accessnow.org

accessnow

RESUMO DE POLÍTICA

10 fatos para combater os mitos da encriptação

A Access Now defende e estende os direitos digitais de usuários em risco em todo o mundo. Ao combinar suporte técnico direto, envolvimento político abrangente, defesa global, doações de base, intervenções jurídicas e convenções como a Rightscon, lutamos pelos direitos humanos na era digital.

RESUMO DE POLÍTICA

10 fatos para combater os mitos da encriptação

Agosto de 2021

Este resumo é uma publicação da Access Now. Ele foi escrito por Namrata Maheshwari. Gostaríamos de agradecer aos membros da equipe da Access Now que forneceram suporte, incluindo Raman Jit Singh Chima, Javier Pallero, Estelle Massé, Natalia Krapiva, Eric Null, Gustaf Björksten e Peter Micek. Também gostaríamos de agradecer aos participantes da reunião privada sobre encriptação e direitos humanos realizada durante o RightsCon 2021, que forneceram feedback sobre um esboço desta publicação.

A Access Now defende e estende os direitos digitais de usuários em risco em todo o mundo. Ao combinar suporte técnico direto, envolvimento político abrangente, defesa global, doações de base, intervenções jurídicas e convenções como a Rightscon, lutamos pelos direitos humanos na era digital.

Para mais informações entre em contato: Namrata Maheshwari em namrata@accessnow.org

Índice

I. Introdução

Durante o surto da pandemia COVID-19 em 2020, vimos um aumento sem precedentes na atividade online. Também testemunhamos um consequente aumento nos desafios de segurança cibernética. No mesmo ano, no entanto, o governo e os órgãos de aplicação da lei em muitos países emitiram declarações domésticas e internacionais profundamente problemáticas, exigindo essencialmente que a encriptação - uma ferramenta crítica para a segurança cibernética e a privacidade - fosse enfraquecida (consulte a Seção IV). Agora, na esteira das revelações do Projeto Pegasus que demonstram o quão vulneráveis nossas comunicações privadas são a hackers e exposição, ressaltando a necessidade de encriptação forte, estamos vendo novos apelos por parte das autoridades para enfraquecer os sistemas criptografados e a implementação de medidas tecnológicas para contornar a encriptação de ponta a ponta. Isso compromete ainda mais nossa privacidade e segurança online.

A encriptação é um processo de criptografia de codificação de informações de forma que apenas pessoas autorizadas (normalmente o remetente e o(s) destinatário(s)) podem decodificar ou descriptografar as informações com uma “chave”. A encriptação, portanto, garante que as comunicações entre duas ou mais partes sejam protegidas contra o acesso não autorizado de terceiros. No caso de encriptação ponta a ponta, mesmo o provedor de um serviço criptografado é incapaz de acessar as informações trocadas. A encriptação pode proteger os dados em trânsito (dados se movendo pela Internet ou uma rede privada) e os dados em repouso (dados armazenados em um dispositivo ou na “nuvem”).

Os benefícios da encriptação robusta são claros. Exemplos na vida diária incluem permitir transações bancárias e financeiras eletrônicas seguras, comunicações privadas confidenciais e a troca segura de informações confidenciais, como dados de saúde. A encriptação forte atende aos interesses de todas as partes interessadas em uma sociedade democrática. Ela protege indivíduos e comunidades reforçando o direito à privacidade, liberdade de expressão e liberdade de associação, permitindo comunicações privadas e armazenamento seguro de dados. A encriptação é benéfica para as empresas porque protege os segredos comerciais, inspira a confiança dos consumidores, limita as violações de dados e incentiva a inovação,

como a tecnologia de *blockchain* e redes privadas virtuais. E, finalmente, os órgãos de aplicação da lei e o governo precisam de encriptação para proteger a segurança nacional, informações confidenciais e dados dos cidadãos.

A finalidade deste artigo é responder a algumas das principais justificativas ou mitos que os governos confiam em suas demandas por acesso direcionado ou excepcional, ou *backdoors*, a sistemas criptografados, para expor as inconsistências e imprecisões inerentes. Mesmo que uma proposta de encriptação *backdoo*r pretenda atingir um objetivo legítimo, enfraquecer a encriptação para todos provavelmente não será uma abordagem necessária ou proporcional e será prejudicial aos direitos humanos, à segurança nacional, à democracia e à economia.

II. 10 fatos para combater os mitos da encriptação

Fato No. 1 Uma encriptação forte é essencial para a segurança da Internet

Mito: Os *backdoors* para acesso direcionado ou excepcional por parte das autoridades policiais não enfraquecerão a segurança da Internet

A encriptação é um processo inteiramente matemático. O conteúdo é criptografado e seguro ou não é - não se pode afirmar de forma significativa que o conteúdo é *principalmente* criptografado, ou seja, criptografado, mas com a possibilidade de um determinado terceiro obter acesso, caso deseje. Esse acesso excepcional essencialmente quebra a encriptação. Não existe uma forma tecnológica de permitir o acesso pelo governo sem também permitir o acesso de outros agentes não autorizados. Uma demanda do governo por acesso excepcional a um sistema criptografado, mas *de uma maneira que preserve a segurança*, é um conceito corretamente descrito como estando em guerra com a matemática.

