PRINCIPIOS FUNDACIONALES ALIANZA POR EL CIFRADO EN LATINOAMÉRICA Y EL CARIBE

ac-lac

CONTENIDO

ANTECEDENTES

Vivimos en un mundo digital en el cual Internet es parte intrínseca de casi todas las actividades que realizamos como seres humanos. Es por esto que la seguridad y la confianza digital como ejercicio de derecho, resultan cada vez más importantes y, en este contexto, el cifrado se convierte en un componente esencial.

En los últimos años se ha incrementado significativamente el uso de criptografía en sitios web, aplicaciones, plataformas y servicios de Internet, en general. El cifrado es fundamental para la seguridad de las transacciones financieras y para el uso confiable y rutinario de la banca, el pago de facturas, las comunicaciones digitales de periodistas, los pedidos de servicios en línea y el comercio electrónico en general. Los tipos y niveles de encriptación varían ampliamente (por ejemplo, algunas tecnologías de encriptación se basan en código abierto y otras en código propietario), pero no hay duda de que todas ellas han supuesto una mejora significativa para la seguridad y del resto de tecnologías digitales. Estas innovaciones también son fundamentales para la seguridad y garantía de los derechos de millones de personas usuarias en todo el mundo, incluso de quienes no conocen de su existencia.

Se debe alentar a las autoridades nacionales y de investigación criminal a buscar formas efectivas y compatibles con la preservación de los beneficios del cifrado para hacer frente a los desafíos derivados de posibles usos fraudulentos de esta tecnología.[1]

¿POR QUÉ ES ESENCIAL PROTEGER EL CIFRADO?

Las potenciales repercusiones de debilitar el cifrado y, como tal, la protección de la privacidad y la seguridad que proporciona, serían múltiples: personas expuestas al fraude, para la seguridad física y digital de las personas (especialmente en países con un continuo desprecio a los derechos humanos) lo que implica mayores riesgos para periodistas, personas defensoras de derechos humanos, disidentes además de grupos y poblaciones en situación de mayor vulnerabilidad. También supondría una merma para la seguridad y estabilidad de la infraestructura crítica de Internet y graves riesgos para la confiabilidad de las instituciones financieras, ya que hay muchos servicios (o componentes) en este nivel que dependen del cifrado como característica esencial para garantizar la seguridad.

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

La idea de que las sociedades necesitan intercambiar derechos por seguridad es engañosa y falsa. Debilitando el cifrado, se perjudica significativamente el ejercicio de una amplia gama de derechos por parte de las personas, sin obtener por ello nada a cambio. Los resultados solo serían mayores riesgos de seguridad y protección, confianza comprometida en la economía digital, mayores vulnerabilidades y acceso no autorizado a nuestras comunicaciones e información sensible, como datos de salud personal, libertades individuales reducidas y daños graves al ejercicio de los derechos humanos, por nombrar algunos efectos negativos.

Existe una falsa dicotomía entre privacidad y seguridad. Si bien está claro que la seguridad digital es un valor importante, se deben lograr mejoras de seguridad al mismo tiempo que se mejora el derecho a la privacidad en Internet.

Poder comunicarse preservando la confidencialidad de las comunicaciones, es una condición previa imprescindible para el ejercicio de la libertad de pensamiento, expresión, reunión y asociación. El debilitamiento de la privacidad también trae como consecuencia inevitable una reducción de la seguridad en Internet. Además de proteger la privacidad, la criptografía es una herramienta de seguridad, por lo que es absolutamente contradictorio buscar más seguridad reduciendo la seguridad.

¿CUÁLES SON LOS BENEFICIOS DE ESTOS ESFUERZOS DE COLABORACIÓN REGIONAL?

