accessnow.org

RESUMEN DE POLÍTICA

# 10 argumentos que desmienten los mitos sobre el cifrado

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamientoa grupos locales emergentes, intervenciones jurídicas y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

RESUMEN DE POLÍTICA

# 10 argumentos que desmienten los mitos sobre el cifrado



**Agosto de 2021**

Este resumen es una publicación de Access Now. Fue escrito por Namrata Maheshwari. Queremos agradecer a los miembros del equipo de Access Now que brindaron su asistencia, incluidos Raman Jit Singh Chima, Javier Pallero, Estelle Massé, Natalia Krapiva, Eric Null, Gustaf Björksten y Peter Micek. También queremos dar las gracias a los participantes de la reunión privada acerca del cifrado y los derechos humanos que se llevó a cabo durante RightsCon 2021 y que proporcionaron sus comentarios para crear un boceto de esta publicación.

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas de incidencia globales, el análisis integral de las políticas públicas, el financiamiento a grupos locales emergentes, intervenciones jurídicas y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

**Para obtener más información, comuníquese con: Namrata Maheshwari at namrata@accessnow.org**

# Índice

# I. Introducción

Cuando estalló la pandemia del COVID-19 en 2020, se produjo un aumento sin precedentes de la actividad en línea. En consecuencia, se maximizaron los desafíos en cuanto a la ciberseguridad. Durante el mismo año, sin embargo, los gobiernos y las autoridades de aplicación de la ley de muchos países emitieron declaraciones domésticas e internacionales extremadamente problemáticas en las que, básicamente, solicitaban que el cifrado, que es una herramienta fundamental para la privacidad y la ciberseguridad, se debilitara (ver sección IV). Hoy, a la luz de las revelaciones del Proyecto Pegasus, que demuestran el alto nivel de vulnerabilidad de nuestras comunicaciones privadas frente al *hackeo* y la exposición y que destacan la necesidad de un cifrado eficiente, observamos nuevos pedidos de las autoridades para debilitar los sistemas encriptados, así como la implementación de medidas tecnológicas para eludir el cifrado de extremo a extremo. Esto implica mayores peligros para nuestra privacidad y nuestra seguridad en línea.

El cifrado es un proceso criptográfico que consiste en codificar información de modo que solo las personas autorizadas (normalmente, los remitentes y destinatarios) puedan decodificar o descifrar la información por medio de una "clave". Esto significa que el cifrado garantiza que la comunicación entre dos o más partes se encuentre protegida de los accesos no autorizados por parte de terceros. En el caso del cifrado de extremo a extremo, ni siquiera los proveedores de los servicios de encriptación pueden acceder a la información que se intercambia. El cifrado brinda seguridad tanto para los datos en tránsito (datos que se transmiten por internet o una red privada) como los datos en reposo (datos almacenados en un dispositivo o en "la nube").

Los beneficios de un cifrado eficiente son claros. Algunos ejemplos de la vida diaria incluyen las transacciones electrónicas bancarias y financieras seguras, la confidencialidad de las comunicaciones privadas y los intercambios seguros de información sensible, como los datos de salud. Un cifrado eficiente beneficia a todas las partes interesadas de una sociedad democrática. Protege a los individuos y las comunidades mediante el fortalecimiento del

derecho a la privacidad y las libertades de expresión y asociación, ya que posibilita las comunicaciones privadas y el almacenamiento seguro de los datos. La encriptación beneficia a las empresas porque permite asegurar los secretos comerciales, fomenta la confianza de quienes consumen, limita las filtraciones de datos y promueve las innovaciones, como la tecnología de *blockchain* y las redes virtuales privadas. Por último, las autoridades de aplicación de la ley y el gobierno necesitan el cifrado para proteger la seguridad nacional, la información confidencial y los datos de las personas.

El objetivo de este artículo es responder a algunos de los principales mitos y justificaciones que utilizan los gobiernos en sus demandas de acceso orientado o excepcional y puertas traseras a sistemas cifrados para exponer los errores y las inconsistencias inherentes. Aun si una propuesta de acceso al cifrado por una puerta trasera tiene el objetivo de lograr un objetivo legítimo, debilitar la encriptación a nivel general probablemente no sea un enfoque necesario o proporcionado y podría implicar riesgos para los derechos humanos, la seguridad nacional, la democracia y la economía.

# II. 10 argumentos que desmienten los mitos sobre el cifrado

## Argumento 1: Los procedimientos de cifrado eficientes son esenciales para la seguridad digital

### Mito: Las puertas traseras que brindan acceso orientado o excepcional a las autoridades de aplicación de la ley no debilitan la seguridad de Internet

El cifrado es un proceso completamente matemático. Los contenidos se encuentran cifrados y seguros o no; un contenido no puede estar *mayormente* cifrado, p. ej., si se encuentra encriptado, pero ciertos terceros tienen la posibilidad de acceder si lo desean. Este tipo de accesos excepcionales destruyen la esencia del cifrado. No hay manera de permitir el acceso por parte del gobierno sin concederlo a otros agentes no autorizados. Las demandas de los gobiernos de obtener acceso excepcional a los sistemas cifrados, pero de una manera que *preserve la seguridad*, se describe correctamente como un concepto incompatible con la matemática.

Una puerta trasera que brinde acceso a contenido cifrado es una falla de seguridad que vuelve vulnerables al sistema y los datos correspondientes. Los accesos orientados o excepcionales, como las demandas de los organismos de orden público, necesitarían crear una puerta trasera de alguna manera. Una vez que se crea dicha vulnerabilidad, hay una amplia variedad de agentes maliciosos que pueden hacer uso de ella. Simplemente, no es posible crear una puerta trasera a la que solo tengan acceso “las personas con buenas intenciones”. Tal como lo explican los científicos y expertos en seguridad, implementar mecanismos de acceso excepcional implica ordenar la existencia de la inseguridad. Por lo tanto, la afirmación de que es posible implementar una puerta trasera de forma segura es paradójica. Cerrar la puerta delantera no tiene mucho sentido si hay una puerta trasera abierta, y la puerta trasera pone en peligro de forma indiscriminada la seguridad de todas las personas que hacen uso del sistema cifrado.