Um *backdoor* para conteúdo criptografado é uma falha de segurança que torna todo o sistema e os dados subjacentes vulneráveis. O acesso direcionado ou excepcional, como exigem os órgãos de aplicação da lei, necessitaria a criação de um *backdoor* de alguma forma. Uma vez que essa fraqueza é criada, ela pode ser explorada por um conjunto de agentes mal-intencionados. Simplesmente não existe um *backdoor* para a qual apenas os "mocinhos" tenham as chaves. Como os cientistas da computação e especialistas em segurança explicaram, implementar mecanismos de acesso excepcionais significa exigir insegurança. Portanto, a afirmação de que um *backdoor* pode ser implementado com segurança é paradoxal. Aparafusar a porta da frente é de pouca utilidade se a porta dos fundos [*backdoor*] estiver destrancada - e um único backdoor coloca indiscriminadamente em risco a segurança de todos os usuários de um sistema criptografado.

Fato No. 2 Dar acesso excepcional à aplicação da lei ameaça os direitos humanos e a democracia

Mito: Os *Backdoors* de aplicação da lei não impactarão nossos direitos ou a democracia

A privacidade é essencial para ser humano. Ela permite que indivíduos e comunidades estabeleçam relações interpessoais, busquem aconselhamento médico ou jurídico sem medo de serem expostos e expressarem suas opiniões livremente - mesmo quando são impopulares ou controversas. Precisamos de privacidade simplesmente para pensar livremente. O conhecimento de uma possível vigilância tem um efeito sufocante no comportamento humano. Como observou o Tribunal Europeu dos Direitos do Homem, a mera existência de uma lei que autoriza o controlo secreto das comunicações está em conflito com a liberdade de expressão e o direito à privacidade. Isso é especialmente importante para jornalistas, médicos, advogados e pessoas alvo de discriminação ou abuso, que dependem de comunicações privadas para se manterem seguros. Em algumas circunstâncias, enfraquecer a encriptação e desmantelar a privacidade coloca vidas em risco.

Ao permitir a comunicação privada e desinibida, livre de vigilância, a encriptação protege os direitos humanos e as liberdades relativas à privacidade, liberdade de expressão e liberdade de reunião e associação. Esses direitos são fundamentais para o funcionamento de uma democracia saudável. A encriptação está, portanto, no centro dos direitos humanos na era digital e um ataque à encriptação é também um ataque aos direitos humanos e à democracia.

Fato No. 3 A encriptação forte fortalece a privacidade e a segurança

Mito: Para alcançar a segurança, devemos sacrificar a privacidade

Os defensores das *backdoors* de encriptação retratam incorretamente a privacidade e a segurança como parte de um jogo de soma zero em que os ganhos de um são necessariamente iguais às perdas do outro e vice-versa. Este enquadramento "privacidade versus segurança" tem como premissa um falso binário. Privacidade e segurança são princípios que se reforçam mutuamente.

A encriptação forte fortalece a privacidade e a segurança. Quando a comunicação e as informações pessoais são protegidas e as transações financeiras são protegidas, o resultado é uma redução nas violações de dados. Os benefícios da encriptação em fornecer uma defesa robusta contra ataques cibernéticos não são apenas para os indivíduos, mas também para o governo e órgãos de aplicação da lei que, de outra forma, teriam que lidar com as consequências desses ataques. A encriptação também é parte integrante da forte infraestrutura de segurança cibernética de que governos e órgãos de aplicação da lei precisam para proteger a segurança nacional. O enfraquecimento deliberado dos sistemas criptografados tornaria, portanto, alvos fáceis de indivíduos, governos e empresas, e daria aos agentes mal-intencionados a capacidade de usar vulnerabilidades nesses sistemas como armas. Um enquadramento mais apropriado do debate seria, portanto, "segurança versus segurança", já que a encriptação não apenas protege a privacidade, mas também a segurança. Uma política de "segurança" que visa a encriptação pode facilmente se tornar uma política de "insegurança", criando mais perigos do que visa prevenir.

Fato No. 4 A aplicação da lei entrou na era de ouro da vigilância - sem quebrar a encriptação

Mito: A aplicação da lei está enfrentando um problema de "escurecimento", o que torna necessário quebrar a encriptação

Os órgãos de inteligência e aplicação da lei reclamam que a encriptação evita a interceptação - um fenômeno conhecido como "escurecimento". A implicação é que as mudanças tecnológicas diminuíram suas capacidades de vigilância. No entanto, a metáfora "escurecer" merece ser questionada.

Ele ignora o fato de que as mudanças tecnológicas disponibilizaram muito mais dados sobre os indivíduos do que nunca. O que vemos hoje não é uma era de "escurecimento", mas sim uma "era de ouro da vigilância", na qual detalhes sobre nossas vidas íntimas, incluindo informações de localização, informações sobre nossos contatos e muitos outros detalhes não registrados anteriormente podem ser facilmente compilados em "dossiês digitais". O aumento sem precedentes de atividade online durante a pandemia COVID-19 apenas aumentou nossas pegadas digitais. Além disso, um relatório do Centro Berkman Klein para Internet e Sociedade da Universidade de Harvard concluiu que a encriptação não é tão difundida quanto os governos sugerem, nem é provável que se torne assim. Enquanto isso, o crescimento da "Internet das Coisas" provavelmente introduzirá novos vetores para vigilância por meio de nossos dispositivos, aumentando o número de pontos fracos de segurança a serem explorados.

Nada disso é novo. As revelações de Snowden em 2013 deixaram claro quantos dados de usuários os governos podem adquirir por meio de programas de vigilância excessivos. A tecnologia digital não está mergulhando nossos dados no escuro; pelo contrário, está tornando-os mais vulneráveis à exposição. Na verdade, mesmo com encriptação e outras ferramentas para proteger os dados, limitar o alcance da vigilância exigirá que organizações e empresas sigam princípios rígidos de minimização de dados e governos implementem reformas significativas de vigilância que protejam direitos e liberdades.

