COALIZÃO DIREITOS NA REDE

A importância social e econômica da

Criptografia

Autoria
André Ramiro e Mariana Canto - Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

Revisão
Gustavo Rodrigues e Luiza Brandão - Instituto de Referência em Internet e Sociedade (IRIS)

Projeto gráfico e Diagramação
Felipe Duarte - Instituto de Referência em Internet e Sociedade (IRIS)

Grupo de Trabalho sobre Privacidade e Vigilância da Coalizão Direitos na Rede
André Ramiro, Mariana Canto e Raquel Saraiva - Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec
Amarela
Barbara Simão - Idec - Instituto Brasileiro de Defesa do Consumidor
Bruna Martins dos Santos e Joana Varon - Coding Rights
Camile Moura - Open Knowledge Brasil
Carlos Alberto Reis e Thiago Moraes - Laboratório de Políticas Públicas e Internet (LAPIN/UnB)
Carolina Israel
Cybelle Oliveira e Geraldo Barros - Casa Hacker
Eduardo Magrani - ITS-Rio - Instituto de Tecnologia e Sociedade do Rio de Janeiro
Fabrício Solagna - ASL - Associação Software Livre
Gustavo Rodrigues - Instituto de Referência em Internet e Sociedade (IRIS)
Henrique Parra e Rafael Zanatta - LAVITS - Rede latino-americana de estudos sobre vigilância, tecnologia e Sociedade
Helena Martins, Jamila Venturini, Marina Pita e Veridiana Alimonti - Intervozes - Coletivo Brasil de Comunicação Social
Janaina Spode - Casa da Cultura Digital Porto Alegre
John Razen e Paulo Renã - Instituto Beta: Internet & Democracia
Jorge Machado - Colaboratório de Desenvolvimento e Participação - COLAB
Leonardo Ribeiro da Cruz - LAVITS - Rede latino-americana de estudos sobre vigilância, tecnologia e Sociedade
Louise Marie Hurel - Instituto Igarapé
Malu Freire - Me Representa
Maraiza Adami - Actantes
Nathalie Fragoso - InternetLab
Paulo Lara - Artigo 19
Paulo Renã – Instituto Beta: Internet & Democracia
Renato Santa Rita - PROTESTE
Rita Freire - Ciranda da Comunicação Compartilhada
Thiago Novaes - Coolab - Laboratório Cooperativista de Tecnologias Comunitárias

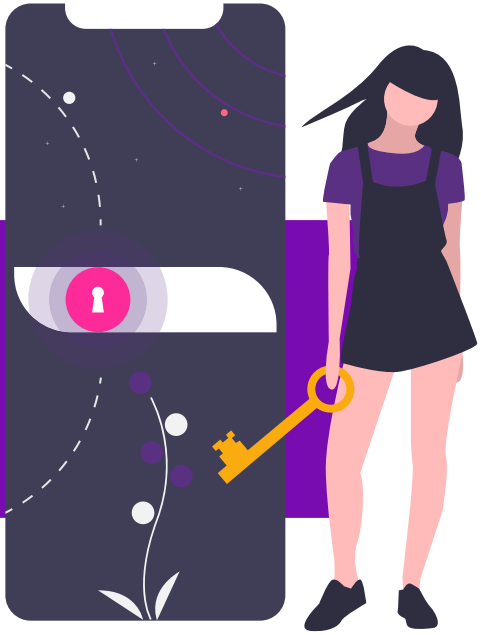
Apoio
FORD FOUNDATION

Apresentação

A Coalizão Direitos na Rede - formada por mais de 40 entidades da sociedade civil e acadêmicas atuantes em nome do acesso à Internet, da proteção da privacidade e da liberdade de expressão - produziu este material educativo para instruir a sociedade e os formuladores de políticas a respeito da importância social e econômica da criptografia e alertar para os riscos relacionados ao seu enfraquecimento.

Convidamos parlamentares, assim como outros setores da sociedade, como empresas, juristas e a sociedade civil, a voltar sua atenção à reflexão e ao debate, tão necessário no cenário político atual.

O QUE É CRIPTOGRAFIA?

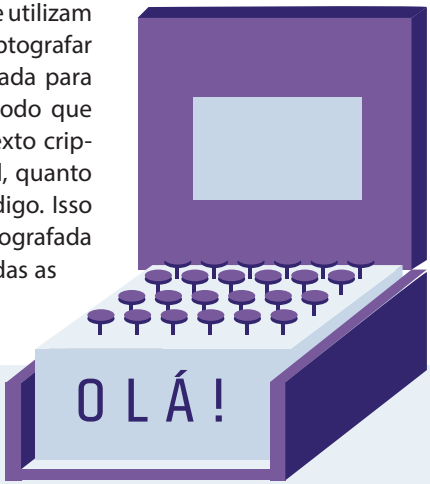


História e técnica

Criptografia é o processo de cifrar dados para que possam ser lidos apenas por alguém com os meios para decifrá-los. Desde a Antiguidade a técnica é utilizada como meio de garantir uma comunicação segura em contextos militares e diplomáticos, havendo registros de seu uso já pelo exército espartano na Grécia Antiga.

Com o passar dos milênios, novos métodos para a preservação das comunicações foram desenvolvidos até que, em meio à segunda Guerra Mundial as máquinas de encriptação desenvolvidas foram consideradas essenciais para o sucesso militar. Uma das mais famosas foi desenvolvida pelos alemães: a **Enigma**.

Hoje, a criptografia funciona por sistemas que utilizam uma ou mais chaves para criptografar e descriptografar informações. Uma chave é uma informação usada para controlar o funcionamento de uma cifra de modo que o detentor dessa informação pode decifrar o texto criptografado, similarmente a uma senha. Em geral, quanto mais longa a chave, mais difícil é decifrar o código. Isso porque, ao tentar decifrar uma mensagem criptografada por tentativa e erro, o invasor teria de tentar todas as combinações possíveis.

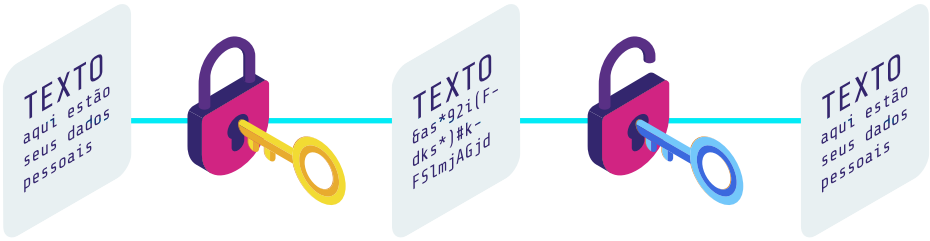


Em 1976, foi desenvolvido um método de distribuição de chaves, o método Diffie-Hellman, capaz de permitir a criação de diversos sistemas em que ninguém além de remetente e destinatário consegue acessar o conteúdo, nem mesmo o provedor do canal. Esses sistemas, baseados na chamada criptografia assimétrica, garantem o sigilo necessário, por exemplo, a transações comerciais e bancárias pela internet.