## Argumento 2: Otorgar acceso excepcional a las autoridades de aplicación de la ley supone un riesgo para la democracia y los derechos humanos

### Mito: Las puertas traseras para las autoridades de aplicación de la ley no afectan nuestros derechos o la democracia

La privacidad es un aspecto fundamental del ser humano. Permite que las personas y las comunidades desarrollen relaciones interpersonales, soliciten asesoramiento médico o legal sin miedo a la exposición y expresen sus opiniones libremente, aun si son controversiales o poco populares. Necesitamos de la privacidad para pensar con libertad. La idea de una posible vigilancia tiene un efecto opresivo sobre el comportamiento de las personas. Tal como lo indica la Corte Europea de Derechos Humanos, la mera existencia de una ley que autorice el monitoreo secreto de las comunicaciones es incompatible con la libertad de expresión y el derecho a la privacidad. Y esto es especialmente importante para los/las profesionales del periodismo, la medicina y la abogacía, así como las víctimas de discriminación o abuso, que dependen de las comunicaciones seguras para proteger su seguridad. En algunas circunstancias, debilitar la encriptación y la privacidad puede poner vidas en peligro.

Dado que el cifrado posibilita las comunicaciones privadas, sin restricciones y libres de vigilancia, protege los derechos humanos y las libertades relacionadas con la privacidad, la expresión, y la reunión y asociación. Estos derechos son fundamentales para el funcionamiento de la democracia. Por lo tanto, el cifrado es esencial para los derechos humanos en la era digital, y los ataques a este mecanismo también afectan los derechos humanos y la democracia.

## Argumento 3: Un cifrado eficiente fortalece la privacidad y la seguridad

### Mito: Para brindar seguridad, es necesario sacrificar la privacidad

Los defensores de las puertas traseras para el cifrado definen incorrectamente la privacidad y la seguridad como una operación matemática de suma cero en la que se deben sacrificar componentes para lograr otros. La premisa de "privacidad vs. seguridad" se basa en una binaridad falsa. La privacidad y la seguridad son principios que se refuerzan mutuamente.

Un cifrado efectivo fortalece tanto la privacidad como la seguridad. Cuando se protegen la información y las comunicaciones personales, y las transacciones financieras son seguras, se reducen inevitablemente las filtraciones de datos. Los beneficios del cifrado para proporcionar una defensa sólida frente a los ciberataques no solo favorecen a las personas, sino también a los gobiernos y autoridades de aplicación de la ley que, de otro modo, deberían lidiar con las consecuencias de estos ataques. El cifrado también es esencial para la eficiencia de la infraestructura de ciberseguridad que necesitan los gobiernos y organismos de orden público para proteger la seguridad nacional. Por lo tanto, debilitar deliberadamente los sistemas cifrados también debilita a las personas, los gobiernos y las empresas, y brinda a los agentes maliciosos la capacidad de utilizar estas vulnerabilidades como armas. Un marco más apropiado para este debate sería el de "seguridad vs. seguridad", ya que el cifrado no solo protege la privacidad, sino también la seguridad. Una política de "seguridad" que procure debilitar el cifrado puede convertirse fácilmente en una política de "inseguridad", ya que crea más daños que los que intenta evitar.

## Argumento 4: Las autoridades de aplicación de la ley entraron en la edad de oro de la vigilancia sin debilitar el cifrado

### Mito: Las autoridades de aplicación de la ley se encuentran progresivamente "a oscuras", lo cual hace que sea necesario romper el cifrado

Las agencias de inteligencia y las autoridades de aplicación de la ley reclaman que el cifrado evita la interceptación, lo que se conoce como "quedarse a oscuras". La implicancia es que los cambios tecnológicos redujeron las capacidades de vigilancia. Sin embargo, la metáfora de "quedarse a oscuras" es cuestionable.

Esto se debe a que ignora el hecho de que, gracias a los cambios tecnológicos, en la actualidad, hay muchos más datos disponibles sobre las personas que antes. Lo que vivimos hoy no es una era de "oscuridad", sino algo más cercano a una "era dorada de la vigilancia", en la que es posible recopilar una amplia variedad de información sobre nuestra vida íntima (como nuestra ubicación, nuestros contactos y muchos otros datos que antes no se registraban) en "expedientes digitales". Y el surgimiento sin precedentes de la actividad en línea durante la pandemia del COVID-19 no hizo más que enriquecer nuestras huellas en línea. Además, el informe de Berkman Klein Center for Internet & Society de la Universidad de Harvard concluyó que el cifrado se encuentra tan generalizado como lo indica el gobierno, ni es probable que lo sea. Mientras tanto, el crecimiento de "Internet de las cosas" probablemente incorporará nuevos vectores de vigilancia a través de nuestros dispositivos, lo cual incrementará las vulnerabilidades de seguridad que se pueden explotar.

Aquí no hay ninguna novedad. Las revelaciones de Snowden en 2013 dejaron en claro la cantidad de datos de las personas que pueden recopilar los gobiernos a través de los programas de vigilancia de alcance excesivo. La tecnología digital no sumerge nuestros datos en la oscuridad, sino que, por el contrario, los vuelve más vulnerables a la exposición. De hecho, incluso con el cifrado y otras herramientas diseñadas para proteger los datos, al limitar el alcance de la vigilancia, las organizaciones deberán seguir estrictos principios de minimización de datos, y los gobiernos deberán implementar reformas de vigilancia significativas para proteger los derechos y las libertades de las personas.