Fato No. 5 O enfraquecimento da encriptação não impedirá que criminosos e terroristas usem encriptação forte

Mito: O enfraquecimento da encriptação é uma medida eficaz para combater o terrorismo e a atividade criminosa

Se as empresas de tecnologia forem obrigadas a introduzir *backdoors* em seus softwares e aplicativos, o único resultado certo será que o público em geral será privado de sua capacidade de escolher uma plataforma onde os direitos fundamentais sejam protegidos e os dados não corram risco. Os criminosos, incluindo terroristas, simplesmente mudarão para plataformas criptografadas disponíveis em jurisdições estrangeiras ou no mercado negro, ou podem até criar as suas próprias. É mais provável que essas plataformas estejam fora do alcance da lei e da aplicação da lei, tornando ainda mais difícil prevenir e investigar o crime. Atualmente, embora as plataformas criptografadas protejam o conteúdo das comunicações dos usuários, na maioria das jurisdições, a aplicação da lei tem o poder de acessar metadados e outras informações que auxiliam significativamente nas investigações. Dada a sensibilidade dos próprios metadados, é imperativo que tal acesso seja permitido apenas quando severamente alinhado com os princípios da necessidade e da proporcionalidade. O uso de metadados para vigilância em massa e mandatos que exigem a retenção de metadados são presumivelmente contrários aos direitos humanos.

O aumento das capacidades de vigilância frequentemente leva à vigilância invasiva sem provas suficientes de sua eficácia. A própria criação da capacidade de acessar informações criptografadas pode levar a uma vigilância não direcionada, em violação dos princípios de minimização de dados e da necessidade e proporcionalidade. Em uma investigação da eficácia da vigilância para prevenir o terrorismo, um estudo nos EUA sugere que a ligação entre o aumento das capacidades de vigilância e a prevenção de ataques é tênue. Em 2004, o FBI analisou um programa de vigilância envolvendo atividades de coleta em massa de telefone e e-mail para discernir quantas haviam feito uma "contribuição significativa para identificar terroristas, deportar um suspeito de terrorismo ou desenvolver um informante confidencial sobre terroristas". Entre 2001 e 2004, apenas 1,2% das dicas cabem na conta. Entre 2004 e 2006, nenhuma das dicas se mostrou útil. Portanto, enfraquecer a encriptação para ampliar a capacidade de vigilância não apenas prejudicaria a segurança da Internet e prejudicaria o público em geral, mas não forneceria necessariamente qualquer capacidade significativa, sustentada e aprimorada para prevenir o terrorismo. Enfraquecer a segurança de todos pela mera possibilidade de identificar alguns malfeitores online é uma abordagem

totalmente desproporcional, colocando em risco a privacidade e a segurança de todos os usuários de uma plataforma sem provas que mostrem que ela alcançará seu objetivo de impedir ataques.

Fato No. 6 A encriptação forte contribui para a segurança das crianças online

Mito: A encriptação torna a Internet insegura para crianças

Alguns proponentes da quebra da encriptação veem isso como uma solução para o problema do Material de Abuso Sexual Infantil (CSAM) online. Porém, assim como outros criminosos, os perpetradores recorrerão a plataformas criptografadas alternativas oferecidas em outras jurisdições ou no mercado negro, ou criarão suas próprias plataformas criptografadas para ocultar suas atividades. Isso significa que o problema persistirá - ele simplesmente ficará fora do alcance da aplicação da lei, impedindo o acesso legal até mesmo aos metadados que podem ser instrumentais nas investigações.

Deve ser enfatizado que a retenção de metadados não deve ser obrigatória. O acesso a quaisquer dados pelas autoridades policiais, incluindo metadados, deve ser permitido apenas dentro de uma estrutura legal que priorize os direitos humanos e obedeça a padrões rígidos de necessidade e proporcionalidade.

Mais importante ainda, as crianças precisam de privacidade e encriptação forte para se manterem seguras online. Elas precisam de plataformas criptografadas onde a identidade das pessoas com as quais estão interagindo possa ser autenticada e onde suas informações pessoais não corram o risco de serem expostas a terceiros. A Convenção das Nações Unidas sobre os Direitos da Criança reconhece que, entre outras coisas, as crianças têm direito à privacidade, liberdade de expressão, acesso à informação e liberdade de associação. A UNICEF enfatizou a importância de proteger esses direitos das crianças online. Além disso, uma pesquisa da UNESCO indicou que a privacidade é importante para mais de 90% dos jovens entrevistados que acreditam que podem ficar seguros online adquirindo as informações e competências tecnológicas necessárias. A encriptação é uma das melhores ferramentas de que dispomos para nos mantermos seguros e protegidos online. Devido à pandemia e ao aprendizado remoto, mais crianças estão online. Consequentemente, os

governos devem encorajar o uso de encriptação forte para manter as crianças seguras, e não introduzir deliberadamente vulnerabilidades de segurança na tecnologia que elas usam.