Já a partir do final dos anos 90, o uso da Internet para fins comerciais tornou ainda mais visível a importância da criptografia assimétrica, pois ela se tornou a técnica mais aceita para operações seguras de comércio eletrônico. Nos últimos anos, à medida que as conexões sem fio à Internet se tornam cada vez mais populares, a necessidade do uso da criptografia se reafirma, pois um alto nível de segurança nessas situações cotidianas é necessário.

Criptografia simétrica ou criptografia de chave privada

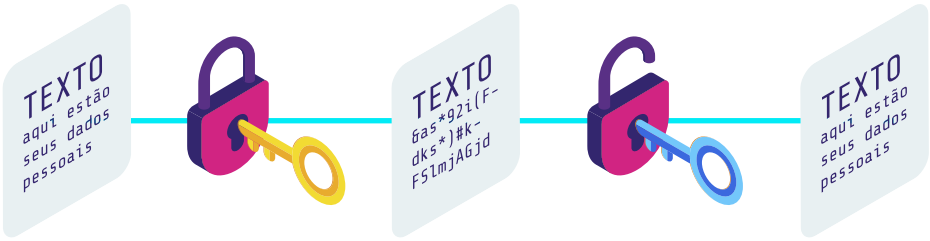
A criptografia pode ser dividida em duas modalidades: simétrica e assimétrica. A primeira, considerada mais simples, envolve a utilização de uma única chave. Assim, tanto o emissor (codificador) quanto o receptor (decodificador) da mensagem se utilizam da mesma chave para cifrar e decifrar a mensagem.



Entretanto, alguns desafios às vezes tornam a utilização desse modelo inviável. Além da necessidade de uma constante troca das chaves, constatou-se sua inaplicabilidade para fins de autenticação. Isso porque há o risco de interceptação durante a transmissão da chave privada do emissor para o receptor da mensagem. Assim, a chave poderia acabar em mãos de terceiros e seria necessária uma confiança inabalável no intermediário. Quem garante que o provedor do serviço não interceptasse , ele mesmo, as mensagens?

Criptografia assimétrica ou criptografia de chave pública

Para enfrentar os riscos de interceptação no modelo de chave simétrica, desenvolveu-se o modelo que busca, por meio do uso de duas chaves, aumentar o nível de segurança durante a troca de informações. Assim, o modelo usa pares de chaves criptográficas: uma chave pública, que pode ser amplamente disseminada, e uma chave privada, conhecida apenas pelo seu detentor. A chave de cifração é diferente da chave de decifração. Assim, uma chave é utilizada para cifrar a mensagem a outra para decifrá-la.



chave pública chave privada

Para garantir a confidencialidade da informação, a chave pública será utilizada para cifrar o texto e a chave privada será utilizada para decifrá-lo. O inverso também é possível. Para fins de autenticidade, no caso de assinaturas digitais, por exemplo, utiliza-se a chave privada para cifrar e a respectiva chave pública para decifrar a mensagem criptografada.

Hoje, a criptografia assimétrica é muito utilizada para garantir a segurança de navegadores, sites e e-mails.

A criptografia de ponta a ponta (end-to-end encryption ou E2EE) é uma implementação da criptografia assimétrica, usada atualmente em aplicativos como o Telegram e o WhatsApp. Desse modo, nenhuma pessoa além dos usuários envolvidos nas trocas de mensagem possui acesso ao conteúdo transmitido, nem mesmo as gestoras dos aplicativos

Além dos tipos de criptografia, é possível que seja aplicada para a proteção de dados em três modalidades:

1. DADOS EM REPOUSO OU ARMAZENADOS

Armazenados em dispositivos, como celulares e computadores. A criptografia funciona como um cofre e apenas a parte com a chave desse cofre pode ter acesso aos dados. O sistema de chave simétrica é o utilizado.

2. DADOS EM USO OU EM PROCESSAMENTO

Visualizados ou manipulados, quando, por exemplo, uma mensagem está sendo redigida. O dado poderia ser comparado à redação de um documento confidencial, em que apenas o seu detentor tem conhecimento do conteúdo. Como apenas uma pessoa tem acesso ao conteúdo do documento, terá a mesma chave, pelo sistema simétrico.

3. DADOS EM TRÂNSITO

Momento em que os dados são transferidos por meio de uma rede entre dispositivos. A dinâmica pode ser comparada ao serviço de correios. No caso das correspondências, a preservação do sigilo pode ser verificada por meio do lacre intacto. No meio digital, a garantia é o sistema de chaves assimétricas.

Importância para a segurança da rede
Previsão legal no Brasil

Para que serve a criptografia? Apesar de muitas vezes imperceptível, a criptografia faz parte da rotina de bilhões de pessoas. A segurança de dados é central não só para o sigilo das comunicações e do bem-estar individual, mas também para a estabilidade e continuidade da oferta de produtos e serviços no meio digital. Ela é cada vez mais importante à medida que conectamos serviços essenciais para a sociedade à rede. Isso inclui serviços de saúde, bancários, de provimento de energia e de comércio eletrônico.

