las fuerzas de seguridad también pueden ser explotadas por agentes malintencionados o utilizadas indebidamente para usos no autorizados.<br>El acceso a los datos sin el conocimiento o consentimiento de los interesados podría plantear diversos problemas de privacidad, violación de derechos civiles o libertades personales. |
| **Asistencia Técnica:** El proceso mediante el cual una empresa especializada puede verse obligada a ayudar a las fuerzas de seguridad a acceder a datos cifrados debilitando el cifrado o creando herramientas para descifrar los datos. | La creación de herramientas o puertas traseras debilita los sistemas, haciéndolos más vulnerables a los ataques.<br>Las empresas tecnológicas pueden perder la confianza de sus usuarios si éstos creen que sus productos cuentan con sistemas de seguridad debilitados intencionadamente para el cumplimiento de la ley.<br>Las empresas tecnológicas pueden tender a crear sistemas más débiles por defecto en previsión de los requisitos de cumplimiento. |

Las propuestas de los últimos años han cambiado la forma en que las fuerzas de seguridad y los gobiernos intentan abordar estos ataques de cifrado, pero no han modificado su impacto potencial.

## La Ley de Seguridad en Línea del Reino Unido

En septiembre de 2023, el Reino Unido aprobó su Ley de Seguridad en Línea[19], que está diseñada para mantener los sitios web y otros servicios basados en Internet libres de material ilegal y dañino. La ley se aplica a un amplio conjunto de proveedores de servicios en línea, incluidos motores de búsqueda, plataformas de redes sociales, anfitriones de contenidos generados por usuarios, foros en línea, juegos y sitios de pornografía[20].

Aunque la ley no prohíbe explícitamente el cifrado de extremo a extremo, exigiría el filtrado de contenidos y la verificación de la edad mediante tecnologías aprobadas por el gobierno. La propuesta también incluía una disposición que obligaría a las empresas tecnológicas que proporcionan mensajería cifrada de extremo a extremo a escanear el contenido de los mensajes en busca de CSAM para poder denunciarlo a las autoridades[21]. Aunque las empresas tecnológicas se opusieron enérgicamente, una enmienda adicional incluida en la ley aprobada establece que no se exigirá a las empresas que analicen los mensajes cifrados hasta que sea "técnicamente viable y se haya acreditado que la tecnología cumple unas normas mínimas de precisión para detectar únicamente contenidos de abuso y explotación sexual infantil"[22]. Sin embargo, la historia

[19] https://bills.parliament.uk/bills/3137

[20] "UK's controversial online safety bill set to become law," https://www.computerworld.com/article/3706810/uks-controversial-online-safety-bill-set-to-become-law.html

[21] https://www.gov.uk/government/publications/end-to-end-encryption-and-child-safety/end-to-end-encryption-and-child-safety

[22] https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email

de la política de cifrado muestra que existen opiniones muy divergentes entre las fuerzas de seguridad, las empresas tecnológicas y los tecnólogos sobre lo que es técnicamente viable en este frente.

Signal, la popular aplicación de mensajería, ha declarado que dejará de operar en el mercado británico si se exigen puertas traseras de cifrado[23]. El Ministerio del Interior británico también ha iniciado una campaña contra el despliegue por parte de Meta del cifrado de extremo a extremo para Facebook e Instagram, utilizando un lenguaje gráfico para describir el CSAM que creen que podría pasar sin ser detectado. En un vídeo aparece una víctima de abuso sexual infantil apelando directamente a Mark Zuckerberg, jefe de Meta, para que reconsidere sus planes de implantar el cifradp[24]. Tras la aprobación de la Ley de Seguridad en Línea, y a pesar de las presiones del Ministerio del Interior británico para que no lo hiciera[25], Meta puso en marcha a finales de año el cifrado de extremo a extremo para Messenger[26], uniéndose a su producto WhatsApp cifrado a finales de año, y seguirá vigilando sus plataformas para detectar la captación de menores y el intercambio de contenidos de abusos a menores utilizando métodos que no requieran que se espíen todos los mensajes de su plataforma[27].

## Ley Australiana de Asistencia y Acceso a las Telecomunicaciones

El Reino Unido no está solo en su intento de frenar el uso del cifrado a través de la legislación. Australia aprobó la Ley de Asistencia y Acceso a las Telecomunicaciones en 2018 para equipar a las fuerzas de seguridad y los organismos de inteligencia con las herramientas necesarias que les permitiese operar eficazmente en la era digital y hacer frente al terrorismo y la delincuencia[28], pero ha sido ampliamente descrita como un ataque al cifrado[29].