Fato No. 7 A obrigatoriedade de "rastreabilidade" colocará em risco a privacidade e a liberdade de expressão

Mito: A rastreabilidade deve ser implementada para evitar a disseminação de desinformação

Os governos propuseram combater a disseminação da desinformação por meio de plataformas de mensagens online, exigindo "rastreabilidade". Tal mandato exigiria que os intermediários rastreassem a origem do conteúdo que circula em suas plataformas. A rastreabilidade desafia a segurança oferecida pela encriptação de ponta a ponta e é problemática por uma série de razões que descrevemos a seguir. Não é apenas um impedimento aos direitos fundamentais, ela tem uma utilidade limitada na prática.

A implementação da rastreabilidade exigiria plataformas criptografadas de ponta a ponta para desenvolver uma nova capacidade de discernir quem enviou qual mensagem para quem, quando e, em alguns casos, de onde. No momento, eles não têm essa capacidade para proteger a privacidade e a segurança. A rastreabilidade obrigaria as plataformas criptografadas de ponta a ponta a serem fundamentalmente reprojetadas, para permitir o acesso e o armazenamento de informações sobre os usuários e suas comunicações de uma forma que atualmente não é possível. Tecnólogos explicaram que rastreabilidade e encriptação ponta a ponta não podem coexistir. Não importa como a rastreabilidade seja implementada, ela terá um impacto adverso na privacidade e na segurança, que constituem a promessa central da encriptação de ponta a ponta.

Ao colocar o anonimato e o direito à privacidade em risco, a rastreabilidade teria inevitavelmente um efeito negativo sobre a liberdade de expressão. Os indivíduos não se comunicarão livremente devido à possibilidade de sofrer consequências caso a mensagem seja amplamente divulgada. Isso constitui uma ameaça aos próprios alicerces de uma democracia. A mera viralidade de uma mensagem não deve ser motivo de culpabilidade ou suspeita. Além disso, a eficácia prática da rastreabilidade é duvidosa. O originador de uma mensagem em uma plataforma específica pode não ser o criador do conteúdo. Além disso, a

prevalência de desinformação em plataformas de mídia social indica que a rastreabilidade pode não ser um impedimento útil.

Finalmente, o argumento de que a rastreabilidade envolve apenas a coleta de metadados, não de conteúdo e, portanto, não viola a privacidade ou a liberdade de expressão, é enganoso. O objetivo declarado da rastreabilidade é descobrir *quem* enviou uma determinada mensagem, porque a aplicação da lei já sabe o que estava na mensagem e a considerou problemática. Nesses casos, são os metadados, ou seja, quem enviou a mensagem, para quem e quando, que protegem a privacidade e a liberdade de expressão dos indivíduos. Como afirmamos acima, a coleta de metadados deve obedecer rigorosamente aos direitos humanos e aos princípios do necessário e proporcional. A implementação da rastreabilidade vai contra esses princípios. Isso implicará necessariamente na coleta e retenção massiva de metadados, o que comprometerá a privacidade e a segurança de bilhões de usuários, pela mera possibilidade de identificar certos agentes mal-intencionados.

Fato No. 8 A encriptação forte é crucial para a segurança cibernética e protege a segurança nacional

Mito: o acesso excepcional ao conteúdo criptografado é necessário para proteger a segurança nacional

A encriptação forte é vital para uma infraestrutura de segurança cibernética resiliente que proteja a segurança nacional. Isso inclui garantir que a encriptação padrão de ponta a ponta proteja as comunicações confidenciais realizadas rotineiramente pelo governo e oficiais de inteligência. Ademais, quando os sistemas e plataformas comumente usados são mantidos seguros usando encriptação, isso também protege a nação. Se apenas alguns indivíduos ou organizações implantam a encriptação, ou a usam apenas para determinados fins, ela sinaliza automaticamente o valor dos dados e aumenta o risco de um ataque.

O aumento de incidentes de segurança cibernética e violações direcionadas é um argumento a favor, e não contra, a encriptação forte. Esses ataques, envolvendo uma série de órgãos, funcionários e indivíduos com dados confidenciais, incluindo órgãos federais nos EUA, o Presidente e o Primeiro-ministro da Índia e ativistas, jornalistas e empresários, colocam a segurança nacional em risco. Sem encriptação forte, veríamos mais acesso não autorizado e

exposição de informações confidenciais e informações pessoais dos cidadãos em conjuntos de dados do governo, um benefício para os cibercriminosos ou adversários patrocinados pelo estado. Também veríamos ataques mais bem-sucedidos à infraestrutura essencial, como sistemas de saúde, eleições e transporte público, pois os sistemas criptografados ajudam a manter suas operações seguras.

Fato No. 9 A encriptação forte mantém a confiança no ecossistema digital e apoia o crescimento econômico

Mito: Enfraquecer deliberadamente a encriptação não terá efeito na economia

A encriptação é crítica para manter a confidencialidade e autenticidade dos dados no ecossistema digital. Por exemplo, os bancos confiam amplamente na encriptação para facilitar as transações, garantir a proteção das informações da conta e de outros dados do cliente e proteger os segredos comerciais. A encriptação também garante que os clientes confiem nas instituições bancárias. Essa base de confiança e segurança alimenta a inovação e estimula o desenvolvimento de uma infraestrutura tecnológica resiliente, impulsionando a competição da indústria e contribuindo para o crescimento econômico de um país. Assim, a encriptação é a pedra angular da economia digital moderna.

Enfraquecer deliberadamente a encriptação imporia custos elevados para as empresas que dependem dela e causaria um impacto adverso na economia. A carga de conformidade imposta por leis para enfraquecer a encriptação obrigou as empresas de tecnologia a se retirarem do mercado em alguns países. Esse tipo de recuo não prejudica apenas a concorrência e a inovação, mas também afeta o emprego. Em um país que prejudica a encriptação, o mercado sofrerá a perda de empresas que oferecem ou dependem de produtos e serviços de segurança, e as empresas serão desestimuladas a inovar e desenvolver tais produtos.

