CRIPTOGRAFIA EM JUÍZO:
CONSIDERAÇÕES SOBRE O JULGAMENTO DA ADI 5527 E DA ADPF 403 PELO STF

COORDENAÇÃO: RAQUEL SARAIVA LÍDER DE PROJETO: MARIANA CANTO

PESQUISADORES: LUANA BATISTA, PEDRO SILVA NETO, RHAIANA VALOIS, THOBIAS PRADO MOURA

AUTORIA: LUANA BATISTA, RAQUEL SARAIVA, RHAIANA VALOIS

REVISÃO: MARIANA CANTO

Instituto de Pesquisa em Direito & Tecnologia do Recife

Internet Society Capítulo Brasil

Como citar: BATISTA, Luana; SARAIVA, Raquel; VALOIS, Rhaiana. Criptografia em juízo: considerações sobre o julgamento da ADI 5527 e da ADPF 403 pelo STF. Recife: Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec, 2025. Disponível em <link>. Acesso em: [data por extenso].

O documento foi elaborado no âmbito do Projeto "Criptografia e Direitos Digitais no Brasil: Capacitação, Diálogo e Incidência Política", realizado em conjunto com a ISOC Brasil e financiado pela ISOC Foundation.

1. CONTEXTO DAS AÇÕES

A criptografia exerce um papel fundamental na defesa e no exercício de direitos fundamentais como a privacidade, a proteção de dados pessoais, a liberdade de expressão, o direito de associação e de reunião, entre outros, além de ser ferramenta chave na segurança de usuários e negócios online. Entretanto, várias são as tentativas, por parte das autoridades de segurança pública e defesa nacional em todo o mundo, de fragilizar a criptografia de plataformas e dispositivos em nome de uma suposta maior efetividade investigativa.

No Brasil, alguns casos sobre o tema tiveram maior destaque, chegando a provocar bloqueios de aplicativos de mensageria que resultaram em duas ações em trâmite no Supremo Tribunal Federal. Os bloqueios se deram entre os anos de 2015 e 2016 e tinham como fundamento a recusa, por parte da empresa controladora do aplicativo Whatsapp, de fornecimento de dados de usuários e consequente descumprimento de ordem judicial.

A primeira decisão[1], em 2015, que não veio a ser executada, foi emitida por um juiz da Central de Inquéritos de Teresina (Piauí), em investigação sobre abuso sexual infantil. Empresas provedoras de acesso à Internet, alvos da ordem de decisão do bloqueio, entretanto, entraram com mandados de segurança, que foram aceitos em segunda instância.

1 INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE; INTERNETLAB. Bloqueios.info, 2022. Disponível em: <https://bloqueios.info/pt/casos/exemplo-de-post-em-casos/>. Acesso em: 02 abr. 2025.

No mesmo ano[2], a 1ª Vara Criminal de São Bernardo do Campo, ordenou o bloqueio do aplicativo pelo descumprimento de ordem de interceptação telemática de mensagens de três investigados, o que foi cumprido pelas empresas provedoras de acesso à Internet. O WhatsApp, por sua vez, entrou com mandado de segurança alegando, entre outros argumentos, violação ao Marco Civil da Internet e ao Decreto nº 3.810/2001.

O terceiro bloqueio[3] contra o aplicativo de mensageria foi emitido por um juiz da Vara Criminal de Lagarto - SE, em maio de 2015. A ordem, solicitada pela Polícia Federal, deu-se em virtude da não realização de uma interceptação em tempo real no serviço de mensageria. Após um mandado de segurança da empresa, a ordem de bloqueio foi suspensa.

O último caso de bloqueio[4] do WhatsApp foi registrado em 2016. Também por descumprimento de entregas de dados criptografados, o serviço de mensageria foi bloqueado por ordem judicial 2ª Vara Criminal de Duque de Caxias (Rio de Janeiro). A medida, entretanto, foi suspensa pelo Ministro do Supremo Tribunal Federal, Ricardo Lewandowski.

Em consequência de tais decisões, duas ações foram protocoladas no STF. A ADPF 403, de relatoria do Ministro Edson Fachin e autoria do Partido Popular Socialista (PPS), argumenta que o bloqueio do Whatsapp viola o preceito fundamental da liberdade de comunicação, previsto no art. 5°, IX, da Constituição Federal e pede que seja declarada a existência da referida violação, com a finalidade de não mais ser possível o bloqueio do aplicativo por qualquer decisão judicial.