La Ley aumentó las responsabilidades de los proveedores de servicios de comunicación, las empresas o los individuos involucrados en la fabricación de equipos, el desarrollo o la actualización de software, o la operación de sitios web para cooperar con las agencias policiales y de seguridad. También creó órdenes de acceso informático para las fuerzas de seguridad y reforzó la autoridad de registro e incautación de las agencias de seguridad para acceder a datos basados en cuentas mediante una orden de registro y a datos no cifrados en ordenadores y dispositivos móviles[30].

Entre los mecanismos clave de la Ley se incluyen las solicitudes voluntarias y obligatorias de acceso excepcional a los datos, así como una disposición para exigir a las organizaciones que proporcionen asistencia que incluya el desarrollo de nuevas capacidades, lo que podría incluir la ruptura de su propio cifrado, su degradación o la construcción de puertas traseras[31].

La ley ha recibido continuas críticas de las empresas tecnológicas, los defensores de la privacidad y el público en general por la rapidez de su aprobación, la falta de transparencia y un proceso de consulta deficiente. Aunque las salvaguardias incorporadas a la ley garantizan que nada puede obligar a la industria a romper el cifrado, los críticos sostienen que la capacidad de la ley

---

23 https://twitter.com/mer edith/status/1704477739871273397

24 https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email

25 https://www.reuters.com/technology/uk-urges-meta-not-roll-out-end-to-end-encryption-messenger-instagram-2023-09-19/

26 https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/

27 https://www.theguardian.com/technology/2023/jun/07/meta-instagram-self-generated-child-sexual-abuse-materials

28 https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

29 https://www.eff.org/deeplinks/2018/12/new-fight-online-privacy-and-security-australia-falls-what-happens-next

30 https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/

31 https://www.abc.net.au/news/2018-12-04/encryption-whatsapp-signal-messages-explained/10580208

para obligar a las empresas a crear nuevas posibilidades de acceso puede utilizarse para forzarlas a debilitar el cifrado o a construir puertas traseras. Al comprometer la seguridad de la información de los australianos, la ley podría tener repercusiones de gran alcance, poniendo en peligro la información de empresas y personas de todo el mundo.

Hasta junio de 2020, no se había emitido ninguna orden obligatoria y se habían redactado menos de 20 solicitudes de asistencia32.

## Otras propuestas

Los gobiernos de todo el mundo están adoptando distintos enfoques en materia de cifrado. A continuación se ofrece una tabla de políticas y leyes propuestas y aprobadas en todo el mundo, con resúmenes y posibles implicaciones.

| País | Norma | Resumen | Implicaciones para el cifrado |
|---|---|---|---|
| India | Sección 69A de la Ley de Tecnología de la Información de 2000 (aprobada) | En virtud de esta ley, el gobierno indio tiene autoridad para ordenar a los intermediarios en línea, incluidos los proveedores de servicios de Internet (ISP por sus siglas en inglés) y los proveedores de servicios de telecomunicaciones, que bloqueen contenidos o información que se consideren una amenaza para la seguridad nacional[33]. | A principios de este año, el gobierno indio aprovechó este estatuto para prohibir 14 aplicaciones de mensajería cifrada por permitir supuestamente la comunicación entre terroristas, bloqueando el acceso a todo el país. |
| Unión Europea | Reglamento para Prevenir y Combatir el Abuso Sexual Infantil (propuesta de Reglamento sobre abuso sexual infantil, o CSAR) | Esta propuesta exigía inicialmente a los proveedores que detectaran, notificaran y eliminaran el CSAM en sus servicios. Estas normas obligarían a los proveedores de servicios a escanear proactivamente sus servicios en busca de CSAM y captación de menores, incluidos los mensajes cifrados[34]. La Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento Europeo votó a favor de eliminar esta disposición y permitir únicamente la vigilancia selectiva[35]. | Una evaluación de impacto realizada por el Parlamento Europeo llegó a la conclusión de que la propuesta inicial socavaría el cifrado de extremo a extremo y la seguridad de las comunicaciones digitales, y probablemente incumpliría el precedente del Tribunal de Justicia de la Unión Europea por el que el cribado de todos los metadatos de las comunicaciones no se considera ni proporcionado ni necesario[36].<br><br>El Parlamento adoptó posteriormente un texto que excluía el cifrado de extremo a extremo del ámbito de aplicación de las órdenes de detección y aclaraba que sólo debería utilizarse si otras medidas paliativas no resultaban eficaces; el texto final sólo permite la vigilancia selectiva[37]. |

32 https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/30904d8b-7cfb-4ef0-99fb-fba2299b57bf/&sid=0000

33 https://tutanota.com/blog/posts/apps-banned-india

34 https://cyberlaw.stanford.edu/blog/2023/06/eu-member-states-still-cannot-agree-about-end-end-encryption

35 https://edri.org/our-work/csar-european-parliament-rejects-mass-scanning-of-private-messages/

36 European Parliament. (2023, April). Complementary impact assessment - Proposal for a regulation laying down the rules to prevent and combat child sexual abuse, https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf

