Intermediarios y cifrado

Presionar a los intermediarios para que debiliten la seguridad no es la respuesta para evitar contenido dañino en línea

Agosto de 2022

Internet es una herramienta poderosa que conecta a las personas en todo el mundo, les brinda información y las ayuda a hacer negocios. Ofrece un potencial prácticamente ilimitado para que las personas puedan innovar, mejorar su calidad de vida, celebrar, aprender de la diversidad, y resolver los desafíos más complejos del mundo. Desafortunadamente, a veces también se utiliza para facilitar o cometer delitos y para difundir información errónea peligrosa y expresiones de odio en línea. En casos extremos, se ha utilizado para transmitir o incitar acciones que han provocado daños físicos.

Algunos gobiernos han sugerido que este mal comportamiento se puede prevenir haciendo que los intermediarios de Internet sean responsables de lo que sus usuarios publican o comparten en línea[1]. Ciertos gobiernos ya han indicado que los intermediarios, como las plataformas de medios sociales y los servicios de mensajería cifrada de extremo a extremo, podrían ser considerados responsables[2] si no pueden "rastrear", es decir, identificar el originador, del contenido que se comparte a través de sus plataformas. Es poco probable que tales propuestas alcancen sus objetivos establecidos y por lo tanto debilitarán las herramientas de seguridad en las que confiamos a diario para proteger a las personas, las empresas, las economías y las naciones de cualquier daño.

Riesgos y desafíos prácticos

Romper el cifrado quiebra la confianza y la seguridad: Como se señaló anteriormente, algunos gobiernos quieren "trazabilidad", incluso para mensajes cifrados de extremo a extremo entre las partes que desean comunicarse de forma confidencial. Los gobiernos quieren poder determinar si un mensaje específico es ofensivo o ilegal y si se originó de un usuario específico. Para hacer esto, los intermediarios necesitarían acceso a uno o más de lo que se enuncia a continuación:

1 Los ejemplos incluyen las Enmiendas a las Normas sobre Tecnología de la Información de la India (Directrices de intermediarios) en virtud de la Ley de Tecnología de la Información.

2 La base legal para la responsabilidad (o la exención de responsabilidad) puede variar en función de la jurisdicción. Por ejemplo, en la India, esto está contemplado en la Sección 79 de la Ley de TI de 2000: https://cis-india.org/internet-governance/resources/section-79-information-technology-act mientras que para los intermediarios en los Estados Unidos se incluye en la Sección 230 de la Ley de Decencia en las Comunicaciones de 1996: https://en.wikipedia.org/wiki/Section_230_of_the_Communications_Decency_Act

CC BY-NC-SA 4.0

- El mensaje no cifrado está en el dispositivo del remitente.
- El mensaje descifrado está en el dispositivo del destinatario.
- El mensaje cifrado y los medios para descifrarlo.

Esto significaría que están evitando o anulando el cifrado del mensaje y, por lo tanto, su confidencialidad.

> **Impacto:** La trazabilidad rompe el principio de comunicación confidencial y socava la confianza del usuario en las plataformas y los proveedores de servicios que utilizan estos métodos para acceder al contenido. En última instancia, si el cifrado es defectuoso por diseño, incluidas las "puertas traseras" intencionales, los "oyentes silenciosos" o las claves gubernamentales obligatorias, los usuarios ya no pueden confiar en la confidencialidad o integridad de sus comunicaciones en línea. Esto rompe funciones fundamentales en las que confiamos a diario para proteger los dispositivos, datos y transacciones, y así mantener a salvo a las personas, las economías, la infraestructura y los lugares de trabajo.

No es útil legislar para lo imposible: algunos gobiernos están tratando de hacer que sus propuestas peligrosas no parezcan polémicas al declarar solo el *resultado* deseado, en lugar de las medidas que serían necesarias para lograr ese resultado. Por ejemplo, la exigencia de intermediarios para garantizar la seguridad de los niños en línea, pero sin declarar cómo esperan que esto se logre.

Sin embargo, al enmarcar el asunto como un problema de información "inaccesible para la aplicación de la ley", están implicando que el problema es el cifrado, y la solución es evitarlo o anularlo. Al menos una propuesta actual afirma que dicha solución puede implementarse sin socavar la seguridad o la confianza de los servicios y usuarios legítimos. Internet Society sigue creyendo que este simplemente no es el caso, y en mayo de 2019, fue uno de los casi 50 signatarios de una carta abierta que establece los riesgos y las deficiencias de dicho enfoque[3].

> **Impacto:** Por muy bien intencionada que sea, cualquier ley que derive en mecanismos de seguridad más débiles aumenta la oportunidad de que se produzca una actividad maliciosa y pone en riesgo a los usuarios y servicios legítimos. Esto incluye las fuerzas del orden y otras agencias gubernamentales.