Além disso, a encriptação forte pode prevenir ou mitigar o impacto dos incidentes de segurança cibernética que, de outra forma, causariam mais danos e custariam mais dinheiro. Os incidentes de segurança cibernética são generalizados e 80% das empresas europeias

sofreram pelo menos um desses incidentes. Na Índia, quase 1,16 milhão de ataques cibernéticos foram relatados em 2020. O custo médio de uma única violação de dados é de aproximadamente US$ 3,86 milhões. A encriptação reduz o risco dessas violações e controla os custos, em benefício dos interesses comerciais e da economia como um todo.

Fato No. 10 Os órgãos de aplicação da lei e inteligência não precisam quebrar a encriptação para investigar o crime

Mito: As autoridades não têm alternativa a não ser quebrar a encriptação

A criação de *backdoors* de encriptação pode permitir que as autoridades acessem os dados que procuram em certas circunstâncias, mas isso não estabelece que as deficiências de segurança deliberadas obrigatórias sejam necessárias, proporcionais ou mesmo adequadas para atingir os objetivos de aplicação da lei ou inteligência em democracias modernas que respeitam os direitos. Conforme discutimos, os órgãos de inteligência e aplicação da lei já se beneficiam do vasto aumento de dados sobre indivíduos disponíveis na era digital. Há muitas alternativas para enfraquecer a encriptação para investigar crimes.

Um exemplo de dados frequentemente disponíveis às autoridades são os metadados das comunicações. Eles podem ser instrumentais para as investigações, contanto que sejam acessados de acordo com os princípios internacionais sobre a aplicação dos direitos humanos à vigilância das comunicações, incluindo os princípios da necessidade e da proporcionalidade. Esses padrões rígidos para o acesso legal aos dados são necessários porque mesmo os dados que não são o conteúdo das comunicações revelam um retrato íntimo de nossas atividades. As autoridades policiais também podem obter testemunhos diretos das partes envolvidas na comunicação e, em alguns casos, podem acessar o conteúdo por meio de *back-ups* de dados.

Além disso, mesmo que o conteúdo das comunicações eletrônicas possa ser útil em alguns casos, raramente é a única prova. Na grande maioria dos casos, os órgãos de aplicação da lei ainda dependem principalmente de provas tradicionais, como testemunhas, informantes, provas físicas e registros comerciais de bancos e empresas de telefonia celular. Vale observar que muitas vezes há situações em que certa quantidade de provas se torna inacessível para a aplicação da lei por uma série de razões. Por exemplo, um usuário exclui permanentemente uma comunicação ou a filmagem de uma câmera de segurança é danificada.

Conclusão: é impossível obter 100% de todas as provas potencialmente disponíveis 100% do tempo. Tentar fazer isso será praticamente impossível e pode violar os direitos das pessoas. Criar *backdoors* de encriptação e enfraquecer a segurança de todos na tentativa de obter todas as provas possíveis em casos específicos não se alinha aos direitos humanos e às liberdades e, na prática, nunca será um substituto para um bom trabalho investigativo.

III. Conclusão: Precisamos de mais segurança na internet, não menos; a encriptação deve ser reforçada, não enfraquecida

Não há dúvida de que devemos abordar as questões de segurança infantil, desinformação, segurança nacional e atividade criminosa na era digital. No entanto, mesmo que o objetivo final declarado para obrigar *backdoors* de encriptação seja legítimo, os meios devem ser necessários e proporcionais. A introdução deliberada de pontos fracos de segurança em sistemas criptografados falha neste teste. O enfraquecimento da encriptação criará mais perigos do que evitará. Além disso, não há base de provas para afirmar que quebrar a encriptação alcançará os resultados desejados. Na melhor das hipóteses, o acesso excepcional ao conteúdo criptografado servirá apenas como uma solução de curto prazo ou parcial para a aplicação da lei.

Conforme explicamos neste resumo, a encriptação é uma ferramenta vital para a proteção dos direitos humanos, da democracia, da segurança cibernética e da economia. O direito à privacidade e o direito à liberdade de expressão são direitos humanos básicos e, no mundo digital de hoje, não podemos separar significativamente esses direitos da necessidade de canais de comunicação online seguros, livres de vigilância indevida. A encriptação é um bloco de construção crucial para uma infraestrutura tecnológica segura, e os governos devem promover seu uso, não buscar repetidamente enfraquecê-la.