37 https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass- surveillance

| | | | |
|---|---|---|---|
| Reino Unido | Enmiendas a la Ley de Regulación de los Poderes de Investigación (IPA por sus siglas en inglés) | La IPA impone amplios requisitos con respecto al acceso extraordinario, y la actualización incluye la capacidad de aprobar previamente o bloquear nuevas tecnologías de seguridad que puedan afectar al mercado mundial[38]. | La actual IPA aparentemente permite al gobierno británico alterar sus servicios para todos los usuarios, incluso para debilitar, limitar o introducir por la puerta trasera el cifrado. También exige a las empresas que notifiquen al gobierno antes de modificar aquellos servicios que puedan afectar ciertas investigaciones, incluida la introducción de funciones de seguridad como el cifrado de extremo a extremo[39] |
| United States | Ley de Eliminación de la Negligencia Abusiva y Rampante de las Tecnologías Interactivas (Ley EARN IT) | Esta legislación pretende hacer frente a la explotación infantil mediante la creación de una Comisión Nacional para la Prevención de la Explotación Sexual Infantil en Internet, la modificación del artículo 230 de la Ley de Decencia en las Comunicaciones para eliminar las protecciones a los proveedores de servicios y el refuerzo de la aplicación de las leyes vigentes sobre explotación sexual infantil[40]. | La Ley EARN IT incentiva a los proveedores de servicios a eliminar el cifrado de extremo a extremo o a crear puertas traseras, lo que introduce vulnerabilidades para todos los usuarios, incluidos los niños y otros grupos vulnerables.<br>Además hay que considerar el eventual carácter político de las mejores prácticas que desarrolle la Comisión, ya que la mayoría de los miembros propuestos son nombrados por los líderes del Congreso. |

## Replanteando el debate moderno sobre el cifrado

La Fundación Carnegie para la Paz Internacional, la Universidad de Princeton y el Centro de Política Tecnológica Internacional formaron el Grupo de Trabajo sobre Cifrado para analizar en profundidad el debate sobre el cifrado con el objetivo de encontrar nuevos enfoques. En 2019 publicaron *"Moving the Encryption Policy Conversation Forward"*[41]. El Grupo propone formas más fructíferas de evaluar el impacto social del cifrado, incluidos tanto los beneficios como los riesgos de cualquier enfoque propuesto que aborde el punto muerto en el que se encuentra el acceso de las fuerzas de seguridad a los datos cifrados. El documento se sumerge específicamente en el cifrado de teléfonos móviles y detalla un enfoque más específico para evaluar las propuestas centradas en el acceso de las fuerzas de seguridad.

El documento de Carnegie -que aborda el tema de forma imparcial y con la participación de múltiples partes interesadas- comienza rechazando los dos argumentos principales a favor y en contra del cifrado, a saber:

1. Las fuerzas del orden deben dejar de buscar enfoques que permitan el acceso a la información cifrada.

2. Las fuerzas del orden no podrán proteger al público a menos que puedan obtener acceso a todos los datos cifrados mediante un procedimiento legal.

En última instancia, el grupo llegó a la conclusión de que hay que seguir trabajando y que es en el cifrado de teléfonos móviles donde se puede avanzar. Las conclusiones fueron las siguientes:

---

[38] https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-overview#what-does-the-investigatory-powers-amendment-bill-do

[39] https://www.justsecurity.org/87615/changes-to-uk-surveillance-regime-may-violate-international-law/

[40] https://tutanota.com/blog/posts/earn-it-barr-encryption

[41] https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

- El debate sobre el cifrado de datos en reposo en los teléfonos móviles probablemente abrirá la discusión entre diversas comunidades de interés y permitirá identificar más claramente los riesgos y beneficios.
- No hay indicios de que las propuestas existentes en este ámbito sean viables, ni de que lo vayan a ser en el futuro, como tampoco de que sea aconsejable modificar las políticas en este momento.
- Si no puede haber un debate de buena fe con todas las partes sobre este tema general de cifrado, es probable que éste no surja en ninguna otra parte.

Un primer paso clave es identificar un terreno común. Hay elementos de este debate en los que creemos que todos podemos estar de acuerdo.

*El cifrado es la mejor defensa que tienen la mayoría de las organizaciones para proteger sus datos y demostrar que las personas son quienes dicen ser.* Y aunque se han producido y seguirán produciéndose importantes filtraciones de datos -que comprometen números de la Seguridad Social, información de tarjetas de pago y otros datos personales-, el cifrado se mantiene como la mejor medida para proteger la información[42]. Por el contrario, si los delincuentes saben que existe un almacén de claves, o que un algoritmo de cifrado tiene una puerta que pueden desbloquear, eso resultará ser un punto muy atractivo para los delincuentes, que harán todo lo posible por desbloquearlo y utilizarlo para sus propios fines.