## Argumento 5: Debilitar el cifrado no impide que delincuentes y terroristas utilicen sistemas de encriptación sólidos

### Mito: Debilitar el cifrado es una medida efectiva para prevenir el terrorismo y la actividad delictiva

Si se solicita a las empresas de tecnología que incluyan puertas traseras en su software y sus aplicaciones, la única certeza es que se le impedirá al público general elegir una plataforma en la que se protejan sus derechos fundamentales y sus datos. Quienes deseen cometer delitos, incluidos los de terrorismo, simplemente acudirán a otras plataformas cifradas disponibles en jurisdicciones extranjeras o en el mercado negro, o hasta podrían crear sus propios sistemas. Estas plataformas tienen altas probabilidades de quedar fuera del alcance de la ley y las autoridades de implementación, lo cual dificulta aún más la posibilidad de impedir e investigar los delitos. Actualmente, si bien las plataformas cifradas protegen el contenido de las comunicaciones de los usuarios, en la mayoría de las jurisdicciones, las autoridades de aplicación de la ley tienen derecho a acceder a metadatos y otros tipos de información útiles para sus investigaciones. Dada la sensibilidad de los metadatos, es clave que el acceso a esta información solo se permita cuando se cumplan los principios de necesidad y oportunidad. El uso de metadatos con fines de vigilancia masiva y las órdenes de retención de metadatos socavan inherentemente los derechos humanos.

El incremento de las capacidades de vigilancia con frecuencia conlleva a la implementación de sistemas de vigilancia invasivos sin que haya suficiente evidencia en cuanto a su efectividad. La sola creación de la capacidad de acceder a información cifrada podría permitir la vigilancia generalizada, la cual infringe los principios de minimización de datos y de necesidad y proporcionalidad. En una investigación sobre la eficacia de la vigilancia para prevenir el terrorismo, un estudio de EE. UU. sugiere que la conexión entre el aumento de las capacidades de vigilancia y la prevención de los ataques es tenue. En 2004, el FBI analizó un programa de vigilancia que incluía la recopilación de correos electrónicos y llamadas telefónicas a nivel masivo para deducir cuántas de estas actividades habían “colaborado significativamente con la identificación de terroristas, la deportación de personas sospechosas de cometer actos de terrorismo o el desarrollo de sistemas de informantes confidenciales que brindasen información sobre terroristas”. Entre 2001 y 2004, solo un 1.2 % de los indicadores realmente fueron acertados. Entre 2004 y 2006, ninguna de las pistas resultaron útiles. Por lo tanto, debilitar el cifrado para ampliar las capacidades de vigilancia no solo socava la seguridad digital y perjudica al público en general, sino que, además, no

proporciona capacidades significativas, sostenibles y mejoradas para prevenir el terrorismo. Debilitar la seguridad de todos por una mera posibilidad de identificar a algunos agentes malintencionados en línea es un enfoque completamente desproporcionado que pone en peligro la privacidad y la seguridad de todas las personas que utilizan una plataforma, sin evidencia de efectividad para lograr el objetivo de prevenir los ataques.

## Argumento 6: Un cifrado eficaz beneficia la seguridad infantil en línea

### Mito: El cifrado genera inseguridad en línea para los niños y las niñas

Quienes defienden el rompimiento del cifrado ven esta medida como una solución para el problema del Material sobre Abuso Sexual Infantil (CSAM) en línea. Sin embargo, al igual que otros agentes delictivos, quienes deseen cometer este tipo de crímenes acudirán a otras plataformas disponibles en otras jurisdicciones o en el mercado negro, o hasta podrían crear sus propias plataformas cifradas, para ocultar sus acciones. Esto significa que el problema persistirá y que, simplemente, quedará fuera del alcance de la ley e impedirá el acceso a metadatos que podrían ser fundamentales para ciertas investigaciones.

Es necesario destacar que no se debe ordenar la retención de metadatos. El acceso de las autoridades públicas a cualquier tipo de datos, incluidos los metadatos, solo debe permitirse cuando exista un marco legal que priorice los derechos humanos y satisfaga estándares estrictos de necesidad y proporcionalidad.

Y lo que es más importante, los niños y las niñas necesitan privacidad y mecanismos de cifrado efectivos para resguardar su seguridad en línea. Necesitan contar con plataformas encriptadas en las que se pueda autenticar la identidad de las personas con quienes interactúan y donde sus datos personales no queden en peligro de exposición frente a terceros. La Convención sobre los Derechos del Niño de las Naciones Unidas reconoce que, entre otras cosas, los menores tienen derecho a gozar de privacidad, libertad de expresión, acceso a la información y libertad de asociación. UNICEF destacó la importancia de proteger estos derechos infantiles en línea. Además, una encuesta de UNESCO indicó que la privacidad es importante para más del 90 % de los/las jóvenes que respondieron, quienes consideran

que pueden tener seguridad en línea si adquieren la información y las competencias tecnológicas necesarias. El cifrado es una de las mejores herramientas que tenemos para preservar la seguridad digital. A causa de la pandemia y el aprendizaje en línea, cada vez más menores de edad navegan en línea. En consecuencia, los gobiernos deben promover el uso de mecanismos eficientes de cifrado para preservar la seguridad de los infantes, no introducir deliberadamente vulnerabilidades de seguridad en las tecnologías que usan.

## Argumento 7: Implementar la "trazabilidad" obligatoria pone en peligro la privacidad y paraliza la libertad de expresión

### Mito: Es necesario implementar medidas de trazabilidad para prevenir la diseminación de información falsa

Algunos gobiernos han propuesto implementar la "trazabilidad" obligatoria para combatir la diseminación de información falsa mediante plataformas de mensajería en línea. Una medida de este tipo requeriría que ciertos intermediarios rastreen el origen del contenido que circula en sus plataformas. El rastreo pone en peligro la seguridad que ofrece el cifrado de extremo a extremo y supone una variedad de problemas que destacaremos a continuación. Además de socavar varios derechos fundamentales, su utilidad es limitada en la práctica.