Independientemente de cómo se enmarque y redacte el objetivo en la ley, la respuesta de la comunidad técnica ha sido clara y consistente: no se puede diseñar una omisión o anulación del cifrado que "solo los buenos puedan usar"[4]. Esto no es un pensamiento dogmático de los expertos técnicos, se basa en las razones fundamentales y matemáticas que hacen que los buenos sistemas de cifrado sean buenos. No se puede tener un sistema de cifrado confiable que sea fuerte contra

3 https://regmedia.co.uk/2019/05/30/letter_to_gchq_ghost_user_cryptobusting_plan.pdf

4 https://mitpress.mit.edu/blog/keys-under-doormats-security-report

CC BY-NC-SA 4.0

algunos atacantes y, a su vez, débil contra otros. No se puede tener un sistema de cifrado robusto que siempre sea robusto, excepto cuando quiera que sea débil.

La autenticación obligatoria del usuario agrega costos y complejidad: para identificar a los creadores de contenido ilegal, algunos países se inclinan por insistir en que los usuarios deban autenticarse para acceder a cualquier servicio en línea[5]. Esto puede sonar simple, pero es difícil lograr una autenticación confiable incluso cuando sea de interés para el usuario (por ejemplo, para retiros de efectivo en cajeros automáticos). Cuando el usuario tiene un incentivo para evitar la identificación, es aún más difícil. Los enfoques que cuentan con que los usuarios se autentiquen con documentos de identidad oficiales (licencia de conducir, pasaporte, identificación electrónica del gobierno) son complejos y costosos, y su confiabilidad depende de una serie de factores técnicos y no técnicos que incluyen procesos confiables para emisión y revocación, la resistencia a la manipulación, la gestión de la identidad y el acceso, entre otros. En la mayoría de los casos, agregar los datos biométricos empeora esta complejidad.

Es más, otras propuestas de "acceso excepcional" se basan en socavar los propios protocolos de autenticación de los que depende el cifrado confiable[6]. Si no puede asegurar que solo el destinatario previsto pueda acceder a las claves para descifrar su mensaje, no puede asegurar su confidencialidad.

> **Impacto:** Las propuestas basadas en la autenticación obligatoria aumentan los costos y las molestias sin lograr necesariamente el objetivo establecido. Las propuestas de políticas en esta área parecen tener demandas contradictorias e incompatibles, para la autenticación confiable en un caso, pero para que los protocolos confiables se debiliten en otro.

La responsabilidad de los intermediarios socava la confianza y la seguridad sin lograr su objetivo

La prevención de la propagación de contenido ilegal en línea es un objetivo importante, y todos debemos esforzarnos por encontrar soluciones. Sin embargo, el contenido ilegal, y el comportamiento que lo produce, existía mucho antes que Internet y, en su raíz, es un problema social en lugar de un problema principalmente técnico.

Un enfoque que sea exclusivo para resolver el problema del contenido ilegal rompiendo el cifrado debilita la seguridad. Desvía el esfuerzo de otras opciones, como mejorar las capacidades generales de las organizaciones encargadas de hacer cumplir la ley para hacer frente a los delitos mediados

5 https://www.chinalawtranslate.com/en/provisions-on-the-management-of-internet-forum-community-services/

6 https://www.internetsociety.org/es/resources/doc/2020/propuestas-fantasma/

CC BY-NC-SA 4.0

técnicamente[7], ya sea que se trate o no de cifrado. Además, confiar únicamente en las soluciones tecnológicas para los problemas sociales puede crear incentivos perversos y provocar daños no deseados, y rara vez es efectivo a largo plazo.

- Evitar que las aplicaciones de mensajería confidencial brinden confidencialidad las vuelve inútiles en el mejor de los casos, y activamente dañinas en el peor. Internet no se vuelve más seguro ni más beneficioso con dichas medidas.
- Las políticas contradictorias sobre autenticación crean más confusión y complejidad técnica, ya que socavan la confianza de los usuarios en los servicios en línea y la comunicación confidencial.

Si bien, a veces, Internet se puede usar para causar daño, debemos resistir ante las propuestas legales que exigen que los proveedores de servicios anulen la capacidad de las personas para asegurar su información e interacciones en línea. Hacerlo así, pone a las personas y las organizaciones en un mayor riesgo sin la garantía de lograr el resultado deseado. Alentamos a los legisladores a respaldar políticas y prácticas de cifrado sólidas. Esto ayudará a mantener seguras a las personas, la infraestructura y los países en línea, y a mantener a Internet como un vehículo global para la innovación, la educación y el progreso social y económico.

7 https://eshoo.house.gov/sites/eshoo.house.gov/files/migrated/wp-content/uploads/2019/10/Eshoo-Wyden-Letter-to-AG-Barr-re-encryption.pdf

CC BY-NC-SA 4.0