*El cambio gradual será la clave para avanzar.* Los debates anteriores se han caracterizado por soluciones demasiado simplificadas. El debate moderno sobre el cifrado debe reconocer cómo los rápidos avances de la tecnología harán que abordar la complejidad y la interoperabilidad de estos sistemas sea un objetivo constantel. "Para lograr un acceso excepcional generalizado, las nuevas funciones tecnológicas tendrían que desplegarse y probarse literalmente con cientos de miles de desarrolladores de todo el mundo", afirma el informe del MIT. "Se trata de un entorno mucho más complejo que la vigilancia electrónica desplegada actualmente en las telecomunicaciones y los servicios de acceso a Internet, que suelen utilizar tecnologías similares y es más probable que dispongan de los recursos necesarios para gestionar las vulnerabilidades que puedan surgir de las nuevas funciones." El gran número de productos y servicios que utilizan el cifrado y sirven para transmitir o almacenar contenidos ha incrementado la complejidad de cualquier intento de acceso excepcional.

*Proverbialmente, el enemigo de mi enemigo es mi amigo.* Las empresas tecnológicas, incluidos los sitios de redes sociales y las aplicaciones de mensajería, no quieren ser conductos de actividades delictivas ni tener material ilícito en sus plataformas. Los operadores de estas plataformas y servicios trabajan para evitar la difusión de CSAM y otros contenidos ilegales en las jurisdicciones en las que operan. Sin embargo, el cumplimiento de la ley no es la única razón por la que trabajan para detectar y eliminar estos contenidos: las organizaciones también están protegiendo al resto de sus usuarios, a la sociedad y la confianza en su negocio.

*Los gobiernos y las fuerzas del orden deben adoptar un enfoque práctico y mesurado de las políticas y la legislación que afectan al cifrado para evitar consecuencias imprevistas.* Habilitar cualquier tipo de puerta trasera para el gobierno o las fuerzas de seguridad haría que la Internet fuera más compleja, dando lugar a vulnerabilidades adicionales y abonando un espacio cada vez más inseguro[43]. Si eventualmente las credenciales para acceder a estas puertas se corrompieran, sería devastador, ya que daría a los atacantes la capacidad de acceder y descifrar la misma información a la que pueden acceder

[42] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[43] https://defense360.csis.org/bad-idea-encryption-backdoors/

las fuerzas de seguridad.

Los autores de este documento creen que ha llegado el momento de replantear la conversación. El debate sobre el cifrado de datos se ha enmarcado en dos bandos opuestos, cuando en realidad estamos luchando contra los mismos enemigos. Es imperativo que nos centremos en el progreso gradual. El resto de este documento abordará los retos potenciales en caso de que el discurso permanezca inalterado.

## Gobernando a los gobiernos

Los tecnólogos están de acuerdo en que permitir el acceso a contenidos cifrados sin afectar significativamente a la seguridad es casi imposible, pero al reto técnico se sumarían los retos de gobernanza de un sistema de acceso excepcional de este tipo[44]. Existen innumerables leyes, muchas jurisdicciones y multitud de partes interesadas que poner sobre la mesa, cada una de las cuales aporta perspectivas valiosas, aunque a menudo contradictorias. Establecer una estructura de gobernanza global para el acceso excepcional a los contenidos cifrados exigiría conciliar desacuerdos, como por ejemplo quién debe sentarse a la mesa, los fines legítimos para acceder a los datos cifrados o plazos realistas para que las partes interesadas atiendan una solicitud o compartan contenidos de forma proactiva.

Resolver incluso una de estas cuestiones dentro de las fronteras de un solo país es una tarea difícil. Por ejemplo, permitir que cientos o miles de agentes de la ley y personal de las agencias dentro de EE.UU. accedan y descifren las comunicaciones de forma segura sería enormemente difícil. Tal vez podría crearse un centro de intercambio de información centralizado gestionado por el FBI que actuara como mecanismo de coordinación, y construirse mecanismos judiciales para permitir su uso por parte de las fuerzas de seguridad federales, estatales y locales. Podrían diseñarse sistemas de respuesta rápida en los que las empresas emplearan a un gran número de personal para dar soporte a los sistemas de acceso excepcional, reduciendo el cifrado o intentando mantener la seguridad del propio sistema de acceso excepcional. Las empresas o los organismos de supervisión pueden enfrentarse a importantes retos a la hora de realizar un seguimiento preciso de cuándo, quién y en qué circunstancias se accede a los datos de los clientes, especialmente si las demandas de datos van acompañadas de órdenes de silencio.

Esta complejidad no haría sino agravarse a escala internacional, ya que la cuestión de quién puede gestionar cada solicitud podría no tener una respuesta tan sencilla. Esto ha llevado a varias empresas a decir que dejarán de hacer negocios en determinados países si las soluciones alternativas al cifrado se convierten en ley[45].