A segunda ação, a ADI 5527, de relatoria da Ministra Rosa Weber, agora aposentada, tem como autor o então Partido da República, agora Partido Liberal, que, entre os pedidos, inclui a declaração de inconstitucionalidade do artigo 12, III e IV, do Marco Civil da Internet, bem como a interpretação conforme a Constituição do art. 10, § 2° da mesma lei, além do pedido subsidiário de adoção da técnica de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, de forma a afastar a sua aplicação aos aplicativos de troca de mensagens virtual; ou, por último, que se dê interpretação conforme a tais dispositivos, condicionando-se, em consequência, a aplicação das sanções de suspensão temporária e de proibição do exercício das atividades somente após as sanções previstas no art. 12, I e II, mostrarem-se frustradas.

O julgamento de ambas as ações foi iniciado em maio de 2020 com a leitura dos votos dos relatores. Após os pronunciamentos, o Ministro Alexandre de Moraes solicitou vistas dos processos, o que interrompeu a sessão. Agora, as ações voltam à pauta de julgamento num contexto bem diferente, permeado por discussões sobre regulação e atribuição de responsabilidades mais robustas às plataformas digitais.

2 INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE; INTERNETLAB. Bloqueios.info, 2022. Disponível em: <https://bloqueios.info/pt/casos/bloqueio-por-descumprimento-de-ordem-judicial-de-entrega-de-dados/>. Acesso em 02 abr. 2025.

3 INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE; INTERNETLAB. Bloqueios.info, 2022. Disponível em: <https://bloqueios.info/pt/casos/bloqueio-por-descumprimento-de-ordem-judicial-de-entrega-de-dados-whatsappiii/>. Acesso em 02 de abril de 2025.

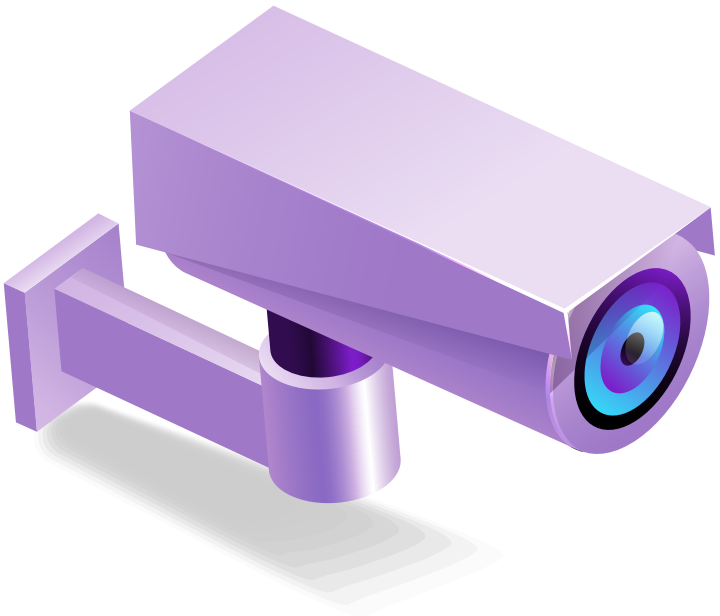
4 INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE; INTERNETLAB. Bloqueios.info, 2022. Disponível em: <https://bloqueios.info/pt/casos/bloqueio-por-descumprimento-de-ordem-judicial-de-entrega-de-dados-2/>. Acesso em 02 abr. 2025.

2. ANÁLISE DOS VOTOS DOS RELATORES

2.1 - ADI 5527 (Rosa Weber)

Conforme exposto, a ADI 5527 parte do entendimento de que o art. 10, §2º, da Lei nº 12.965/2014 (Marco Civil da Internet) dá respaldo legal às ordens judiciais de disponibilização do conteúdo das comunicações por provedores de Internet, estabelecendo no art. 12 as penalidades possíveis, entre as quais se incluem a suspensão temporária e proibição das atividades, em caso de descumprimento da determinação.

Em termos gerais, questiona a constitucionalidade dessas penalidades, argumentando que as ordens de bloqueio do WhatsApp, com base nesses dispositivos, comprometeram, de forma desproporcional e arbitrária, o direito à livre comunicação de milhões de cidadãos, além de violarem os princípios constitucionais da livre iniciativa, da livre concorrência e da proporcionalidade. Dessa forma, argumentou por uma interpretação conforme a Constituição para que a quebra de sigilo nesses casos seja autorizada exclusivamente para fins de persecução penal.



