Resolver delitos sin debilitar el cifrado

Resumen de tres páginas

Junio de 2026

Introducción: la falsa disyuntiva

Los formuladores de políticas suelen enfrentarse a un peligroso dilema: debilitar el cifrado para atrapar a los delincuentes o dejar que Internet "quede a oscuras" (apagón digital). Esta es una falsa disyuntiva.

Los organismos de aplicación de la ley no necesitan vulnerar la seguridad digital de miles de millones de usuarios para investigar los delitos con eficacia. Vivimos en la era dorada de las pruebas digitales. Hoy en día, los organismos tienen acceso a más datos que nunca, incluidos historiales de ubicaciones, metadatos y registros de transacciones.

Debilitar el cifrado —a través de puertas traseras, escaneo del lado del cliente o acceso obligatorio— no supera las pruebas legales de necesidad y proporcionalidad. Introduce vulnerabilidades sistémicas que los delincuentes y los estados hostiles explotarán, poniendo en riesgo la seguridad de todos.

La solución: herramientas eficaces (apoyarlas)

En vez de exigir "llaves mágicas", los gobiernos deberían financiar y legalizar estos métodos de investigación eficaces:

- **Denuncia de los usuarios**: muchas veces se pueden obtener pruebas importantes directamente de los testigos, víctimas o personas que participan en las actividades delictivas y deciden cooperar. Proporcione mecanismos fáciles de usar para que los usuarios puedan denunciar los delitos y para recuperar pruebas digitales de los dispositivos.
- **Operaciones encubiertas para delitos graves como el abuso sexual infantil**: la vigilancia policial tradicional adaptada a la era digital —por ejemplo, infiltrarse en grupos y usar cuentas señuelo— sigue siendo el método de referencia para atrapar a los depredadores.
- **Cooperación voluntaria**: la existencia de canales rápidos y confiables para que las plataformas compartan datos que no son contenido (historial de inicio de sesión, actividad de una cuenta) resuelve más delitos que las debilidades técnicas impuestas.
- **Análisis de metadatos**: el cifrado protege el contenido, no el comportamiento. Los investigadores pueden crear cronologías, mapear redes criminales e identificar sospechosos utilizando datos que no son contenido (quién, cuándo, dónde) sin descifrar los mensajes.

Esta medida no implica un llamado a recopilar y retener de manera indiscriminada esta información de todos los usuarios.

- Informática forense digital en los dispositivos incautados: acceder a los datos almacenados físicamente en el dispositivo incautado de un sospechoso es una alternativa específica a la vigilancia masiva. De esta forma se accede a las pruebas en el punto final, sin afectar el "canal" seguro para el resto de las personas.

La zona roja: propuestas peligrosas (rechazarlas)

- Puertas traseras impuestas: insertar vulnerabilidades en el software de manera intencional.
- Escaneo del lado del cliente: convertir los dispositivos de los usuarios en herramientas de vigilancia.
- "Acceso legalmente autorizado por diseño": un término de marketing para referirse a vulnerabilidades sistémicas.

En resumen: proteger el cifrado fuerte no es un obstáculo sino un requisito previo para la seguridad pública. Los formuladores de políticas deben dejar de buscar una puerta trasera técnica y empezar a invertir en las capacidades humanas y forenses que permiten resolver los delitos.

Recomendaciones

Las políticas que surgen en respuesta a delitos graves en el entorno digital deberían basarse en los siguientes principios:

- Preservar un cifrado fuerte: el cifrado es fundamental para mantener la confidencialidad, la integridad y la autenticidad de los datos y las comunicaciones. Es la base de una Internet segura y confiable y protege a las personas, las empresas, los gobiernos y la infraestructura crítica. Las políticas deben fortalecer el cifrado, no debilitarlo.
- Garantizar la necesidad y la proporcionalidad: las medidas de investigación deben ser específicas, legales, limitarse a lo estrictamente necesario y proporcionales a la gravedad del delito. Las medidas que socavan la seguridad de todos los usuarios para investigar una cantidad limitada de casos no cumplen con este requisito y no deben aplicarse.
- Apoyar una Internet segura y confiable: las políticas y los enfoques operativos deben estar alineados con el objetivo de una Internet resiliente que proteja la confidencialidad, la integridad y la disponibilidad de los datos. Mantener una ciberseguridad sólida en todo el ecosistema digital es fundamental para la seguridad pública, la estabilidad económica y la confianza en los servicios digitales.