Además, la gobernanza tendría que abordar cómo se gestionarían las credenciales y las herramientas de acceso. Habría que promulgar políticas y procedimientos estrictos para que los funcionarios no utilicen el sistema para algo que no deberían[46]. Con los diversos programas de vigilancia de la NSA dirigidos a la información de los usuarios de muchas de las principales empresas tecnológicas y de otras fuentes, incluso los analistas de bajo nivel podrían acceder a la información sin ningún tipo de supervisión. La agencia incluso tenía un nombre para ello: LOVEINT, en el que los empleados utilizaban estas herramientas para vigilar a sus parejas, cónyuges y otras personas que no estaban sujetas a vigilancia[47]. Más recientemente, un tribunal estadounidense concluyó que el FBI buscó indebidamente información en una base de datos estadounidense de inteligencia extranjera 278.000 veces a lo largo de varios años, incluso sobre estadounidenses sospechosos de delitos[48].

---

[44] https://www.accessnow.org/secure-the-internet/

[45] https://www.theverge.com/23409716/signal-encryption-messaging-sms-meredith-whittaker-imessage-whatsapp-china

[46] https://www.newyorker.com/news/amy-davidson/america-through-the-n-s-a-s-prism

[47] https://slate.com/technology/2013/09/loveint-how-nsa-spies-snooped-on-girlfriends-lovers-and-first-dates.html

[48] https://www.reuters.com/world/us/fbi-misused-intelligence-database-278000-searches-court-says-2023-05-19/

Y los gobiernos no son inmunes a sus propias brechas, como demuestra Shadow Brokers, una persona o grupo que ha filtrado un gigabyte de exploits de software de la NSA[49]. Esta brecha incluía exploits y herramientas de jaqueo dirigidas a la mayoría de las versiones de Microsoft Windows y pruebas de sofisticados jaqueos en el sistema bancario SWIFT de varios bancos de todo el mundo. También hay otros ejemplos significativos, como la filtración de 21,5 millones de registros personales de la Oficina de Gestión de Personal de Estados Unidos, los registros de 76 millones de militares de los Archivos Nacionales y la Administración de Registros de Estados Unidos, la filtración de datos de los números Aadhar de India, la Agencia Sueca de Transporte y la base de datos de votantes de Estados Unidos, entre muchos otros[50].

## Las puertas traseras de cifrado podrían utilizarse para perseguir a poblaciones vulnerables

De la mano de la gobernanza está la preocupación de que las puertas traseras de cifrado puedan ser explotadas por quienes ocupan puestos de autoridad para oprimir a opositores políticos, grupos religiosos y otras minorías. El cifrado desempeña un papel crucial en la protección de la libertad de expresión de las poblaciones vulnerables, incluidos los disidentes en países autoritarios o las poblaciones perseguidas. Muchas empresas tecnológicas han optado históricamente por no cumplir las exigencias con implicaciones para los derechos humanos. Por ejemplo, la entrega de datos sobre la sexualidad de los usuarios o su actividad o afiliación política puede acarrear importantes sanciones. En Estados Unidos, los legisladores sostienen que debe concederse el acceso a las fuerzas de seguridad si éste es relevante para un delito, pero en otros países, este acceso podría conducir a abusos de los derechos humanos.

Hay varias opciones para las empresas tecnológicas en lo que respecta a los mandatos de puerta trasera. Podrían tratar a todos los gobiernos de la misma manera, lo que podría convertirlas en cómplices de abusos contra los derechos humanos. O podrían evaluar cada solicitud caso por caso, sin información completa y eventualmente facilitando la comisión de abusos contra los derechos humanos[51].

Los argumentos históricos contra el cifrado se centran en la lucha contra la delincuencia, especialmente aquella que sufren las poblaciones más vulnerables. Sin embargo, estos argumentos también se han utilizado internacionalmente para silenciar a los opositores políticos[52]. A principios de este año, en virtud de la Ley de Tecnología de la India, se prohibieron 14 aplicaciones de mensajería en el país bajo el pretexto de que habían sido utilizadas por terroristas[53]. La prohibición se produjo sin audiencia ni notificación por parte del gobierno indio, lo que sorprendió a los operadores de las plataformas.

Representantes de las Naciones Unidas se han pronunciado a favor del cifrado por considerarlo fundamental para proteger a las personas que puedan ser objetivo de regímenes opresivos. "Las herramientas de cifrado son ampliamente utilizadas en todo el mundo, incluso por los defensores de los derechos humanos, la sociedad civil, los periodistas, los denunciantes de irregularidades y los disidentes políticos que se enfrentan a la persecución y el acoso", dijo Zeid Ra'ad Al Hussein, Alto Comisionado de la ONU para los Derechos Humanos en 2016[54]. "El cifrado y el anonimato son necesarios como facilitadores tanto de la libertad de expresión y de opinión, como del derecho a la privacidad. No es ni fantasioso ni exagerado afirmar que, sin herramientas de cifrado, se pueden poner vidas en peligro. En el peor de los casos, la capacidad de un gobierno para entrar en los teléfonos de sus ciudadanos puede llevar a la persecución de personas que simplemente están ejerciendo sus derechos

---

[49] https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

[50] https://www.executech.com/insights/the-5-scariest-data-breaches-in-government/

[51] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[52] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[53] https://internetfreedom.in/14-mobile-apps-banned/

[54] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf

humanos fundamentales".