Para implementar medidas de trazabilidad, las plataformas con cifrado de extremo a extremo deben desarrollar una nueva capacidad para identificar a los remitentes y destinatarios de cada mensaje, así como el momento de envío y, en algunos casos, la ubicación. Actualmente, dichas plataformas no tienen la posibilidad de acceder a esta información para proteger la privacidad y la seguridad. Las medidas de trazabilidad requerirían que las plataformas cifradas de extremo a extremo se rediseñen completamente para habilitar el acceso a la información sobre las personas y sus comunicaciones, así como el almacenamiento de estos datos, de un modo que no se permite actualmente. Diferentes profesionales de tecnología explican que la trazabilidad y el cifrado de extremo a extremo no pueden coexistir. Independientemente de cómo se implemente la trazabilidad, indefectiblemente perjudicará la privacidad y la seguridad, que constituyen el compromiso central del cifrado de extremo a extremo.

Dado que la trazabilidad pone en peligro el anonimato y el derecho a la privacidad, este tipo de medida tiene inevitablemente un efecto paralizante sobre el derecho a la libertad de expresión. Las personas no podrían comunicarse con libertad debido a la posibilidad de enfrentar consecuencias si sus mensajes se divulgasen a gran escala. Esto representa una amenaza para los fundamentos de la democracia. La mera viralidad de un mensaje no debe constituir una causa de culpabilidad o sospecha. Además, la efectividad práctica de la trazabilidad no está comprobada. Quien publica un mensaje en una plataforma puede no ser el creador de dicho contenido. A su vez, la prevalencia de información falsa en las plataformas de redes sociales indica que la trazabilidad no es del todo eficiente.

Por último, el argumento de que la trazabilidad solo implica la recolección de metadatos, no contenido, y, por lo tanto, no afecta la privacidad o la libertad de expresión es un tanto engañoso. El supuesto propósito de la trazabilidad es identificar al *remitente* de un mensaje en particular porque las autoridades de aplicación de la ley ya conocen su *contenido* y lo consideran problemático. Pero, justamente, los metadatos (p. ej., quién envió el mensaje a quién y cuándo) son los que protegen la privacidad y la libertad de expresión de las personas. Como lo indicamos anteriormente, la recolección de metadatos debe respetar de manera estricta los derechos humanos y los principios de necesidad y proporcionalidad. La implementación de la trazabilidad es incompatible con estos principios. Implica necesariamente la recolección y retención masivas de metadatos, lo cual pone en peligro la privacidad y la seguridad de miles de millones de personas en favor de la mera posibilidad de identificar a unos pocos agentes delictivos.

## Argumento 8: Un cifrado eficiente es fundamental para la ciberseguridad y para proteger la seguridad nacional

### Mito: El acceso excepcional a contenido cifrado es necesario para proteger la seguridad nacional

Contar con sistemas de cifrado eficientes es fundamental para crear una infraestructura de ciberseguridad resiliente que proteja la seguridad nacional. Esto incluye garantizar que el cifrado de extremo a extremo proteja las comunicaciones sensibles que se llevan a cabo regularmente entre el gobierno y las agencias de inteligencia. Además, resguardar los sistemas y las plataformas de uso frecuente mediante un cifrado seguro permite brindar seguridad a la nación. Si solo algunas personas u organizaciones implementan mecanismos de cifrado, o si este procedimiento se utiliza únicamente con algunos propósitos, se revela el valor de los datos y se exacerba el peligro de ataque.

El aumento de los incidentes de ciberseguridad y las filtraciones orientadas representan argumentos a favor, no en contra, del cifrado. Estos ataques, que involucran una amplia variedad de organizaciones, autoridades y personas con datos sensibles, incluidas algunas agencias federales en EE.UU., el presidente y el primer ministro de la India y grupos de activistas, periodistas y personas de negocios, ponen en peligro la seguridad nacional. Si no se utilizaran sistemas de cifrado seguros, se producirían más exposiciones y accesos no autorizados a información clasificada y datos personales almacenados en las bases de datos de los gobiernos, lo cual favorece a ciberdelincuentes y adversarios patrocinados por gobiernos. También ocurrirían más ataques exitosos a las infraestructuras esenciales, como los sistemas de atención médica, los registros electorales y el transporte público, ya que los sistemas cifrados ayudar a proteger su seguridad.

## Argumento 9: Los mecanismos de cifrado seguros mantienen la confianza en el ecosistema digital y favorecen el crecimiento económico

### Mito: Debilitar deliberadamente los sistemas de cifrado no afecta la economía

El cifrado es clave para mantener la confidencialidad y la autenticidad de los datos en el ecosistema digital. Por ejemplo, los bancos dependen en gran medida del cifrado para facilitar las transacciones, garantizar la protección de la información de las cuentas y otros datos de sus clientes y proteger los secretos comerciales. A su vez, el cifrado favorece la confianza de la clientela en las instituciones bancarias. Esta base de seguridad y confianza promueve la innovación e incentiva el desarrollo de una infraestructura tecnológica resiliente, lo cual fomenta la competencia industrial y contribuye con el crecimiento de la economía nacional. Por lo tanto, el cifrado es la clave de la economía digital moderna.

Debilitar deliberadamente el cifrado implicaría altos costos para las empresas que dependen de este proceso y tendría un efecto negativo en la economía. La carga de cumplimiento impuesta legalmente para debilitar el cifrado ha forzado a las empresas de tecnología a retirarse del mercado en algunos países. Este tipo de retiro no solo afecta la competencia y la innovación, sino también el empleo. En los países donde se debilita el cifrado, el mercado se ve afectado por la pérdida de empresas que ofrecen este tipo de productos o servicios de seguridad, o que dependen de ellos y, al mismo tiempo, se desalienta la innovación y el desarrollo de productos nuevos.

A su vez, los sistemas de cifrado eficientes pueden prevenir o mitigar el impacto de los incidentes de ciberseguridad que, de otro modo, causarían más daños y costos. Los incidentes de ciberseguridad son cada vez más dominantes, y el 80 % de las empresas europeas han experimentado, al menos, un incidente de este tipo. En la India, se informaron alrededor de 1,16 millones de ciberataques en 2020. El costo promedio de una filtración de datos es de USD 3,86 millones aproximadamente. El cifrado reduce el riesgo de que se produzcan estas filtraciones y permite controlar los costos, lo cual beneficia los intereses de las empresas y la economía en general.