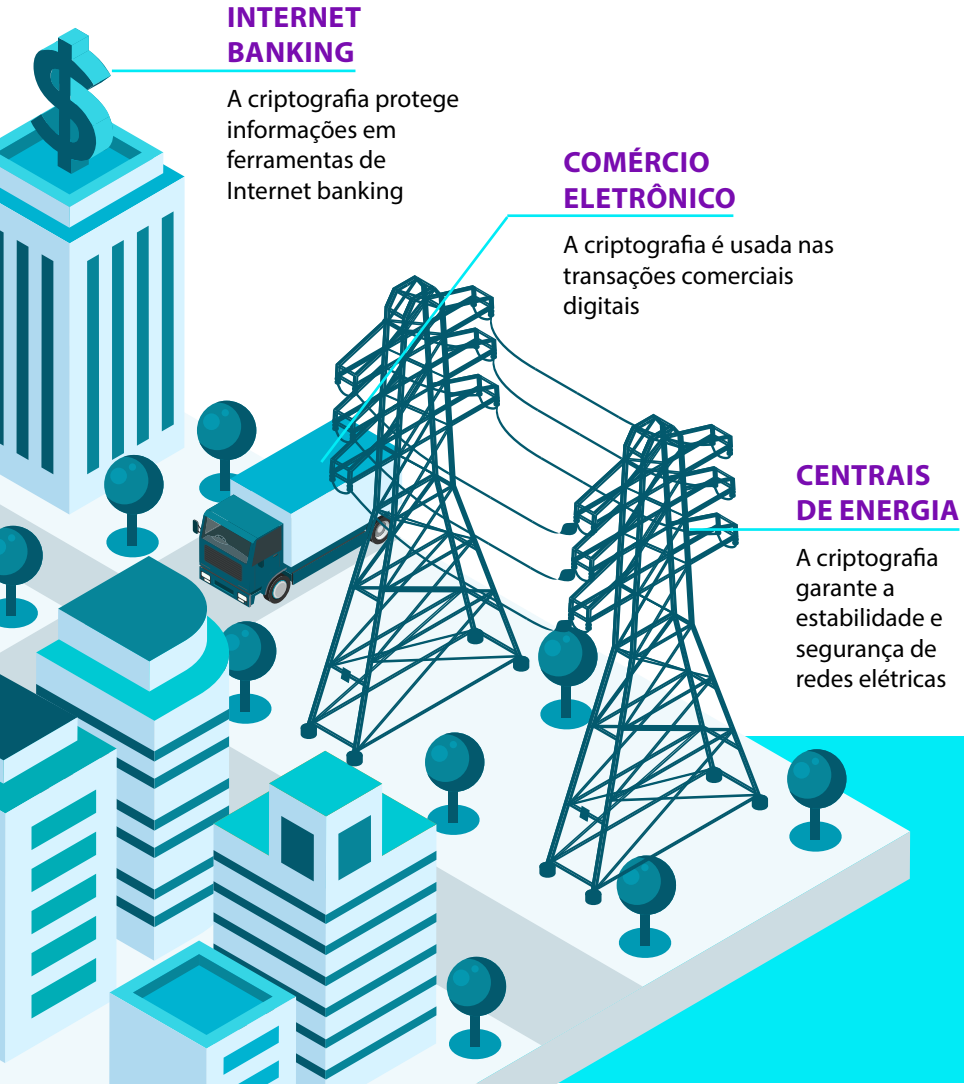
APLICATIVOS DE MENSAGEM

A criptografia garante o sigilo e a integridade das mensagens em aplicativos

SERVIÇOS DE SAÚDE

A criptografia protege dados sensíveis de pacientes e sistemas digitais hospitalares

Além de ser essencial para preservação do direito à liberdade de expressão e do sigilo das comunicações (previstos na Constituição Federal, art 5º, IX e XII) , a criptografia é uma peça chave na proteção dos direitos à privacidade e à proteção de dados (previstos no Marco Civil da Internet e na Lei Geral de Proteção de Dados). O uso de "recursos criptográficos no âmbito da sociedade em geral" no Brasil também é recomendado pela Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222/2020), que incentiva o "desenvolvimento de competências e de soluções em criptografia". A Estratégia inclui a criptologia, a ciência que estuda a criptografia, como "matéria de extrema relevância" em projetos de pesquisa e de inovação nacionais.



ARCABOUÇO LEGAL PROTETIVO

Legislação	Conteúdo
Estratégia Nacional de Segurança Cibernética - Decreto nº10.222/2020	Recomenda a adoção e o desenvolvimento de soluções nacionais de criptografia; Aponta a criptografia como método eficiente para mitigar riscos e evitar ameaças digitais e atingir os "níveis desejados de proteção de dados em repouso ou em trânsito"; Recomenda o investimento na técnica de forma a considerar seu potencial e seu valor estratégico para a segurança da informação e para a segurança cibernética do País.
Lei Geral de Proteção de Dados - Lei nº 13.709/2018	Torna claro que medidas de proteção de dados de ponta devem ser adotadas em questões de segurança da informação. A lei incentiva indiretamente a adoção da criptografia em seu artigo 46.
Política Nacional de Segurança da Informação - Decreto 9.637/2018	Ressalta a importância da criptografia para proteção do sigilo das comunicações da alta administração pública, incentivando a utilização de recursos criptográficos adequados aos graus de sigilo exigidos no tratamento das informações.
Decreto Regulamentador do Marco Civil da Internet - Decreto 8.771/2016	Estabelece que os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, fazer uso e soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

A importância social da criptografia: protegendo direitos fundamentais

A criptografia acompanhou o desenvolvimento da Internet. Por meio dela, cada vez mais, ocorrem atividades do cotidiano, como transações financeiras, relações profissionais, familiares e manifestações de ideias, emoções e sentimentos sobre religião, sexualidade e, por fim, política.

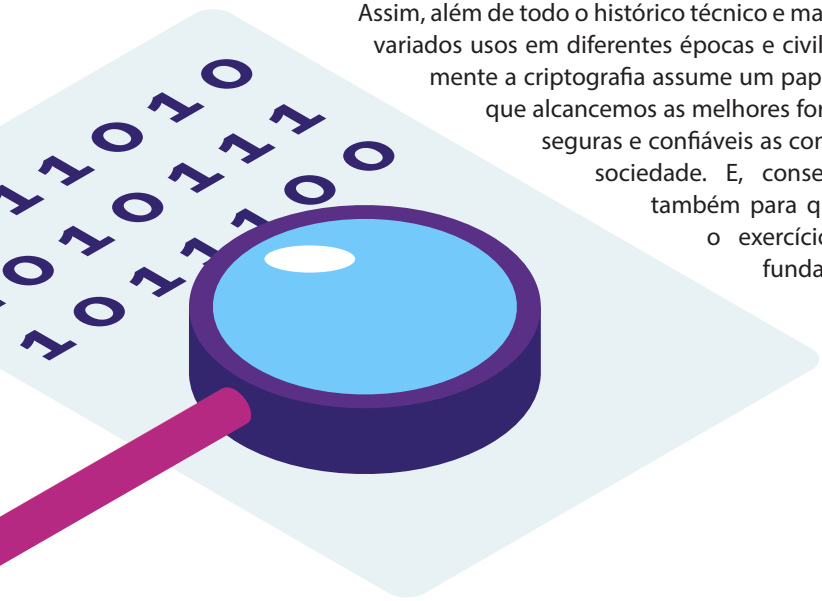
Enquanto as mais variadas camadas da vida em sociedade circulam em dados na rede, vazamento de dados, acesso por terceiros não autorizados, falsidade ideológica, ataques maliciosos e abusos governamentais, como vigilância e censura, são cada vez mais frequentes e impactam direitos como a privacidade e a liberdade de expressão na Internet. Segundo a Anistia Internacional[1], apenas com a segurança das comunicações é que usuários comuns da Internet, defensores de direitos humanos, ativistas e jornalistas investigativos podem se proteger tanto de cibercrimes, quanto dos olhos curiosos de governos do mundo todo.