El cifrado permite comunicarse libremente a quienes podrían ser blanco de ataques. Según un informe de Amnistía Internacional de 2016, "solo protegiendo las comunicaciones frente a injerencias externas podrán los usuarios de Internet, los defensores de los derechos humanos, los políticos de la oposición, los activistas políticos y los periodistas de investigación protegerse de la ciberdelincuencia y de las miradas indiscretas de gobiernos de todo el mundo[55]".

## El rol de las empresas tecnológicas como fuerzas de seguridad

En los últimos años, la conversación ha pasado de la necesidad de una puerta trasera de cifrado por parte de las fuerzas de seguridad a la necesidad de que las empresas tecnológicas analicen los mensajes para asegurarse de que no se transmite material dañino. Si lo encuentran, deberán notificarlo a las autoridades competentes. Este es el núcleo de la legislación propuesta y aprobada más recientemente, y sitúa a las empresas tecnológicas en el papel de facto de las fuerzas de seguridad.

En 2021, Australia amplió y reforzó las protecciones existentes mediante la Ley de Seguridad en Línea, que introdujo las Expectativas Básicas de Seguridad en Línea[56] para los proveedores de servicios en línea y exigió códigos obligatorios del sector para los contenidos ilegales y restringidos[57]. Más recientemente, el gobernador de California, Gavin Newsom, firmó en octubre una ley que penalizará a los servicios por su papel en "facilitar, ayudar o instigar a sabiendas la explotación sexual comercial" de los niños[58]. La Unión Europea también quiere que las plataformas de mensajería escaneen mensajes en busca de CSAM, pero ha excluido el cifrado de extremo a extremo del alcance de las órdenes de detección basándose en la preocupación de promover la vigilancia extrema por parte de estas plataformas[59].

La legislación y las políticas han intentado encontrar el equilibrio entre la necesidad de las fuerzas de seguridad de acceder a la información, y la seguridad y privacidad, animando a las empresas tecnológicas a ser más proactivas a la hora de identificar dónde puede haber CSAM y otras actividades ilegales. Como resultado, las empresas tecnológicas se ven atrapadas en medio de legisladores y responsables políticos que les piden que protejan sus productos digitales y los datos que almacenan de los usuarios, al tiempo que brindan acceso a más datos a las fuerzas de seguridad y los servicios de inteligencia.

"Los legisladores se han embarcado en la desaconsejable misión de cortar por la mitad al bebé del cifrado", escribieron Tarah Wheeler y Geoffrey Cain en un blog para el *Council on Foreign Relations*[60]. "Están exigiendo un conjunto de excepciones legales que permitirían a la policía entrar en tu hogar digital por la puerta de atrás, mientras preservan las férreas puertas delanteras del cifrado para todos los demás". Pero no es realista creer que otros no buscarán también puertas traseras.

Estas supuestas vías intermedias permitirían a las empresas tecnológicas preservar el cifrado de extremo a extremo e identificar al mismo tiempo contenidos potencialmente nocivos. Sin embargo, los expertos creen que estas tecnologías de

---

55 https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-_a_matter_of_human_rights_-_def.pdf

56 https://www.esafety.gov.au/industry/basic-online-safety-expectations

57 https://www.esafety.gov.au/newsroom/whats-on/online-safety-act

58 https://www.firstpost.com/tech/news-analysis/californias-governor-signs-ban-penalising-social-media-platforms-for-aiding-or-abetting-child-abuse-13229372.html

59 https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass- surveillance

60 https://www.cfr.org/blog/theres-cop-my-pocket-policymakers-need-stop-advocating-surveillance-default

escaneado del lado del cliente "atentarían contra las garantías de privacidad y seguridad del usuario que ofrece el cifrado"[61]. Incluso quienes han construido un prototipo funcional para encontrar CSAM en servicios cifrados de extremo a extremo creen que estas tecnologías son peligrosas[62]. Estos sistemas de escaneado pueden reutilizarse fácilmente para la vigilancia y la censura, y las peticiones a empresas tecnológicas de todo el mundo han demostrado el deseo de atacar a disidentes políticos, minorías religiosas y otros.