## Argumento 10: Las agencias de inteligencia y las autoridades de aplicación de la ley no necesitan romper el cifrado para investigar delitos

### Mito: Las autoridades no tienen alternativa más que romper el cifrado

Crear puertas traseras para el cifrado permite a las autoridades acceder a ciertos datos que pueden ser necesarios en determinadas circunstancias, pero eso no significa que implementar medidas que debiliten la seguridad sea necesario, proporcionado o incluso apropiado para lograr objetivos de inteligencia o aplicación de la ley en una democracia moderna y respetuosa de los derechos. Tal como lo establecimos anteriormente, las agencias de inteligencia y las autoridades de aplicación de la ley ya obtienen beneficios debido al gran incremento de los datos personales que se encuentran disponibles en la era digital. Existen muchas alternativas al debilitamiento del cifrado para investigar delitos.

Un ejemplo de datos que suelen estar disponibles para las autoridades son los metadatos de las comunicaciones. Pueden ser fundamentales para las investigaciones siempre que se acceda a ellos conforme a los principios internacionales sobre el respeto por los derechos humanos en la vigilancia de las comunicaciones, incluidos los principios de necesidad y proporcionalidad. Estos estándares estrictos sobre el acceso lícito a los datos son necesarios porque, incluso los datos que no forman parte del contenido de las comunicaciones, revelan aspectos íntimos sobre las actividades de las personas. Las autoridades de aplicación de la ley también pueden obtener testimonios directos de las distintas partes involucradas en las comunicaciones y, en algunos casos, acceder al contenido mediante respaldos de datos.

Además, aun si el contenido de las comunicaciones electrónicas puede ser útil en algunos casos, casi nunca es la única evidencia. En la gran mayoría de los casos, las autoridades de aplicación de la ley aún dependen principalmente de las evidencias tradicionales, como testigos, informantes, evidencia física y registros comerciales de bancos y empresas de telefonía celular. Vale la pena destacar que, en ocasiones, una cierta cantidad de información puede no estar disponible para las autoridades de aplicación de la ley por diferentes motivos. Por ejemplo, si una persona borra una comunicación de forma permanente o si se daña una cámara de seguridad.

Como conclusión, Acceder al 100 % de la evidencia potencialmente disponible en todo momento es imposible y supone un peligro para los derechos de las personas. Crear puertas

traseras para el cifrado y debilitar la seguridad para todos a fin de obtener toda la evidencia posible en algunos casos no respeta las libertades y los derechos humanos y, en la práctica, no podrá sustituir el trabajo de investigación de calidad.

## III. Conclusión: Necesitamos más seguridad digital, no menos, y el cifrado debe fortalecerse, no debilitarse

Definitivamente debemos tomar medidas con respecto a la seguridad infantil en línea, la desinformación, la seguridad nacional y la actividad delictiva en la era digital. Sin embargo, aun si el objetivo final por el cual se ordena la creación de la puerta trasera es legítimo, los medios deben ser necesarios y proporcionados. Incorporar deliberadamente puntos débiles de seguridad en los sistemas cifrados no es una medida válida. Debilitar el cifrado crea más peligros que los que previene. Además, no hay evidencia que garantice que romper el cifrado genere los resultados deseados. En el mejor de los casos, el acceso excepcional al contenido cifrado podría servir como una solución parcial o de corto plazo para la aplicación de la ley.

Tal como lo explicamos en este resumen, el cifrado es una herramienta vital para la protección de los derechos humanos, la democracia, la ciberseguridad y la economía. Los derechos a la privacidad y la libertad de expresión son derechos humanos básicos y, en el mundo digital que habitamos hoy, no es posible separar verdaderamente estos derechos de la necesidad de contar con canales de comunicación en línea seguros y libres de vigilancia excesiva. El cifrado es un componente esencial para obtener una infraestructura tecnológica segura, y los gobiernos deben promover su uso, no desalentarlo.

# IV. Apéndice

## A. Principales declaraciones de gobiernos y autoridades sobre el cifrado

### DECLARACIONES INTERNACIONALES

| | | |
|---|---|---|
| 26 de julio de 2021 | Opinión de Catherine De Boelle, directora ejecutiva de Europol, y Cyrus R. Vance Jr., abogado de distrito del Condado de Nueva York, Nueva York. | "El cifrado no regulado es una negación de la justicia."<br><br>Fuente: Politico |
| 10 de junio de 2021 | Declaración conjunta sobre la visita al Reino Unido del presidente de EE.UU. Joe Biden por invitación del Primer Ministro británico Boris Johnson. | "Estamos ansiosos por implementar un acuerdo sólido y bilateral de acceso a datos basado en el reconocimiento mutuo de que los dos países tienen un nivel alto de protección de datos que permite llevar a cabo investigaciones legales en ambos lados del Atlántico y, así, obtener la evidencia necesaria para ajusticiar a quienes cometan delitos y mantener estándares rigurosos de privacidad. Trabajaremos en conjunto para controlar estrictamente el acceso legal al contenido de las comunicaciones que sea fundamental para las investigaciones y la persecución de criminales graves, incluido a quienes sean responsables de actos de terrorismo y abuso infantil. También trabajaremos de cerca con las empresas de tecnología para proteger la seguridad de nuestros/as ciudadanos/as en el proceso."<br><br>Fuente: Declaración conjunta de EE.UU. y Reino Unido |
| 2020 | Informe de seguridad de Munich | "Dada la necesidad de superar frecuentemente a extremistas yihadistas en el uso y el alcance de las publicaciones de redes sociales, la extrema derecha depende en gran medida de las plataformas de Internet para comunicarse y diseminar sus ideas. Con el aumento de las bajas de contenido extremista en plataformas como Twitter, Facebook y YouTube, la extrema derecha ha migrado progresivamente a aplicaciones cifradas como Telegram y Discord, así como otras plataformas no reguladas como 8chan o Gab. Estos rincones lejanos de Internet |