Além da Constituição brasileira, a privacidade e a liberdade de expressão também são protegidas na Declaração Universal dos Direitos Humanos (arts. 12 e 19). Ninguém, portanto, deverá ser sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência. Da mesma forma, todo ser humano tem direito à liberdade de opinião e expressão. Isso inclui estar livre de interferências para procurar, receber ou transmitir informações e ideias por quaisquer meios - incluindo os criptografados. As mesmas garantias são reafirmadas no Pacto Internacional para os Direitos Civis e Políticos (ICCPR), ratificado pelo Brasil em 1992.

1 https://www.amnesty.org/en/documents/pol40/3682/2016/en/

Na medida em que mais dados são armazenados em aparelhos celular ou computadores pessoais, é notável o crescimento massivo de cibercrimes para obtenção de uma vasta quantidade informações para o cometimento de fraudes ou falsidade ideológica. Protocolos de segurança baseados em criptografia são uma proteção robusta contra esses ataques. O quadro se torna ainda mais sugestivo se notarmos a queda no número de furtos de celular desde que a Apple implementou criptografia de disco por padrão, como apontam estatísticas[2]. Sinal de que os dados, caso devidamente protegidos, se tornam inúteis a pessoas não autorizadas.

Isso é particularmente grave para figuras públicas, políticos ou indivíduos que assumem papéis sociais estratégicos, como diretores de grandes empresas, chefes governamentais, superintendentes de órgãos públicos, promotores ou juízes de direito. Caso suas informações caiam em mãos maliciosas e não estejam criptografadas, podem pôr em risco de vida testemunhas, o provimento de energia a uma cidade, a segurança empresarial ou o planejamento econômico de um país. Técnicas de criptografia das comunicações e dos dados armazenados permeiam grandes estruturas econômicas e sociais e afastam essas informações de mãos não autorizadas.



Assim, além de todo o histórico técnico e matemático, seus variados usos em diferentes épocas e civilizações, atualmente a criptografia assume um papel central para que alcancemos as melhores formas de tornar seguras e confiáveis as comunicações da sociedade. E, consequentemente, também para que efetivemos o exercício de direitos fundamentais.

2 https://slate.com/technology/2015/08/default-smartphone-encryption-will-stop-more-crimes-than-it-permits.html

Garantir a criptografia é fortalecer a privacidade

O crescente uso de dispositivos conectados (como sensores, smartphones, câmeras, aplicativos ou mesmo páginas web) multiplica, também, os meios pelos quais os Estados operam programas de vigilância ilegais. Esses programas envolvem desde a interceptação de mensagens, hacking governamental, formação de perfis comportamentais, infiltração em grupos políticos, até o mapeamento de deslocamento dos indivíduos. Muitas vezes, operam sem qualquer autorização judicial[3] e envolvem a criação de vulnerabilidades em sistemas de criptografia.

Ainda na década de 90, a Agência de Segurança Nacional (NSA) dos Estados Unidos tentou inaugurar um programa que envolvia a distribuição de chips para criptografar as ligações através de acordos com as empresas de telecomunicações. O sistema, no entanto, envolvia a criação de uma "porta dos fundos", um mecanismo de acesso excepcional para a agência. Assim, as comunicações dos cidadãos estariam sempre expostas à vigilância governamental. Conhecido como Clipper Chip[4], o programa sofreu grande oposição do setor privado e, principalmente, de organismos de defesa dos direitos humanos.

Edward Snowden, analista de sistemas e ex-contratado pela NSA revelou ao mundo um amplo programa de vigilância em massa operado pela agência[5]. As práticas envolviam desde acesso direto a dados de usuários em servidores de redes sociais até programas de quebra de criptografia de ponta, como o *Bullrun*

3 https://www.aclu.org/other/faces-surveillance-targets-illegal-spying
4 https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html
5 https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

O aumento no uso de criptografia nos últimos anos se deve bastante às sucessivas denúncias de vigilância em massa[6] e representa uma reação social a esses abusos. Os setores de investigação e inteligência dos Estados, consequentemente, reagem à dificuldade de monitorar as comunicações, reconfiguradas a favor da autonomia dos indivíduos. Assim, o direito à privacidade alcançado através da criptografia é atacado por operações tecnológicas e ações políticas dos governos. Narrativas, portanto, são construídas como forma de criminalizar a criptografia e justificar seu enfraquecimento.

A Freedom House documenta[7] a perseguição ilegal promovida pelo governo da Etiópia a sete blogueiros no país que realizavam trabalho jornalístico e eram críticos ao governo. De forma legítima, usavam recursos de criptografia para proteger suas informações, o que foi interpretado, de forma injusta, como atividade suspeita e análoga à prática de crimes. A privacidade, nesse caso, vai de encontro à cultura de acesso indiscriminado às comunicações típica de governos antidemocráticos, onde surgem novas narrativas para intimidar grupos que valorizam a segurança, a liberdade de expressão e o sigilo de suas comunicações.

Sem a criptografia, mesmo nos países considerados democráticos, como o Brasil, práticas abusivas do Estado levam à repressão de dissidentes políticos. No Caso Escher, o país foi condenado pela Corte Interamericana de Direitos Humanos pela interceptação ilegal, por 49 dias, de lideranças ligadas a movimentos sociais. Atualmente, com as comunicações por meios digitais, a criptografia se apresenta como meio necessário contra esses abusos.

Aparatos de observação e escuta ilegal das comunicações tolhem as diversas formas de expressão dos indivíduos, suas liberdades de pensamento, associação e reunião pacíficas e exercício de suas personalidades por projetarem uma auto-censura. A criptografia permite que, mesmo interceptadas ilegalmente, as comunicações não sejam lidas. É uma ferramenta, portanto, que efetiva a defesa internacional dos direitos humanos e dos direitos fundamentais assegurados pela Constituição Federal no Brasil.

6 https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/

7 https://freedomhouse.org/sites/default/files/inline_images/Freedom%20House_OHCHR_report_encryption%20and%20anonymity%20online.pdf

Criptografar comunicações é exercitar a liberdade de expressão

Meios de comunicação criptografados protegem o sigilo e desempenham importante papel na divulgação segura de informações. É fundamental para profissões de risco político, como jornalistas e defensores de direitos humanos, bem como de grupos vulneráveis, como comunidades LGBTQ+ e minorias étnicas e religiosas. Ao propiciar um canal seguro, a criptografia viabiliza a expressão dessas comunidades em seu máximo potencial, sem receios de represálias. Cria, portanto um espaço de privacidade que permite a livre formação e circulação de opiniões.

Investidas contra os meios de comunicação são artifícios comuns por parte de Estados autoritários, pois inibem o potencial de circulação de informações necessárias à construção política democrática. David Kaye[8] relata que governos antidemocráticos procuram enfraquecer a criptografia como forma de perseguir oponentes políticos e silenciar suas vozes: em 2014, o Irã decretou uma lei que deu margens à criminalização do uso da criptografia; em 2016, o Paquistão também seguiu o mesmo caminho, podendo punir o usuário de criptografia com prisão; e a Turquia chegou a prender centenas de usuários de aplicativos com criptografia, associando-a arbitrariamente com tentativas de golpe de Estado, em 2016.