Tal vez lo primero a considerar sería que los gobiernos no deberían poner a las empresas tecnológicas en situaciones en las que se les asignen funciones policiales[63]. Pedir a las empresas que se pongan en la piel de las fuerzas de seguridad es desdibujar una línea importante y coloca a los empleados en una posición en la que habrá inherentemente conflictos de intereses entre sus deberes con los usuarios, con sus empresas y con los gobiernos. Y si se delega en la empresa y se le exige que realice este tipo de investigación, y con ello contribuye a causar daños o a violar derechos, no está claro quién tendrá que rendir cuentas.

## El cifrado no es la única forma de atrapar delincuentes

A pesar de los repetidos llamamientos para romper el cifrado, no está claro que irrumpir en los dispositivos y mensajes cifrados sea la mejor manera de atrapar delincuentes. En 2018, el Centro de Estudios Estratégicos e Internacionales (CSIS por sus siglas en inglés) publicó *"Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge"*[64]. El informe afirma que, si bien las preocupaciones del gobierno y las fuerzas de seguridad sobre el cifrado que impide las investigaciones criminales son válidas en algunos casos, no existe una solución única y directa. De hecho, las respuestas a la encuesta de las fuerzas de seguridad federales, estatales y locales indicaron que la incapacidad para identificar a los proveedores de servicios con datos relevantes - muchos de los cuales no están cifrados - es el mayor problema en términos de su capacidad para utilizar pruebas digitales en sus casos. El informe arroja luz sobre las lagunas en la formación de las fuerzas del orden en materia de pruebas digitales. Esto incluye al personal responsable de las pruebas colectivas, del mantenimiento de la cadena de custodia e incluso a los jueces, que son cruciales en los procesos de solicitud[65].

Esta brecha de conocimientos y habilidades tiene implicaciones en el mundo real, ya que puede contribuir a crear expectativas poco realistas sobre el funcionamiento de las distintas tecnologías y sobre cómo pueden utilizarse las pruebas digitales para respaldar casos policiales. En 2017, el FBI afirmó que no podía acceder a 7.000 dispositivos cifrados para recabar información[66], aunque resultaron ser entre mil y dos mil[67]. Y un informe del Investigator General del FBI reveló que el FBI no había intentado acceder a fondo al teléfono del caso de San Bernardino antes de pedir a un tribunal que obligara a Apple a jaquearlo[68]. En muchos casos, sin embargo, los dispositivos no son tan útiles como los investigadores podrían imaginar. Los delincuentes más hábiles no suelen exponer sus planes y es más probable que utilicen los mensajes como el resto de nosotros: en breves ráfagas sin un contexto claro. A menudo puede que ni siquiera haya información en esos dispositivos que

---

61 https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption

62 https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/

63 https://www.cfr.org/blog/theres-cop-my-pocket-policymakers-need-stop-advocating-surveillance-default

64 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf

65 Ibid

66 https://www.bbc.com/news/technology-41721354

67 https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html

68 https://www.washingtonpost.com/world/national-security/inspector-general-fbi-didnt-fully-explore-whether-it-could-hack-a-terrorists-iphone-before-asking-court-to-order-apple-to-unlock-it/2018/03/27/b56a9dca-31cf-11e8-8abc-22a366b72f2d_story.html

hubiera ayudado a las fuerzas de seguridad[69], y el informe no señala cuántos de los casos se resolvieron utilizando pruebas alternativas u otros medios. Después de toda la controversia en torno al caso de San Bernardino, el FBI no obtuvo ninguna información útil del dispositivo[70].

Las técnicas de investigación tradicionales, adaptadas a la era digital, siguen siendo útiles para atrapar a los delincuentes. Por ejemplo, la espía rusa Anna Chapman cifró su información y anotó sus contraseñas, que fueron encontradas por los funcionarios y utilizadas para acceder a la información. Para atrapar al presunto cabecilla del mercado ilícito Silk Road, los investigadores esperaron a que hubiera iniciado sesión en su ordenador antes de llevarse el dispositivo[71]. En los casos del FBI relacionados con la Ley All Writs (Ley de todas las órdenes de la Corte), los teléfonos se descifraron mediante jaqueo o incluso pidiendo a amigos y familiares que compartieran la contraseña.

En muchos casos, puede que no se necesite el contenido concreto de los mensajes. En Estados Unidos, las fuerzas de seguridad y las agencias de inteligencia pueden obtener otros datos -incluidos metadatos y análisis de tráfico- para ayudar en las investigaciones a través de los procedimientos legales tradicionales[72]. Estados Unidos cuenta con una ventaja en este sentido: las fuerzas de seguridad extranjeras se encuentran en una situación mucho peor que sus homólogas estadounidenses porque muchos de los mayores proveedores de servicios de comunicaciones están en Estados Unidos y sujetos a la legislación estadounidense, aunque las empresas están cada vez más sujetas a requisitos basados en el lugar donde se encuentran sus instalaciones y no en el lugar donde tienen su sede. Pero también existen sólidas alianzas entre las agencias de inteligencia al servicio de los gobiernos democráticos, y la cooperación sirve a menudo para cerrar casos globales complejos[73].