| | | |
|---|---|---|
| | | también contribuyen decisivamente con el proceso de autoradicalización."<br><br>Fuente: Informe de seguridad de Munich de 2020 |
| 11 de octubre de 2020 | Five Eyes, India y Japón | Declaración internacional: Cifrado de extremo a extremo y seguridad pública<br><br>Demanda de puertas traseras para el acceso obligatorio a contenido cifrado en pro de la seguridad pública. |
| Septiembre de 2020 | Comisión Europea. | Informe "Technical solutions to detect child sexual abuse in end-to-end encrypted communications" (Soluciones técnicas para detectar contenido de abuso sexual infantil en las comunicaciones cifradas de extremo a extremo)<br><br>Se analizaron distintos métodos para identificar el Material de Abuso Sexual de Menores (CSAM) en comunicaciones electrónicas privadas que utilizan cifrado de extremo a extremo. |
| Septiembre de 2020 | Comisión Europea. | Una nota interna indicó que la Comisión Europea está contemplando maneras de habilitar el acceso de las fuerzas de aplicación de la ley a las comunicaciones cifradas de extremo a extremo siempre que sea dentro del marco legal adecuado, a fin de terminar con el CSAM y los delitos organizados.<br><br>Fuente: Now, U.E. Is Deliberating On Law Enforcement Access To End-To-End Encrypted Communications (Actualmente, la U.E. analiza maneras de habilitar el acceso de las fuerzas de aplicación de la ley a las comunicaciones cifradas de extremo a extremo)<br><br>[Nota: Luego, la Comisión Europea envió una aclaración a MediaNama en la que indicaba que no se deben introducir puertas traseras y no se debe debilitar el cifrado ]. |
| Julio de 2020 | Ministro de Tecnologías de Información de la India, Ravi Shankar Prasad, en la reunión de Ministros de Economía Digital del G20 | "Es momento de reconocer que las plataformas digitales de todo el mundo deben responsabilizarse por los problemas de soberanía de los países, incluidos la defensa, la privacidad y la seguridad de las personas."<br><br>Fuente: Comunicado de prensa del Ministro de Electrónica y Tecnologías de la Información de la India |

| | | |
|---|---|---|
| 4 de octubre de 2019 | Carta de Priti Patel. Ministra del Interior del Reino Unido, William Barr, Fiscal General de EE.UU., Kevin McAleenan (entonces) Secretario de Seguridad Nacional de EE.UU. y Hon Peter Dutton, Ministro de Asuntos Internos de Australia, a Mark Zuckerberg | Carta abierta: Facebook's "Privacy first" proposals (Propuestas de Facebook basadas en la privacidad)<br><br>En esta carta, se solicitó a Facebook que no proceda con su plan para implementar el cifrado de extremo a extremo en sus servicios de mensajería a fin de proteger a las personas y los/las menores. |
| Julio de 2019 | Five Eyes | Reunión conjunta de FCM y Quinteto de Fiscales Generales<br><br>Estableció que "las empresas de tecnología deben incluir mecanismos en el diseño de sus productos y servicios cifrados que permitan a los gobiernos, siempre que actúen con la autoridad legal pertinente, acceder a los datos en un formato legible y utilizable". |
| Julio de 2017 | G20 | "Otro conjunto de problemas, informó Merkel, son los servicios de mensajería. La declaración publicada suena clandestina, ya que indica que: 'Conforme a las expectativas de nuestros pueblos, también promovemos la colaboración con la industria para brindar acceso legal y no arbitrario a la información disponible siempre que dicho acceso sea necesario para la protección de la seguridad nacional frente a las amenazas terroristas'. Pero está claro que el objetivo es el cifrado. Deben poder comprender, cuando haya sospechas razonables, el contenido de las comunicaciones terroristas, explicó Merkel."<br><br>Fuente: G20 Reaches Agreement Against Terrorism, Appears To Target Encryption (El G20 llega a un acuerdo frente al terrorismo que parece tener al cifrado como objetivo) |

## DECLARACIONES INTERNAS

| | | |
|---|---|---|
| 3 de diciembre de 2020 | Ministro de Asuntos Internos de Australia Peter Dutton | "El cifrado es positivo porque nos protege del crimen, pero es negativo si protege al crimen de la policía".<br><br>Fuente: AFP's new approach to flush pedophiles from 'sewer of the internet'(El nuevo enfoque de la AFP para eliminar la pedofilia de Internet) |
| Diciembre de 2020 | Anne Longfield, Comisionada de la Infancia en Inglaterra | Report on how end-to-end encryption threatens children's safety online (Informe sobre cómo el cifrado de extremo a extremo supone un riesgo para los/las menores en línea)<br><br>Recomienda cuatro pruebas que deben superar las empresas de tecnología para implementar el cifrado de extremo a extremo. |
| Noviembre de 2020 | Agencia Nacional contra el Crimen, Reino Unido | Si el contenido publicado en Facebook se encuentra cifrado de extremo a extremo, existe un gran peligro de que la justicia no pueda asistir a las víctimas de abuso infantil.<br><br>Fuente: Facebook's encryption plans could help child abusers escape justice, NCA warns (Los planes de cifrado de Facebook podrían ayudar a responsables de abuso infantil a escapar de la justicia, advierte la NCA) |
| 13 de noviembre de 2020 | Ministros y Ministras de Asuntos Internos de la U.E. | Joint statement by the E.U. home affairs ministers on the recent terrorist attacks in Europe (Declaración conjunta de Ministros y Ministras de Asuntos Internos en cuanto a los ataques terroristas recientes en Europa)<br><br>Argumenta que el acceso de las autoridades competentes a la información digital (ya sea información sobre el tráfico o, en algunos casos, datos de contenido) es "esencial para prevenir y eliminar los actos terroristas". Solicita al Consejo que considere el asunto del cifrado de datos para garantizar la recolección legal de evidencia sin debilitar la confiabilidad de la tecnología de cifrado.<br>(Nota: Esta declaración no condena explícitamente ni busca socavar el cifrado, pero esto podría ser una consecuencia). |
| 20 de octubre de 2020 | Secretario del Departamento de Asuntos Internos de Australia Mike Pezullo | "Nos preocupan particularmente los planes de Facebook para implementar el cifrado de extremo a extremo en toda su plataforma y, así, crear la mayor *dark web* del mundo."<br><br>Fuente: Facebook Set to Create 'Biggest Dark Web' With End-To-End Encryption, Says Australian Minister (Facebook se prepara para crear |