Em 2016, o Alto Comissariado de Direitos Humanos da ONU à época, Zeid Ra'ad al Hussein, afirmou que

> **não é fantasioso ou exagerado afirmar que, sem ferramentas de criptografia, vidas podem estar em perigo.**
>
> *- Zeid Ra'ad al Hussein*

8 https://www.ohchr.org/Documents/Issues/Opinion EncryptionAnonymityFollowUpReport.pdf

De acordo com a Association for Progressive Communication (APC)[9] a livre circulação de ideias e opiniões não se limita a alcançar um grande público sem medo de sofrer interferências ou ameaças de responder judicialmente, mas também se relaciona à escolha de quais pessoas receberão aquela mensagem, ou seja, a autonomia para limitar seu alcance. Logo, a criptografia também protege a liberdade de expressão na medida em que assegura o compartilhamento de comunicações confidenciais com médicos, psicólogos, advogados ou mesmo com parceiros íntimos. Já para a atividade jornalística, a criptografia não somente protege a integridade do profissional, mas também o sigilo da fonte, afastando-a do comprometimento físico, emocional ou psicológico. Nos meios digitais - sujeitas, portanto, a vulnerabilidades típicas da rede - essas relações devem ser sigilosas, íntegras e sempre autênticas.

Ao proporcionar controle sobre o alcance das informações apenas para aqueles que têm permissão ou legitimidade para recebê-las, a criptografia cria canais de comunicação seguros para denunciantes. Tecnologias que fornecem criptografia - como os conhecidos Signal ou Pretty Good Privacy (PGP) - garantem a incolumidade de denunciantes de práticas ilegais de empresas, atos excessivos de setores do poder público e outros crimes, sem que sejam perseguidos ou assediados politicamente. Aqui, a liberdade de expressão não somente se relaciona com a visibilidade ou a vocalização das opiniões, mas também com a confidencialidade e com o sigilo.

O exercício da liberdade de expressão e a defesa da privacidade estão, intrinsecamente, relacionados entre si e são potencializados pela criptografia. Por isso tem uma posição central para a defesa contemporânea dos direitos e para a construção de confiança sobre o que trafega na Internet. Conseguiríamos exercer os direitos políticos e civis sem a presença dela? Dificilmente.

9 https://www.apc.org/en/news/anonymity-and-encryption-are-key-freedom-expressio

A importância econômica da criptografia

Dos novos modelos de negócio ao desempenho de infraestruturas críticas (como sistemas de fornecimento e distribuição de energia, controle de tráfego aéreo ou o funcionamento da própria Internet) necessitamos de robustos níveis de segurança.

Ao mesmo tempo, à medida em que mais sites, aplicativos e dispositivos se projetam nos meios digitais, novas dinâmicas econômicas se apresentam e podem oferecer um aumento nos níveis de geração de renda, faturamento e inovação tecnológica. Confiança e estabilidade desses sistemas são consideradas alicerces da economia moderna. Logo, a expansão de serviços e produtos baseados em novas tecnologias confirma a interdependência entre altos padrões de segurança e as relações de consumo.

A criptografia, ao desempenhar indispensável papel para a confiabilidade desses sistemas, contribui para a continuidade do crescimento econômico na medida em que torna informações íntegras, autênticas e sigilosas. Para que esta nova realidade econômica seja possível e sustentável, é fundamental que as tecnologias dos serviços e produtos impeçam vulnerabilidades ou brechas de segurança.

A criptografia como canal de confiança para o desenvolvimento das relações bancárias online

O acesso a contas de banco através de dispositivos conectados cresce a cada dia entre os brasileiros. A comodidade oferecida pelas transações, pagamentos, depósitos e outras operações via Internet faz do *online banking* um substituto às visitas às agências bancárias. Essa tendência se confirma com a redução dos custos de aparelhos celular e do acesso à Internet móvel. Hábitos de consumo de novas gerações, sobretudo, sugerem uma tendência de demanda por mais canais de comunicação online com serviços bancários.

Segundo a Pesquisa de Tecnologia Bancária de 2019[10], a cada 10 operações bancárias feitas pelos brasileiros, 6 são por meios digitais e 40% de todas as operações são feitas via dispositivos móveis. Sinalizando essa tendência, aponta-se que entre 2014 e 2018 foi identificado um aumento de 566% no uso de aplicativos de bancos. Enquanto isso, o Banco Central aponta uma redução no número de postos, agências e caixas de autoatendimento em detrimento do crescente uso de dispositivos móveis[11]. Esse cenário sugere que os padrões de segurança, especialmente protocolos de criptografia, devem acompanhar a reconfiguração do nosso relacionamento com esses serviços. Isso se torna ainda mais nítido em serviços financeiros pautados unicamente em plataformas digitais - as chamadas *fintechs*.

Qualquer espécie de interferência ou enfraquecimento nos mecanismos de criptografia põe em risco não apenas tanto os usuários - que podem ter suas informações vazadas e monetizadas em mercados paralelos - quanto amplas redes econômicas intermediadas pelos serviços bancários. Isso impacta concessões de crédito, empréstimos consignados, contas corrente ou serviços de poupança, além de dar margem para o aumento no número de clonagem de cartões e fraudes financeiras. A segurança e o desenvolvimento dessas operações apenas são alcançadas através da plena capacidade da criptografia.

10 https://www2.deloitte.com/br/pt/pages/financial-services/articles/pesquisa-deloitte-febraban-tecnologia-bancaria.html

11 https://www.revistaencontro.com.br/canal/economia/2018/11/cresce-uso-de-internet-banking-no-brasil.html

Segurança digital como engrenagem para novas gerações do comércio e consumo

Assim como na relação bancária, bons níveis de confiança e segurança digital são essenciais às relações entre setores do comércio e consumidores em um ecossistema conectado. Isso se reflete no desenvolvimento do comércio online (*e-commerce*), cada vez mais protagonista nas relações de consumo e projeções de inovação tecnológica.

Estatísticas apontam que cerca de 14% do total das vendas em varejo em 2019 se deram pela Internet[12] e, no Brasil, representante de um terço do total das vendas do comércio online na América Latina, estima-se que serão movimentados mais de 90 bilhões de reais em 2020[13]. É notável a importância de protocolos de criptografia sobre os dados em trânsito em sites e aplicativos a fim de gerar confiabilidade, autenticidade e sigilo para os mecanismos de compra e venda online.