IV. Anexo

a. Principais declarações sobre encriptação por governos e autoridades

DECLARAÇÕES INTERNACIONAIS

26 de julho de 2021	Opinião de Catherine De Bolle, diretora executiva da Europol; e Cyrus R. Vance, Jr., o procurador distrital do Condado de Nova York, Nova York	“Encriptação não regulamentada é justiça negada” Fonte: Politico
10 de junho de 2021	Declaração conjunta sobre a visita ao Reino Unido do presidente dos EUA, Biden, a convite do primeiro-ministro Johnson, do Reino Unido	"Esperamos colocar em vigor um acordo bilateral robusto de acesso a dados, baseado no reconhecimento mútuo de que ambos os países têm um nível adequadamente alto de proteção de dados, que permite investigações de aplicação da lei em ambos os lados do Atlântico para obter as provas necessárias para levar os infratores à justiça, mantendo padrões de privacidade rigorosos. Trabalharemos juntos para manter o acesso legal severamente controlado ao conteúdo de comunicações que é vital para a investigação e o julgamento de crimes graves, incluindo terrorismo e abuso infantil. E trabalharemos em parceria com empresas de tecnologia para fazer isso, protegendo a segurança de nossos cidadãos. " Fonte: Declaração Conjunta EUA-Reino Unido
2020	Relatório de Segurança de Munique	“Frequentemente ultrapassando os extremistas jihadistas no uso e alcance de postagens nas redes sociais, os extremistas de direita contam fortemente com as plataformas da internet para comunicar e disseminar suas ideias. Com o aumento da remoção de conteúdo extremista por plataformas como Twitter, Facebook e YouTube, extremistas de direita mudaram cada vez mais para aplicativos criptografados como Telegram e Discord, bem como plataformas não regulamentadas como 8chan ou Gab. Esses ‘cantos longínquos da internet’ também contribuem decisivamente para os processos de auto-radicalização. ” Fonte: Relatório de Segurança de Munique 2020

11 de out. de 2020	Five Eyes, Índia e Japão	Declaração Internacional: Encriptação de ponta a ponta e segurança pública Exige *backdoors* para que as autoridades tenham acesso a conteúdo criptografado no interesse da segurança pública.
Set. de 2020	Comissão Europeia	Relatório intitulado "Soluções técnicas para detectar abuso sexual infantil em comunicações criptografadas de ponta a ponta" Analisou diferentes métodos para identificar Material de Abuso Sexual Infantil (CSAM) em comunicações eletrônicas privadas que usam encriptação ponta a ponta.
Set. de 2020	Comissão Europeia	Uma nota interna indicou que a Comissão Europeia está contemplando formas de permitir o acesso da aplicação da lei a comunicações criptografadas de ponta a ponta, dentro de um quadro jurídico adequado, para abordar o CSAM e o crime organizado. Fonte: [Agora a U. E. Está Deliberando Sobre o Acesso das Autoridades Policiais a Comunicações Criptografadas de Ponta a Ponta] [Nota: A Comissão Europeia emitiu posteriormente um esclarecimento ao MediaNama afirmando que *backdoors* não devem ser introduzidos e a encriptação não deve ser enfraquecida.]
Julho de 2020	Ministro indiano de tecnologia da informação, Ravi Shankar Prasad, na reunião de ministros da economia digital do G20	"É hora de reconhecer que as plataformas digitais em qualquer lugar do mundo devem ser responsivas e responsáveis em relação às preocupações soberanas dos países, incluindo defesa, privacidade e segurança dos cidadãos" Sonte: Comunicado de Imprensa do Ministério Indiano de Eletrônica e Tecnologia da Informação
4 Out de 2019	O Secretária do Interior do Reino Unido, Priti Patel, o Procurador-geral dos EUA Barr, osecretário de Segurança Interna (em exercício) McAleenan e o Ministro australiano de	Carta aberta com referência às propostas de "privacidade em primeiro lugar" do Facebook Solicitou que o Facebook não prossiga com seu plano de implementar encriptação ponta a ponta em seus serviços de mensagens para proteger usuários e crianças.

	Assuntos Internos Dutton - para Mark Zuckerberg	
Julho de 2019	Five Eyes	Reunião Conjunta da FCM e Quinteto de Procuradores-Gerais Declarou que “as empresas de tecnologia devem incluir mecanismos no design de seus produtos e serviços criptografados pelos quais os governos, agindo com autoridade legal apropriada, possam obter acesso aos dados em um formato legível e utilizável”.
Julho de 2017	G20	“Outro conjunto de problemas, relatou Merkel, são os serviços de mensagens. A declaração publicada parece clandestina, dizendo: 'Em linha com as expectativas de nossos povos, também incentivamos a colaboração com a indústria para fornecer acesso legal e não arbitrário às informações disponíveis onde o acesso é necessário para a proteção da segurança nacional contra ameaças terroristas.' é claro que o alvo é a encriptação. Eles têm que ser capazes de entender, onde houver suspeita razoável, o conteúdo da comunicação terrorista, explicou Merkel. ” Fonte: G20 Chega a Acordo Contra o Terrorismo, Parece Ter Como Alvo a Encriptação

DECLARAÇÕES DOMÉSTICAS

3 de dez. de 2020	Ministro de Assuntos Internos da Austrália, Peter Dutton	“A encriptação é boa nesse sentido onde nos protege dos criminosos, mas a encriptação é ruim quando protege os criminosos da polícia.” Fonte: Nova abordagem da AFP para expulsar pedófilos do “esgoto da internet”
Dez. de 2020	Comissária das Crianças para a Inglaterra, Anne Longfield	Relatório sobre como a encriptação de ponta a ponta ameaça a segurança das crianças online Recomenda quatro testes que as empresas de tecnologia devem cumprir antes de implementar a encriptação ponta a ponta.
Nov. de 2020	Agência Nacional do Crime, Reino Unido	Se o conteúdo do Facebook for criptografado de ponta a ponta, há um risco real de que a justiça não seja feita às vítimas de abuso infantil. Fonte: Os planos de encriptação do Facebook podem ajudar abusadores de crianças a escapar da justiça, alerta a NCAS