| | | |
|---|---|---|
| | | la 'mayor dark web' con el cifrado de extremo a extremo, afirma el ministro australiano) |
| 23 de octubre de 2020 | Ministro de Asuntos Internos de Australia Peter Dutton | Los gigantes de las redes sociales, incluido Facebook, bloquean los intentos de las autoridades globales de implementación de la ley para combatir la explotación sexual de menores. Dutton afirmó que Facebook, en particular, está tomando medidas deliberadas con el cifrado de extremo a extremo para denegar el acceso a información sobre asuntos que, años antes, las autoridades de aplicación de la ley hubiesen garantizado.<br><br>Fuente: Facebook putting children at risk: Dutton (Facebook pone en peligro a los/las menores: Dutton) |
| 3 de febrero de 2020 | India | Informe del Comité Adhoc de Rajya Sabha sobre el Alarmante Problema de la Pornografía en las Redes Sociales y sus Efectos en la infancia y la sociedad<br>Recomienda que la ley se enmiende para permitir el rompimiento del cifrado de extremo a extremo a fin de rastrear a quienes distribuyan material de abuso sexual infantil (CSAM). |
| 3 de junio de 2020 | Anterior Fiscal General de EE.UU. William P. Barr | Statement from Attorney General William P. Barr on Introduction of Lawful Access Bill in Senate (Declaración del Fiscal General William P. Barr sobre la introducción del Proyecto de Ley de Acceso Legal en el Senado)<br><br>Argumenta que el cifrado sin puerta trasera permite que predadores, terroristas, traficantes de drogas y hasta hackers operen con impunidad. |
| Enero de 2020 | Anterior Fiscal General de EE.UU. William P. Barr | En cuanto a los problemas de las autoridades de aplicación de la ley con respecto al cifrado: "No queremos entrar a un mundo en el que necesitemos dedicar meses y hasta años agotando recursos mientras hay vidas en peligro… Deberíamos poder acceder a estos datos ni bien tengamos conocimiento de una posible actividad delictiva."<br><br>Fuente: Barr's Encryption Push Is Decades in the Making, but Troubles Some at FBI (La propuesta de cifrado de Barr lleva décadas en proceso, pero es problemática para el FBI) |
| Octubre de 2019 | Ravi Shankar Prasad, Ministro de Tecnologías de | El origen de los mensajes de WhatsApp debe ser accesible. Quienes hacen un mal uso de las plataformas de comunicación no merecen gozar del derecho a la privacidad. |

| | | |
|---|---|---|
| | Información de la India | Fuente: Right to privacy not for those who abuse internet platform: Ravi Shankar Prasad (Quienes abusan de las plataformas de Internet no merecen gozar del derecho a la privacidad: Ravi Shankar Prasad) |

## b. Resumen de argumentos y mitos acerca del cifrado

### Argumento 1: Los procedimientos de cifrado eficientes son esenciales para la seguridad digital

**Mito: Las puertas traseras que brindan acceso orientado o excepcional a las autoridades de aplicación de la ley no debilitan la seguridad de Internet**

- ➔ El cifrado es un proceso matemático que no se puede aplicar de forma selectiva. Cualquier solicitud de una puerta trasera que solo funcione para el gobierno es, básicamente, una guerra contra la matemática.
- ➔ Una puerta trasera que brinde acceso a contenido cifrado es una falla de seguridad que vuelve vulnerables al sistema y los datos correspondientes. Aun si solo se crea para el acceso por parte del gobierno, inevitablemente, será aprovechada por una amplia variedad de agentes maliciosos.

### Argumento 2: Otorgar acceso excepcional a las autoridades de aplicación de la ley supone un riesgo para la democracia y los derechos humanos

**Mito: Las puertas traseras para las autoridades de aplicación de la ley no afectan nuestros derechos o la democracia**

- ➔ El cifrado es fundamental para la gobernanza democrática y la protección de los derechos a la privacidad y la libertad de expresión en la era digital. Debilitar el cifrado mediante mecanismos de acceso excepcionales pone en peligro los derechos humanos y la democracia en general.
- ➔ El cifrado es particularmente necesario para ciertas personas y grupos, como periodistas, representantes legales, profesionales del ámbito de la medicina y aquellas comunidades cuyo trabajo y vida dependen de la disponibilidad de canales de comunicación libres de vigilancia.

### Argumento 3: La encriptación efectiva fortalece la privacidad y la seguridad

**Mito: Para brindar seguridad, es necesario sacrificar la privacidad**

- ➔ El marco del debate en torno a las políticas de cifrado que opone la privacidad ante la seguridad es incorrecto y se basa en una binaridad falsa. Estos dos principios se refuerzan mutuamente.
- ➔ Un marco más apropiado para este debate sería el de “seguridad vs. seguridad”, ya que el cifrado no solo protege la privacidad, sino también la seguridad. Este cambio

podría colaborar con el desarrollo de una política de “seguridad” que no se convierta en una política de “inseguridad” que cree más peligros que los que intenta prevenir.