A revolução na economia mundial leva à construção de políticas nacionais de incentivo ao comércio e aos novos negócios relacionado às contrapartidas sociais. Dia após dia, o planejamento econômico dedica-se à expansão de melhores infraestruturas para as tecnologias de informação e comunicação, bem como dos mecanismos de segurança que respeitem direitos dos consumidores. Nesse sentido, a Estratégia Nacional de Desenvolvimento Econômico e Social (ENDES) de 2019[14], no planejamento para uma economia digital até 2031, assume que devemos:

12 https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/
13 https://www.statista.com/topics/4697/e-commerce-in-brazil/
14 http://www.sudam.gov.br/conteudo/menus/retratil/planos-desenvolvimento/prda/arquivos/2019/estrategia-nacional-de-desenvolvimento-economico-e-social.pdf

incentivar **desenvolvimento da economia digital**, aumentando o apoio à difusão de tecnologias emergentes (interconectividade, automação, energias, nanotecnologia, novos materiais e biotecnologias, por exemplo) e suas aplicações no país;

estimular o **desenvolvimento de novas TICs**, com a ampliação da produção científica e tecnológica e a transformação do Brasil de um país usuário para desenvolvedor, gestor e distribuidor de tecnologias digitais, **acompanhando a fronteira econômica mundial**;

e **transformar a internet em um ambiente seguro, confiável, propício aos serviços e ao consumo, com respeito aos direitos dos cidadãos**

A confiabilidade dos processos de pagamentos, por exemplo, estaria comprometida sem os mecanismos de autenticação, integridade e sigilo sobre os dados em trânsito na rede que a criptografia oferece. Sem isso, além de onerar o consumidor com prejuízos financeiros e mais encargos ao poder de consumo, milhões de operações diárias de transferência e pagamento aos fornecedores de produtos seriam impossíveis. Também prejudicaria a inovação tecnológica, pois os novos mercados online se devem, em grande medida, à praticidade associada à segurança oferecida pela criptografia que acompanha essas plataformas.

Políticas de criptografia

A criptografia é amplamente compreendida como ferramenta essencial à garantia de direitos definidos na Constituição Federal e no plano internacional. Ao promover segurança técnica a aplicativos, sites e dispositivos, é um recurso fundamental ao exercício de direitos, como as liberdades de expressão e opinião, reunião e associação. Também fortalece o direito à privacidade dos indivíduos, sobretudo daqueles com maiores chances de serem vítimas de vigilância abusiva de governos, como movimentos sociais, jornalistas e dissidentes políticos.

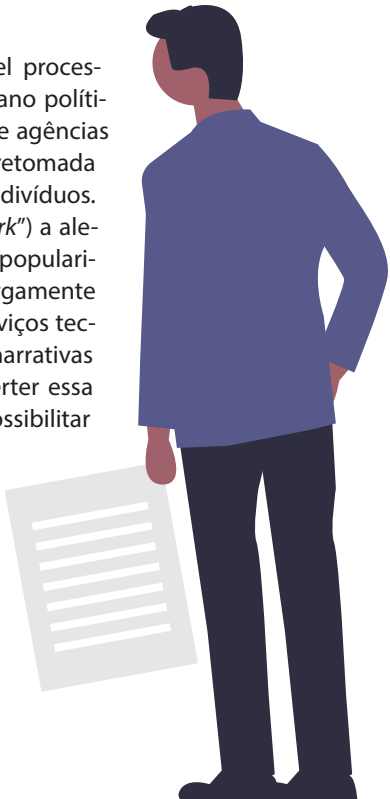
Contudo, agências de investigação ainda problematizam e buscam intervir no funcionamento das técnicas de criptografia em busca de seu enfraquecimento. Valendo-se de fatos políticos sensíveis que abalaram a opinião pública, criam narrativas contrárias a décadas de construção de entendimento científico sobre a importância técnica, econômica e social das ferramentas de encriptação. Esse panorama deu margem a tensões nacionais e internacionais que assumiram a forma de propostas legislativas, decisões judiciais e retóricas governamentais contrárias a fatos técnicos, entendimentos constitucionais e infraconstitucionais consolidados.

Como nascem e morrem as propostas anti-criptografia

As críticas a uma criptografia forte - historicamente provenientes de agências de investigação como o *Federal Bureau of Investigation* (FBI) ou do Departamento de Justiça (DOJ) dos Estados Unidos, com algumas expressões em agências brasileiras e de outras regiões - residem na defesa do acesso dessas agências às provas necessárias a uma investigação, como o conteúdo das comunicações de suspeitos. Isso porque as comunicações, em sua maioria, são feitas por meio de aplicativos de mensagens com criptografia ponta a ponta ou estão armazenadas em dispositivos criptografados, como aparelhos celular. Assim, mesmo com uma ordem judicial, não é possível acessar esses conteúdos.

Capítulo notável e representativo dessa disputa foi o ocorrido no contexto dos atentados na cidade de San Bernardino, na Califórnia. Entre 2015 e 2016, o FBI buscou o auxílio da Apple para obter acesso ao conteúdo do iPhone de um dos responsáveis pelo tiroteio. A empresa se recusou ou foi incapaz de cumprir com os consecutivos mandados judiciais. Já no Brasil, a impossibilidade técnica em cumprir ordens judiciais de acesso a dados de comunicações encriptadas ponta a ponta pelo WhatsApp levou à suspensão do aplicativo por três vezes no país[15]. Ambos os cenários desenham o plano de fundo geopolítico da criptografia e de suas expressões em território nacional.

Essas tensões não acontecem simplesmente à nível processual criminal, judicial ou legislativo, mas também no plano político. Rótulos são fabricados para reafirmar a campanha de agências governamentais para a flexibilização da criptografia e a retomada de tradicionais meios de acesso às comunicações dos indivíduos. Chamam, por exemplo, de "obscurecimento" ("*Going Dark*") a alegada crise nas capacidades investigativas em razão da popularização da criptografia[16]. Ao passo que a criptografia é largamente associada à segurança, à confiança e a resiliência de serviços tecnológicos pelos mais variados setores da sociedade, as narrativas das agências de investigação em questão buscam inverter essa lógica: a criptografia seria oposta à segurança, por impossibilitar o acesso às comunicações e informações encriptadas no âmbito de investigações criminais.



15 http://bloqueios.info/

16 https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

As propostas derivadas desses setores apostam, em sua maioria, em um modelo de criptografia que preveja um "**acesso excepcional**", ou seja, uma **porta dos fundos** que eventualmente forneça uma **brecha na segurança** para fins investigação criminal. Propostas dessa natureza, no entanto, não se sustentam porque qualquer vulnerabilidade proposital em um sistema criptográfico geraria um risco estrutural a todas as camadas de serviços e aplicações às quais a criptografia fornece segurança.