Sin embargo, para poder utilizar estas técnicas, las fuerzas del orden deben saber dónde buscar la información. Si se financian adecuadamente los centros de formación y las diversas iniciativas en torno a la recopilación de pruebas digitales, las fuerzas de seguridad de todos los niveles, no sólo las fuerzas de seguridad y los servicios de inteligencia nacionales, estarán mejor equipadas para investigar estos incidentes sin tener que depender de puertas traseras de cifrado que pueden dar lugar a otros problemas[74].

En Estados Unidos, un paso a tomar sería el financiar adecuadamente al Instituto Nacional de Informática Forense (NCFI, por sus siglas en inglés), que ofrece formación en pruebas digitales para agentes de la ley estatales y locales y profesionales del derecho. En 2018, la administración propuso eliminar por completo el NCFI. Solo se rescató después de que el Congreso tomara nota y restableciera la financiación. Sin embargo, en años posteriores, la financiación para la formación forense se ha recortado en más del 80 %[75]. Del mismo modo, la Agencia de Cooperación Policial de la Unión Europea (Europol) sirve como centro de coordinación para la inteligencia criminal y la cooperación nacional en toda la UE, y sería un lugar ideal para centralizar los recursos para la formación en análisis forense digital. Aunque la formación forense podría ayudar a las fuerzas del orden en todos los niveles de la sociedad, pocas propuestas para luchar contra el CSAM u otras amenazas públicas la incluyen como parte de la currícula del investigador moderno. Organizaciones y programas de formación similares ayudarían a la seguridad pública en todos los países que luchan por investigar la actividad delictiva.

---

69 https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

70 https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads

71 Ibid

72 https://www.justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/

73 https://www.lawfaremedia.org/article/rethinking-encryption

74 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf

75 Ibid

Una vez obtenidas, las fuerzas de seguridad tienen dificultades para gestionar las pruebas digitales. Un informe reciente del Centro de Estudios Estratégicos e Internacionales encuestó al personal de las fuerzas de seguridad y descubrió que muchos de ellos no saben cómo solicitar a las empresas tecnológicas los datos que necesitan para investigar delitos en general, no sólo delitos informáticos[76].

También es fácil suponer que los datos de estos sistemas serán una prueba irrefutable, pero también existe la posibilidad de que sean una pista falsa o un falso positivo. La *An Garda Síochána* -la policía nacional irlandesa- ha recibido información sobre CSAM del Centro Nacional para Menores Desaparecidos y Explotados (NCMEC) de EE.UU. desde 2010. En 2020, *la An Garda Síochána* verificó que más del 11 % de esas remisiones no eran CSAM y que los materiales eran falsos positivos: imágenes o vídeos inocuos, como niños jugando en una playa[77]. Pero a pesar de exculpar a las personas en cuestión, *la An Garda Síochána* no borró sus datos. No sabemos cuántas de las personas absueltas de sospecha de compartir CSAM permanecen en los archivos de la policía nacional irlandesa, o en los archivos de otras organizaciones policiales de todo el mundo.

## Conclusion

El cifrado desempeña un papel fundamental en la privacidad y seguridad de los datos al salvaguardar las comunicaciones en línea, permitir la libertad de expresión y proteger las transacciones financieras, entre otras cosas. Los argumentos históricos contra el cifrado se han caracterizado por el deseo de proteger los datos confidenciales y evitar al mismo tiempo que los adversarios accedan a las mismas capacidades. Aunque la tecnología ha seguido evolucionando, el "debate sobre el cifrado" se ha estancado. Para hacerlo avanzar, debemos replantearnos la conversación y aceptar que el progreso incremental es clave para la innovación.

El acceso excepcional se ha promocionado como la única forma de resolver el CSAM y otros delitos, pero es una distracción: el verdadero problema es el delito, no el cifrado ni la tecnología. El *Center for Cybersecurity Policy & Law*, junto con la gran mayoría de los miembros de la comunidad de ciberseguridad, cree que debilitar el cifrado pondría en peligro la seguridad, la privacidad y los intereses sociales vitales de cada organización e individuo. Existen otras soluciones y métodos para resolver estos delitos al tiempo que se protege la privacidad de los ciudadanos respetuosos con la ley. Estos enfoques han sido defendidos por el Centro de Estudios Estratégicos e Internacionales (CSIS), así como por la Fundación Carnegie para la Paz Internacional, la Universidad de Princeton y el Centro de Política Tecnológica Internacional. Es imperativo cambiar nuestro enfoque hacia el progreso gradual.

---

76 Ibid

77 https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing- of-child-sex-abuse-material/