## Argumento 4: Las autoridades de aplicación de la ley entraron en la edad de oro de la vigilancia sin debilitar el cifrado

**Mito: Las autoridades de aplicación de la ley se encuentran progresivamente “a oscuras”, lo cual hace que sea necesario romper el cifrado**

- ➔ La metáfora de “quedarse a oscuras” es incorrecta. Supone que los cambios tecnológicos redujeron las capacidades de vigilancia, cuando, en realidad, las ampliaron significativamente.
- ➔ Una metáfora más precisa es la de “la edad de oro de la vigilancia”, ya que, hoy en día, hay mucha más información disponible sobre las personas que en cualquier otro momento de la historia. Esto incluye los datos sobre nuestra ubicación, nuestros contactos y muchos otros detalles que antes no se registraban y ahora pueden recopilarse para crear “expedientes digitales” con información íntima sobre nuestras vidas diarias.

## Argumento 5: Debilitar el cifrado no impide que delincuentes y terroristas utilicen mecanismos de cifrado sólidos

**Mito: Debilitar el cifrado es una medida efectiva para prevenir el terrorismo y la actividad delictiva**

- ➔ Al debilitar el cifrado, se impide al público general acceder a una plataforma en la que sus datos y derechos fundamentales se encuentran protegidos. Quienes deseen cometer delitos, simplemente acudirán a otras plataformas cifradas disponibles en jurisdicciones extranjeras o en el mercado negro, o hasta podrían crear sus propios sistemas.
- ➔ El incremento de las capacidades de vigilancia con frecuencia conlleva a la implementación de sistemas de vigilancia invasivos sin que haya suficiente evidencia en cuanto a su efectividad. Un estudio realizado en EE.UU. sugiere que la conexión entre el aumento de las capacidades de vigilancia y la prevención del terrorismo es tenue. Independientemente de su eficacia para luchar contra el terrorismo, no es necesario ni proporcional poner en peligro la privacidad y la seguridad de todas las personas que usan una plataforma o un sistema para identificar la fracción que comete actos delictivos.

## Argumento 6: El uso de mecanismos de cifrado eficientes favorece la seguridad infantil en línea

**Mito: El cifrado genera inseguridad en línea para los/las menores**

- ➔ Al igual que otros tipos de delincuentes, quienes cometen crímenes en contra de menores acudirán a otras plataformas disponibles en otras jurisdicciones o en el mercado negro, o hasta podrían crear sus propias plataformas cifradas, para ocultar sus acciones. Esto significa que la actividad delictiva continuará y, simplemente,

quedará fuera del alcance de la ley e impedirá el acceso a metadatos que podrían ser fundamentales para ciertas investigaciones.

- ➔ Los/las menores necesitan contar con plataformas cifradas en las que se pueda autenticar la identidad de las personas con quienes interactúan y donde sus datos personales no queden en peligro de exposición frente a terceros. Con más menores en línea debido a la pandemia global, los gobiernos deben promover el uso de cifrados eficientes para preservar su seguridad, no introducir deliberadamente vulnerabilidades de seguridad en las tecnologías que usan.

**Argumento 7: La "trazabilidad" obligatoria pone en peligro la privacidad y paraliza la libertad de expresión Mito: Es necesario implementar medidas de trazabilidad para prevenir la diseminación de información falsa**

- ➔ La trazabilidad pone en peligro el anonimato y el derecho a la privacidad y paraliza la libre expresión. Por lo tanto, es incompatible con los derechos humanos y la democracia.
- ➔ En la práctica, la trazabilidad tiene una utilidad limitada y no es una herramienta efectiva para combatir la desinformación.

**Argumento 8: Un cifrado eficiente es fundamental para proteger la ciberseguridad y la seguridad nacional**
**Mito: El acceso excepcional a contenido cifrado es necesario para proteger la seguridad nacional**

- ➔ Contar con mecanismos de cifrado eficientes es fundamental para crear una infraestructura de ciberseguridad resiliente que proteja la seguridad nacional. Debilitar el cifrado supone un riesgo para la seguridad nacional.
- ➔ El aumento de los incidentes de ciberseguridad y las filtraciones orientadas representan argumentos a favor, no en contra, del cifrado. Si no se utilizaran sistemas de cifrado seguros, se producirían más exposiciones y accesos no autorizados a información clasificada, lo cual favorece a ciberdelincuentes y adversarios patrocinados por gobiernos. También ocurrirían más ataques exitosos a las infraestructuras esenciales, como los sistemas de atención médica, los registros electorales y el transporte público, ya que los sistemas cifrados ayudan a proteger su seguridad.

**Argumento 9: Los mecanismos de cifrado seguros favorecen la confianza en el ecosistema digital y el crecimiento económico**
**Mito: Debilitar deliberadamente los sistemas de cifrado no afecta la economía**

- ➔ El cifrado es la clave de la economía digital moderna, ya que permite mantener la confidencialidad de los datos de los clientes y la autenticidad de las transacciones financieras. La confianza en los sistemas cifrados promueve las inversiones, la innovación y el crecimiento económico.

- ➔ A su vez, los mecanismos de cifrado eficientes pueden prevenir o mitigar el impacto de los incidentes de ciberseguridad que, de otro modo, generarían más daño y costos. El cifrado reduce el riesgo de que se produzcan filtraciones de datos y permite controlar los costos de dichas filtraciones, lo cual beneficia los intereses de las empresas y la economía en general.

## Argumento 10: Las agencias de inteligencia y las autoridades de aplicación de la ley no necesitan romper el cifrado para investigar delitos

### Mito: Las autoridades no tienen alternativa más que romper el cifrado

- ➔ Las agencias de inteligencia y las autoridades de aplicación de la ley ya obtienen beneficios significativos debido al gran incremento de los datos personales que se encuentran disponibles en la era digital. No hay evidencias que demuestren que debilitar el cifrado es una medida necesaria, proporcional o efectiva para lograr los objetivos del gobierno en una democracia moderna y respetuosa de los derechos.
- ➔ En la mayoría de los casos, las autoridades aún dependen principalmente de las evidencias tradicionales, como testigos, informantes, evidencia física y registros comerciales de bancos y empresas de telefonía celular. Socavar el cifrado y debilitar la seguridad para todos a fin de obtener toda la evidencia posible para algunos casos específicos no respeta las libertades y los derechos humanos y, en la práctica, no podrá sustituir el trabajo de investigación de calidad.