Em primeiro lugar, não é simples criar uma brecha de segurança em um mecanismo de criptografia. Especialistas em cibersegurança concordam que uma vulnerabilidade gera consequências não previamente antecipadas, pois cada recurso interage com diversos outros, gerando novas combinações de fragilidades inesperadas;

Os órgãos responsáveis por guardar essa chave para uma "porta dos fundos" serão vítimas de ataques. Há grande risco de concentração de investidas maliciosas nesses supostos guardiões da chave para uso "excepcional". Seria muito mais difícil administrar os acessos autorizados e não autorizados.

Além disso, veríamos um retrocesso no recurso de forward secrecy. Bastante utilizado em aplicativos de mensagem, por exemplo, permitem que uma chave nova seja gerada a cada mensagem, evitando que o acesso não autorizado a uma chave não comprometa o restante das comunicações. Para serem "eficazes" as propostas de acesso excepcional, apenas uma chave deveria dar acesso a toda a comunicação, aprofundando os riscos.

Por fim, a própria ideia de "excepcionalidade" pode ser veementemente contestada em razão da cultura de vigilância ilegal operada por diversos Estados. O monitoramento em massa das comunicações seria claramente facilitado, dando margem à violação estrutural de direitos.

É inverídica a dicotomia entre a privacidade conferida pela criptografia e a suposta segurança pública alcançada pelo "acesso excepcional". Na medida em que há riscos em qualquer cenário de criação de vulnerabilidade aos sistemas de encriptação, essas propostas não somente tornam as comunicações mais inseguras, como também geram riscos a informações sigilosas e críticas ao desenvolvimento econômico e à segurança nacional, cada vez mais atreladas às redes digitais de informação e à segurança cibernética. Além disso, agentes maliciosos, suspeitos cujas comunicações seriam perseguidas, podem facilmente migrar para outras plataformas, clandestinas, longe do radar das agências de investigação. Sequer a eficácia é garantida: inúmeros são os riscos e escassos são os proveitos das propostas de "acesso excepcional".Há consenso entre especialistas em segurança quanto à oposição a qualquer política de enfraquecimento da criptografia[17]. Tentativas de flexibilizá-la afetam negativamente o pleno funcionamento da Internet, o desenvolvimento tecnológico e o exercício de liberdades fundamentais, os quais dependem estreitamente do potencial de criptografar dados e comunicações.

A criptografia em juizo
As Crypto Wars brasileiras

Também no Brasil o acesso ao conteúdo de mensagens transmitidas por meio de aplicativos com criptografia de ponta a ponta, a exemplo do WhatsApp, gera diversas reações do judiciário e autoridades.

Decisões judiciais de bloqueio do aplicativo em todo território nacional - e além dele, já que o serviço em países vizinhos também foi afetado - geraram uma série de repercussões. Exemplos disso são as ações que, até a finalização desta cartilha, tramitam no Supremo Tribunal Federal relacionadas ao tema.

17 https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf

A Ação Direta de Inconstitucionalidade (ADI) nº 5527 trata do requerimento de suspensão imediata de bloqueios. Requer, ainda, a declaração de inconstitucionalidade dos incisos III e IV do art. 12 da Lei n. 12.965/14 (Marco Civil da Internet), sobre sanções como "suspensão" e "proibição" de serviços.

A ação surge em meio a um erro interpretativo dos incisos III e IV do Art. 12 já que estes não prevêem a suspensão de serviços em decorrência de descumprimento de ordem judicial de entrega de dados a investigações criminais. Na verdade, prevê as sanções em decorrência de violações da privacidade de usuários pelas empresas. Assim, as sanções se aplicam apenas a casos como vazamento de dados pessoais e do conteúdo de comunicações privadas e violações à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Nesse sentido, é o entendimento da Advocacia Geral da União, seguido pelo Senado Federal e respaldado pelo Comitê Gestor da Internet no Brasil (CGI.br): os incisos do art. 12 não representam uma norma inconstitucional, pois protegem direitos fundamentais e prevêem sanções para violações à proteção de registros, dados pessoais e comunicações privadas.

Em seu voto[18], a relatora da ADI, a Ministra Rosa Weber, ressalta que os bloqueios comprometem o exercício, por milhões de brasileiros, de liberdades fundamentais de expressão e comunicação asseguradas pela Constituição Federal. Também considera indevida a invocação ao Art. 12 do Marco Civil da Internet, pois o dispositivo não ampara bloqueios por descumprimento de ordem judicial.

> **O Estado não pode compelir aplicativo a oferecer serviço de forma menos segura com o pretexto de usar essa vulnerabilidade para acessar dados em investigações criminais**
>
> *- Rosa Weber*

18 http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

Weber lembra ainda que não há *trade-off* segurança pública e privacidade. Para ela, além de violar frontalmente a proteção da liberdade de expressão e a proteção do sigilo das informações, medidas de acesso excepcional como backdoors "tornar[iam] as tecnologias de comunicação menos seguras para todos os seus usuários". Essa opção, para a Ministra, é "potencialmente inócua", pois quem utiliza as aplicações com o intuito criminoso migraria para outros aplicativos fora do alcance das autoridades.

> **Seria um retrocesso limitar ou tornar ilegal a criptografia.**
>
> *- Rosa Weber*

Rosa Weber cita Zeid Raad Al Hussein, Alto-Comissário das Nações Unidas para os Direitos Humanos de 2014 a 2018, ao considerar o enfraquecimento da criptografia como abertura da Caixa de Pandora, que arrisca ativistas de direitos humanos, jornalistas, denunciantes e dissidentes políticos.

Assim, a Ministra julgou improcedente o pedido de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº 12.965/2014. Considerou que sua incidência não é sobre bloqueios em caso de descumprimento judicial.

O cenário da criptografia no Brasil tem ainda a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403. Proposta logo após a execução do segundo bloqueio judicial do aplicativo WhatsApp no Brasil, requer a suspensão dos efeitos da decisão de abril de 2015. Na época, a justiça penalizou a empresa Facebook Brasil por não atender ordens de interceptação. A ação busca estabelecer o entendimento que as ordens de bloqueios de aplicativos como o WhatsApp violam o direito à comunicação, a liberdade de expressão e de associação da coletividade.

O relator da ADPF, o Ministro Edson Fachin votou[19] que "os direitos que as pessoas têm offline devem também devem ser protegidos online. Direitos digitais são direitos fundamentais". O Ministro também embasou a sua decisão na garantia do direito à privacidade e à liberdade de expressão nas comunicações. Para ele, estes são condição para o pleno exercício do direito de acesso à internet.

Fachin considerou a criptografia e o anonimato especialmente úteis para o desenvolvimento e compartilhamento de opiniões. Para ele, a criptografia é "um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública".