13 de nov de 2020	Ministros de Assuntos Internos da UE	Declaração conjunta da E.U. ministros de assuntos internos sobre os recentes ataques terroristas na Europa Argumentou que o acesso das autoridades competentes às informações digitais - sejam dados de tráfego ou, em alguns casos, dados de conteúdo - é “essencial para prevenir e eliminar ações terroristas”. Instou o Conselho a considerar a questão da encriptação de dados para garantir a coleta legal de provas, mantendo a confiabilidade da tecnologia criptografada. [Observação: Esta declaração não condena explicitamente ou procura enfraquecer a encriptação. Mas essa última pode ser uma consequência possível]
20 de out. de 2020	Secretário do Departamento de Assuntos Internos da Austrália, Mike Pezzullo	"Estamos particularmente preocupados com os planos do Facebook de usar a encriptação ponta a ponta de toda a sua plataforma para criar, de fato, a maior *dark web* do mundo." Fonte: Facebook Definido para criar 'A Maior Dark Web do Mundo' com Encriptação de Ponta a Ponta, Afirma o Ministro Australiano
23 de out. de 2020	Ministro do Interior da Austrália, Peter Dutton	Gigantes da mídia social, incluindo o Facebook, estão bloqueando as tentativas globais de aplicação da lei para combater a exploração sexual de crianças. Dutton disse que o Facebook, em particular, está tomando decisões deliberadas com encriptação de ponta a ponta para impedir o encaminhamento de questões que, de outra forma, em anos anteriores, teriam sido feitas às autoridades. Fonte: Facebook colocando crianças em risco: Dutton
3 de fev. de 2020	Índia	Relatório do Comitê Adhoc de Rajya Sabha para Estudar a Questão Alarmante da Pornografia nas Mídias Sociais e seus Efeitos sobre as Crianças e a Sociedade como um Todo Recomenda-se que a lei seja alterada para permitir a quebra da encriptação de ponta a ponta para rastrear distribuidores de Material de Abuso Sexual Infantil (CSAM).
3 de junho de 2020	Ex-procurador-geral dos EUA William P. Barr	Declaração do Procurador-geral William P. Barr sobre a introdução do Projeto de Lei de Acesso Legal no Senado Argumentou que a encriptação à prova de mandado permite que predadores de crianças, terroristas, traficantes de drogas e até mesmo hackers operem com impunidade.

Jan. de 2020	Ex-procurador-geral dos EUA William P. Barr	Sobre as lutas da aplicação da lei com a encriptação: “Não queremos entrar em um mundo onde temos que gastar meses e até anos exaustivos esforços quando vidas estão em equilíbrio... Devemos ser capazes de entrar assim que tivermos um mandado que estabeleça que a atividade criminosa provavelmente está em andamento Fonte: O Encryption Push de Barr está ocorrendo há décadas, mas Preocupam Alguns no FBI
Out. de 2019	Ministro indiano de Tecnologia da Informação, Ravi Shankar Prasad	A origem das mensagens no WhatsApp deve ser acessível. O direito à privacidade não é para quem faz mau uso das plataformas de comunicação. Fonte: Direito à privacidade, não para aqueles que abusam da plataforma da Internet: Ravi Shankar Prasad

b. Resumo de fatos de encriptação vs. mitos

Fato No. 1: A encriptação forte é essencial para a segurança da internet
Mito: Os *backdoors* para acesso direcionado ou excepcional por parte das autoridades não enfraquecem a segurança da Internet

- ➔ A encriptação é um processo matemático que não pode ser aplicado seletivamente. Qualquer demanda por um *backdoor* que só funcione para o governo está essencialmente em guerra com a matemática.

- ➔ Um *backdoor* para conteúdo criptografado é uma falha de segurança que torna todo o sistema e os dados subjacentes vulneráveis. Mesmo que seja criado apenas para acesso do governo, será inevitavelmente explorado por uma série de outros agentes mal-intencionados.

Fato No. 2: Dar acesso excepcional à aplicação da lei ameaça os direitos humanos e a democracia
Mito: Os *backdoors* de aplicação da lei não impactarão nossos direitos ou a democracia

- ➔ A encriptação é fundamental para a governança democrática e a proteção do direito à privacidade e à liberdade de expressão na era digital. O enfraquecimento da encriptação por meio de mecanismos de acesso excepcionais põe em risco esses direitos humanos básicos e a democracia como um todo.
- ➔ A encriptação é particularmente necessária para certos indivíduos e grupos, incluindo jornalistas, advogados, médicos e comunidades vulneráveis cujo trabalho e vida

dependem da disponibilidade de canais de comunicação livres da possibilidade de vigilância.

Fato No. 3: A encriptação forte fortalece a privacidade e a segurança

Mito: Para alcançar a segurança, devemos sacrificar a privacidade

- ➔ O enquadramento do debate sobre a política de encriptação como "privacidade versus segurança" é impreciso e tem como premissa um falso binário. Os dois são princípios que se reforçam mutuamente.
- ➔ Um enquadramento mais apropriado seria "segurança versus segurança", já que a encriptação não apenas protege a privacidade, mas também protege a segurança. Essa reformulação ajudaria a garantir que uma suposta política de "segurança" não se tornasse uma política de "insegurança", criando mais perigos do que visa prevenir.

