PRINCIPIOS FUNDACIONAIS DA ALIANÇA PARA A CRIPTOGRAFIA NA AMÉRICA LATINA E CARIBE

ac-lac

CONTEÚDO

ANTECEDENTES

Vivemos em um mundo no qual as tecnologias digitais de informação e comunicação são parte intrínseca de quase todas as atividades que realizamos como seres humanos. É por isso que a segurança e a confiança digital são cada vez mais importantes, e a criptografia se torna um componente essencial.

Nos últimos anos, o uso de criptografia em sites, aplicativos, plataformas, transações bancárias e serviços de Internet em geral aumentou significativamente. A criptografia é fundamental para a segurança de operações financeiras e para o uso confiável e rotineiro de serviços bancários, pagamento de contas, pedidos de serviços online e comércio eletrônico em geral. Os tipos e níveis de criptografia variam amplamente (por exemplo, algumas tecnologias de criptografia são baseadas em código aberto e outras em código licenciado), mas não há dúvida de que todas elas representaram uma melhoria significativa para a segurança da tecnologia digital. Essas inovações também permitem melhorias em relação à segurança e ao exercício de direitos para milhões de pessoas em todo o mundo, até mesmo para quem não sabe de sua existência.

As autoridades nacionais e de investigação criminal devem ser encorajadas a buscar maneiras eficazes e compatíveis de preservar os benefícios da criptografia para enfrentar os desafios que podem enfrentar o uso fraudulento dessa tecnologia[1]

POR QUE PROTEGER A CRIPTOGRAFIA É FUNDAMENTAL?

As repercussões potenciais do enfraquecimento da criptografia e, como tal, da proteção de privacidade e segurança que ela fornece, seriam múltiplas: pessoas expostas a fraudes, riscos para a segurança física e digital das pessoas (especialmente em países com histórico sistemático de desrespeito a direitos humanos), o que implica maiores riscos para jornalistas, defensores dos direitos humanos, dissidentes além de grupos e populações em situação de maior vulnerabilidade. Também seriam prejudicadas a segurança e a estabilidade da infraestrutura crítica da Internet, e sérios riscos para a estabilidade das instituições financeiras, pois há muitos serviços (o componentes) neste nível que dependem da criptografia como recurso essencial para a garantia de segurança.

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

A ideia de que as sociedades precisam negociar direitos por segurança é enganosa e falsa. O enfraquecimento da criptografia prejudica significativamente o exercício de uma ampla gama de direitos pelas pessoas, sem oferecer nada em troca. "Os resultados seriam somente riscos agravados de segurança e proteção, comprometimento da confiança na economia digital, maiores vulnerabilidades e acesso não autorizado às nossas comunicações e informações sensíveis, como dados pessoais de saúde, redução das liberdades individuais e sérios danos ao exercício de direitos humanos, para citar alguns efeitos negativos

Existe uma falsa dicotomia entre privacidade e segurança. Embora esteja claro que a segurança digital é um valor importante, melhorias na segurança devem ser alcançadas enquanto se aumenta o direito à privacidade na Internet. Ser capaz de se comunicar preservando a confidencialidade é uma condição prévia para o exercício da liberdade de pensamento, expressão e associação. O enfraquecimento da privacidade também traz a consequência inevitável de uma segurança mais fraca na Internet. Além de proteger a vida privada, a criptografia é uma ferramenta de segurança, sendo, portanto, absolutamente contraditório buscar mais segurança por meio da redução da segurança.

QUAIS SÃO OS BENEFÍCIOS DE UM ESFORÇO DE COLABORAÇÃO REGIONAL?

A preocupação legítima dos cidadãos com sua segurança online tem uma relação direta sobre a forma precipitada como se acaba agindo, quando se trata de abordar a necessidade de articular mecanismos eficientes contra abusos e usos ilegítimos que possam ocorrer. Para lidar com esses problemas, a perspectiva de quebrar / desativar/ enfraquecer a criptografia parece ser uma solução tentadora para ajudar a resolver crimes e prevenir crimes futuros, mas traz consigo uma série de consequências perigosas.

Ao reunir diversas vozes que têm um objetivo comum de construção de capacidade e conhecimento, seguido pela defesa da preservação da criptografia, buscamos equilibrar essa crescente preocupação social e encontrar soluções para essas demandas, soluções que se construam a partir da manutenção da integridade da ferramenta e da promoção e proteção dos direitos humanos online.

A defesa da criptografia não afasta a geração de princípios, alternativas e formas de colaboração para resolver o problema do mau uso na rede. É, portanto, necessário chegar a um consenso para estabelecer este tipo de mecanismo, mantendo o compromisso de manter uma criptografia forte.

É importante observar que o uso e preservação da ferramenta não implica falta de colaboração com os governos. Nesse sentido, é oportuno insistir em explorar a criação de processos que mantenham a integridade da criptografia e que permitam, por sua vez, colaborar com a prevenção do crime e com as Forças de Segurança em geral, ao utilizar informações não criptografadas. Os processos não devem implicar qualquer obrigação de fragilizar as proteções de segurança e privacidade presentes nas plataformas ou serviços. Além disso, os parâmetros legais de acesso pelas forças da lei a estas informações devem ter garantias de respeito à privacidade e aos direitos humanos. Deve-se promover a criação de espaços e diálogos voltados para a busca de acordos sobre boas práticas de colaboração.

A pandemia COVID-19 acelerou os esforços para expandir a conectividade e impulsionar a transformação digital. Mas, por outro lado, intensificou consideravelmente o debate sobre a privacidade e a segurança das comunicações" , bem como a exposição a riscos derivados de vazamentos de informação, entre outros

Mesmo em um contexto de criptografia, devemos procurar maneiras inteligentes de abordar questões legítimas de segurança e de enfrentamento a atores mal-intencionados,contribuindo para tornar os direitos e a segurança na rede mais fortes e melhores para todos os usuários.

Esta iniciativa se propõe a criar uma aliança regional multissetorial para a defesa e promoção da criptografia com o objetivo de estabelecer uma plataforma para a construção coletiva de capacidades e conhecimento na América Latina e no Caribe, a partir da criptografia como ferramenta essencial para a segurança e o respeito pelos direitos humanos e fundamentais na região, como a liberdade de expressão e a privacidade. Ao mesmo tempo, propõe-se avançar uma agenda proativa para promover e defender a criptografia na América Latina e no Caribe, que a fortaleça e gere um ecossistema de confiança, segurança e estabilidade da rede, abrangendo a infraestrutura crítica da Internet, seus aplicativos e serviços. Finalmente, a aliança objetiva coordenar esforços com as diferentes iniciativas em nível global, regional e nacional, gerando espaços de intercâmbio e mobilização diante do impacto do enfraquecimento da criptografia sobre direitos e a segurança.

MISSÃO DA AC-LAC

Uma proposta para a missão desta Aliança, que será discutida e refinada com seus participantes quando estiver operacional, é:

"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".