> **Direitos digitais são direitos fundamentais.**
>
> *- Edson Fachin*

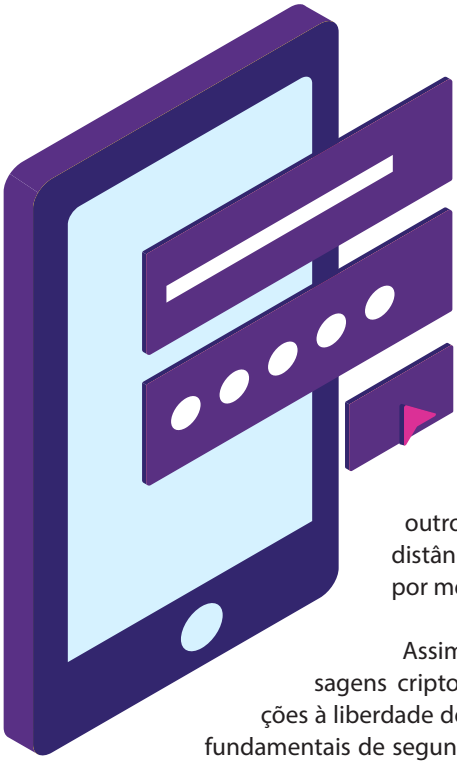
O Ministro afirma ser contraditório que, em nome da segurança pública, deixe-se de promover e buscar uma internet mais segura. Ele ressalta: "Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas.". Para Fachin uma medida que restringe direitos fundamentais deve ser "necessária", mais do que "útil", "razoável" ou "desejável", como indicou a Corte Europeia de Direitos Humanos (*The Sunday Times v. United Kingdom*, julgamento de 26 de abril de 1979, par. 59).

> **A criptografia é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública.**
>
> *- Edson Fachin*

Ele entende também que "o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional ou ainda outras soluções que diminuam a proteção garantida por uma criptografia forte". Escolhe

19 http://www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaPastaFachin/anexo/ADPF403voto.pdf

"afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet." Afirma a inconstitucionalidade de proibir a utilização da criptografia ponta-a-ponta, pois uma ordem como essa impacta desproporcionalmente aqueles mais vulneráveis[20].



Aplicativos de mensagem como possibilitadores do acesso a serviços essenciais

Muitas vezes, os bloqueios a certos aplicativos de mensagem impedem o acesso a serviços essenciais por eles viabilizados. Diversas Defensorias Públicas, por exemplo, ofereceram os seus serviços durante a pandemia da covid-19 pelo Whatsapp. Além da oferta de serviços durante calamidades públicas, outros serviços como o atendimento médico à distância e serviços bancários são possibilitados por meio dos aplicativos de mensagem.

Assim, a suspensão dos serviços de troca de mensagens criptografadas pode representar, além de violações à liberdade de expressão e comunicação, riscos a direitos fundamentais de segunda geração, como direito à saúde, trabalho, previdência social e assistência aos desamparados.

20 Até a finalização desta cartilha, o julgamento da ADI 5527 e da ADPF 407 encontra-se interrompido em razão do pedido de vistas solicitado pelo Ministro Alexandre de Moraes. O pedido paralisa o julgamento para que o magistrado possa estudar melhor o processo.

Recomendações

Aos legisladores e formuladores de políticas públicas:

* Encorajar a construção de políticas que visem a aplicação e desenvolvimento da criptografia na esfera pública. São necessárias para gerar segurança e estabilidade aos serviços essenciais à sociedade, bem como manter atualizada a segurança cibernética nacional.

* Desestimular propostas legislativas que visem o enfraquecimento, de forma direta ou indireta, da criptografia. Tais iniciativas são temerárias e oferecem riscos estruturais à segurança dos brasileiros e ao ecossistema de inovação tecnológica.

* Investir em diretrizes que estimulem a adoção de recursos criptográficos enquanto estratégia de estímulo ao comércio e outros serviços online. Atualmente, a criptografia é um ativo substancial para o desenvolvimento econômico nacional.

Aos membros do judiciário e autoridades com poderes investigativos:

* Consolidar o entendimento sobre a ilegalidade e desproporcionalidade de medidas judiciais que restrinjam o uso da criptografia. O bloqueio de aplicações em função da proteção conferida pela criptografia às comunicações não encontra respaldo legal. Para além do impacto às plataformas, a suspensão dos serviços atinge, desproporcionalmente, os usuários finais.

* Desestimular conduções processuais que envolvam o enfraquecimento da criptografia. Restrições à criptografia não reduzem a criminalidade. Pelo contrário, possibilitam um maior número de vulnerabilidades que podem ser exploradas por agentes criminosos, pondo em risco o usuário comum da rede e infraestruturas críticas.

* Buscar o constante diálogo com setores de interesse especializados, como a sociedade civil organizada e a comunidade científica. Essa aproximação, através de audiências públicas e eventos educativos sobre segurança da informação, por exemplo, é essencial para a tomada de decisões judiciais bem fundamentadas e para a persecução criminal que respeite os direitos fundamentais.

Aos provedores de aplicação

* Buscar a adoção de criptografia por padrão e ponta a ponta em serviços de comunicação e no armazenamento de dados. Compreende-se que recursos de sigilo, autenticidade e integridade são fundamentais para a segurança da cadeia de usuários, assim como para a interoperabilidade entre aplicações e jurisdições

* Desencorajar qualquer iniciativa de criação de backdoor ou políticas de acesso ao conteúdo encriptado. Além disso, cooperar com agências de investigação apenas mediante ordem judicial. Do contrário, o serviço irá desrespeitar o devido processo legal e criará mais brechas e vulnerabilidades ao sistema de segurança da aplicação e à Internet como um todo.

* Adotar e defender publicamente altos padrões de segurança, como a criptografia, contribuindo para a retomada da confiança do usuário na Internet e fomentando engajamento e inovação ao ecossistema tecnológico. Sucessivas revelações de vazamento de dados e violações à privacidade por parte dos setores público e privado vêm alimentando suspeições no usuário quanto aos interesses da plataformas.

Às organizações da sociedade civil:

* Posicionar-se expressamente em defesa da criptografia enquanto garantidora do exercício de direitos políticos e das liberdades liberdades de expressão, de imprensa, de associação.

* Estimular campanhas educacionais, eventos e outras formas de comunicação com o objetivo de popularizar as ferramentas e o conhecimento sobre a importância da criptografia. O entendimento sobre a criptografia não se resume ao público científico ou político. Pelo contrário, devido a sua importância, deve ser constantemente disseminado entre todos os setores da sociedade.

* Exercitar o potencial de tradução das questões técnicas e legais, de forma didática, a fim de agregar públicos mais amplos e diversos à defesa da criptografia. A defesa dos direitos fundamentais é um trabalho coletivo. Muitas vezes, também diz respeito ao setor público e empresarial, bem como às organizações do terceiro setor com agendas distintas. Portanto, depende de cooperações multissetoriais.

COALIZÃO DIREITOS NA REDE

direitosnarede.org.br

Direitos na Rede

direitosnarede

Direitos na Rede

@cdr_br