Fato No. 4: A aplicação da lei entrou na era de ouro da vigilância - sem quebrar a encriptação

Mito: A aplicação da lei está enfrentando um problema de "escurecimento", o que torna necessário quebrar a encriptação

- ➔ A metáfora do "escurecimento" é imprecisa. Isso implica que as mudanças tecnológicas diminuíram as capacidades de vigilância, quando foram amplamente expandidas.
- ➔ Uma metáfora mais precisa é "uma era de ouro da vigilância", já que muito mais dados sobre indivíduos estão disponíveis hoje do que nunca, incluindo nossas informações de localização, informações sobre nossos contatos e muitos outros detalhes não registrados anteriormente que podem ser compilados para criar "dossiês digitais" que pintam um retrato íntimo de nosso cotidiano.

Fato No. 5: O enfraquecimento da encriptação não impedirá que criminosos e terroristas usem encriptação forte

Mito: O enfraquecimento da encriptação é uma medida eficaz para combater o terrorismo e a atividade criminosa

- ➔ O efeito do enfraquecimento da encriptação é que o público em geral é privado de uma plataforma onde os dados e os direitos fundamentais são protegidos. Os criminosos simplesmente mudarão para plataformas criptografadas disponíveis em jurisdições estrangeiras ou no mercado negro, ou podem até criar as suas próprias.
- ➔ O aumento das capacidades de vigilância frequentemente leva à vigilância invasiva sem provas suficientes de sua eficácia. Um estudo nos EUA sugere que a ligação entre o aumento das capacidades de vigilância e a prevenção do terrorismo é tênue. Independentemente da eficácia no combate ao terrorismo, não é necessário ou proporcional comprometer a privacidade e a segurança de todos os usuários de uma plataforma ou sistema na esperança de identificar a fração que se envolve em conduta criminosa.

Fato No. 6: A encriptação forte contribui para a segurança das crianças online

Mito: A encriptação torna a Internet insegura para crianças

- ➔ Como outros criminosos, os autores de crimes contra crianças recorrerão a plataformas criptografadas alternativas oferecidas em jurisdições estrangeiras ou criarão suas próprias plataformas para ocultar suas atividades. Isso significa que a atividade criminosa persistirá - ela simplesmente ficará fora do alcance da aplicação da lei, impedindo o acesso legal até mesmo a metadados que podem ser instrumentais nas investigações.
- ➔ As crianças precisam de plataformas criptografadas onde a identidade das pessoas com as quais estão interagindo possa ser autenticada e onde suas informações pessoais não corram o risco de serem expostas a terceiros. Com mais crianças online devido à pandemia global, os governos devem encorajar o uso de encriptação forte para manter as crianças seguras, e não introduzir deliberadamente vulnerabilidades de segurança na tecnologia que usam.

Fato No. 7: A obrigatoriedade de "rastreabilidade" colocará em risco a liberdade de expressão de privacidade

Mito: A rastreabilidade deve ser implementada para evitar a disseminação de desinformação

- ➔ A rastreabilidade coloca o anonimato e o direito à privacidade em risco e tem um efeito negativo sobre a liberdade de expressão. Portanto, é incompatível com os direitos humanos e a democracia.
- ➔ A rastreabilidade tem utilidade limitada na prática e não servirá como uma ferramenta eficaz para combater a desinformação.

Fato No. 8: A encriptação forte é crucial para a segurança cibernética e protege a segurança nacional

Mito: o acesso excepcional ao conteúdo criptografado é necessário para proteger a segurança nacional

- ➔ A encriptação forte é vital para uma infraestrutura de segurança cibernética resiliente que protege a segurança nacional. Enfraquecer a encriptação coloca em risco a segurança nacional.
- ➔ O aumento de incidentes de segurança cibernética e violações direcionadas é um argumento a favor, e não contra, a encriptação forte. Sem uma encriptação forte, veríamos mais acesso não autorizado e exposição de informações classificadas, um benefício para os criminosos cibernéticos ou adversários patrocinados pelo estado. Também veríamos ataques mais bem-sucedidos à infraestrutura essencial, como sistemas de saúde, eleições e transporte público, pois os sistemas criptografados ajudam a manter suas operações seguras.

Fato No. 9: A encriptação forte mantém a confiança no ecossistema digital e apoia o crescimento econômico

Mito: Enfraquecer deliberadamente a encriptação não terá efeito na economia

- ➔ A encriptação é a base da economia digital moderna, mantendo a confidencialidade dos dados dos clientes e a autenticidade das transações financeiras. A confiança em sistemas criptografados estimula o investimento, a inovação e o crescimento econômico.
- ➔ A encriptação também pode prevenir ou mitigar o impacto dos incidentes de segurança cibernética que, de outra forma, causariam mais danos e custariam mais dinheiro. Ela reduz o risco de violações de dados e controla os custos de tais violações, auxiliando os interesses comerciais e apoiando a economia como um todo.

Fato No. 10: Os órgãos de aplicação da lei e de inteligência não precisam quebrar a encriptação para investigar o crime

Mito: As autoridades não têm alternativa a não ser quebrar a encriptação

- ➔ Os órgãos de inteligência e de aplicação da lei já se beneficiam muito do grande aumento de dados disponíveis sobre indivíduos na era digital. Não há provas que mostrem que enfraquecer a encriptação é um meio necessário, proporcional ou eficaz de atingir os objetivos do governo em democracias modernas que respeitam os direitos.
- ➔ Na maioria dos casos, as autoridades ainda confiam principalmente em provas tradicionais, como testemunhas, informantes, provas físicas e registros comerciais de bancos e empresas de telefonia celular. Minar a encriptação e enfraquecer a segurança de todos na tentativa de obter todas as provas possíveis em casos específicos não se alinha aos direitos humanos e às liberdades e, na prática, nunca será um substituto para um bom trabalho investigativo.