Las legítimas preocupaciones de las personas sobre su seguridad en línea tienen un traslado directo en cómo se termina actuando de manera apresurada, a la hora de abordar la necesidad de articular mecanismos eficientes contra los abusos y usos ilegítimos que puedan darse. Para lidiar con tales problemas, la perspectiva de romper / deshabilitar/ debilitar el cifrado, demuestra ser una solución tentadora para ayudar a resolver crímenes y prevenir crímenes futuros, pero trae consigo una serie de consecuencias peligrosas.

Al unir distintas voces que tienen un objetivo común en la construcción de capacidades y conocimiento, seguido de una defensa de la preservación del cifrado, buscamos equilibrar esta creciente preocupación social y encontrar soluciones a estas demandas, soluciones que se construyan desde el mantenimiento de la integridad de la herramienta y la promoción y protección de los derechos humanos en línea. La defensa de la criptografía debe venir unida a la generación de principios, alternativas y vías de colaboración para resolver el problema de los usos indebidos en la red. Es, por tanto, necesario llegar a un consenso para establecer este tipo de mecanismos, reforzando el compromiso con el mantenimiento de un cifrado fuerte.

Es importante señalar que el uso y preservación de la herramienta no implica una falta de colaboración con los gobiernos en armonía con las leyes y principios reconocidos internacionalmente. En este sentido, es oportuno insistir en explorar la creación de procesos que mantengan la integridad del cifrado, la protección de los derechos humanos y que permitan a su vez colaborar con la prevención del delito, y con las Fuerzas y Cuerpos de Seguridad en general al utilizar información no cifrada. Procesos que no deben implicar obligación alguna de debilitamiento de las protecciones de seguridad y privacidad presentes en las plataformas o servicios. Además los parámetros legales para acceder a esta información deben tener las garantías de respeto a la privacidad y derechos humanos. Se debe promover la creación de espacios y diálogos orientados a la búsqueda de acuerdos con relación a las buenas prácticas en materia de colaboración.

La pandemia de COVID-19 ha acelerado los esfuerzos para expandir la conectividad e impulsar la transformación digital. Pero, por otro lado, también se ha incrementado notablemente el debate sobre la privacidad y seguridad de las comunicaciones, así como la exposición a riesgos derivados de fugas de información, entre otros.

Incluso en un contexto de cifrado, debemos buscar formas inteligentes de abordar las preocupaciones legítimas de seguridad y aplicación de la ley, evitando que determinados actores hagan un uso pernicioso o dañino. Un proceso que contribuya a que los derechos y la seguridad en la red sean más fuertes y mejores para todas las personas usuarias.

Esta iniciativa propone crear una Alianza regional de múltiples partes interesadas para la defensa y promoción del cifrado con el objetivo de establecer una plataforma para la construcción colectiva de capacidades y conocimiento en América Latina y Caribe, con base en el encriptado como una herramienta imprescindible para la seguridad y el respeto de los derechos humanos y

fundamentales en la región, tales como la libertad de expresión y la privacidad. A su vez, se plantea avanzar en una agenda proactiva para promover y defender el cifrado en América Latina y Caribe, que lo fortalezca y genere un ecosistema de confianza, seguridad, y estabilidad de la red, como la infraestructura crítica de Internet, sus aplicaciones y servicios. Finalmente coordinar esfuerzos con las distintas iniciativas a nivel global, regional y nacional, generando espacios de intercambio y movilización ante el impacto del debilitamiento del cifrado sobre los derechos y la seguridad.

MISIÓN DE AC-LAC

Una aproximación a la misión de esta alianza, que debería ser discutida y perfeccionada por sus participantes una vez que esté operativa, sería::

> “Promover y proteger los derechos fundamentales de las personas en América Latina mediante el uso masivo del cifrado de extremo a extremo (E2EE) en la región y preservarlo como una herramienta importante para la seguridad digital de individuos, gobiernos, empresas, aplicaciones, infraestructura. Además, colaborar para que las alternativas de cooperación en ciberseguridad preserven los beneficios y principios del cifrado, así como la privacidad y el ejercicio de otros derechos que el E2EE promueve".