Ao analisar a questão, a relatora do caso, a Ministra Rosa Weber, reconheceu em seu voto a importância do Marco Civil da Internet por colocar o país em uma posição de vanguarda na defesa dos direitos dos usuários da rede, além dos subsídios trazidos pela audiência pública realizada em conjunto com a ADPF 403[5]. Seu posicionamento se alinha ao de especialistas em segurança digital, ao destacar que a criptografia desempenha papel central não apenas na proteção da privacidade e da liberdade de expressão, mas também na garantia da segurança da informação e do sigilo das comunicações. Conforme enfatiza em seu voto, a tecnologia cria condições materiais para o exercício desses direitos nos dias atuais, de modo que o Estado não deve retroceder na defesa das garantias e liberdades individuais no ambiente virtual[6].

Nesse contexto, a Ministra sustenta que medidas como os bloqueios já ocorridos colocam o Brasil em uma posição semelhante à de Estados autoritários, alheios às tradições e valores que sustentam um verdadeiro Estado Democrático de Direito[7]. Além disso, ressalta a importância da criptografia para a defesa dos direitos humanos, como um importante mecanismo para garantir a segurança e a proteção de ativistas, acadêmicos, artistas e opositores em regimes autoritários ao redor do mundo[8].

Na análise do mérito, a Ministra, mesmo reconhecendo, nos termos do art. 5º, XII, da

5 BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 5.527/DF. Relator: Rosa Weber. Brasília, DF. Diário da Justiça Eletrônico, Brasília, DF, 27 mai. 2020. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf. Acesso em: 16 abr. 2025.

6 Ibidem.

7 Ibidem.

8 Ibidem.

Constituição Federal, que o art. 10, § 2º, do MCI autoriza a determinação de ordens judiciais para disponibilização de conteúdos em comunicações privadas nas hipóteses de investigação ou instrução processual penal, afirma que a previsão não torna, por si só, ilegal o uso da criptografia por aplicativos de mensageria[9]. **Pelo contrário, trata-se de uma tecnologia legítima, utilizada para assegurar maior privacidade e segurança nas comunicações**.

Assim, **o Estado não pode exigir que empresas ofertem serviços intencionalmente menos seguros ou vulneráveis** sob o argumento de que, em circunstâncias futuras, seria necessário explorar tais vulnerabilidades para viabilizar o cumprimento de ordens judiciais. Além disso, como muito bem expõe no seu voto, a implementação de vulnerabilidades, também chamados de backdoors, não expõe apenas os supostos alvos da persecução criminal, mas sim todos que utilizam o serviço em sua grande maioria para finalidades legítimas[10]. Além disso, a proibição do uso da tecnologia não impede que criminosos migrem para camadas mais profundas e restritas da Internet, dificultando ainda mais eventuais investigações.

Dessa forma, ressalta que, uma vez criada a vulnerabilidade no sistema para viabilizar acesso das autoridades ao conteúdo das comunicações de eventuais investigados, abre-se também uma porta para que criminosos e outros agentes maliciosos explorem essas brechas implementadas, comprometendo, assim, a segurança de todos os usuários[11]. Isso é particularmente perigoso para a segurança dos serviços utilizados, porque pode resultar em um aumento significativo nos riscos de ciberataques, roubo de identidade, fraudes, extorsões, chantagem, vazamento de informações confidenciais, entre outros crimes.

9 Ibidem.

10 Ibidem.

11 Ibidem.

No que diz respeito às penalidades previstas no art. 12, III e IV, da Lei, os quais, respectivamente, permitem a suspensão temporária e a proibição do exercício das atividades dos provedores, a Ministra sustenta que as referidas sanções servem para proteger os direitos dos usuários em caso da violação da privacidade e do sigilo das comunicações e não, como entendeu o juiz autor das ordens de bloqueio, para amparar casos de descumprimento de ordens judiciais[12].

Isso porque as penalidades em questão fazem referência expressa aos atos previstos no art. 11 da Lei. Dessa forma, a partir da interpretação conjunta com esse dispositivo, conclui-se que a aplicação das penalidades será possível apenas quando houver violação à legislação brasileira no que tange aos direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros. Essa condição se aplica às operações que envolvam a coleta, o armazenamento, a guarda e o tratamento de registros, dados pessoais ou comunicações por provedores de conexão e de aplicações de internet, desde que ao menos um desses atos ocorra em território nacional.

12 Ibidem.

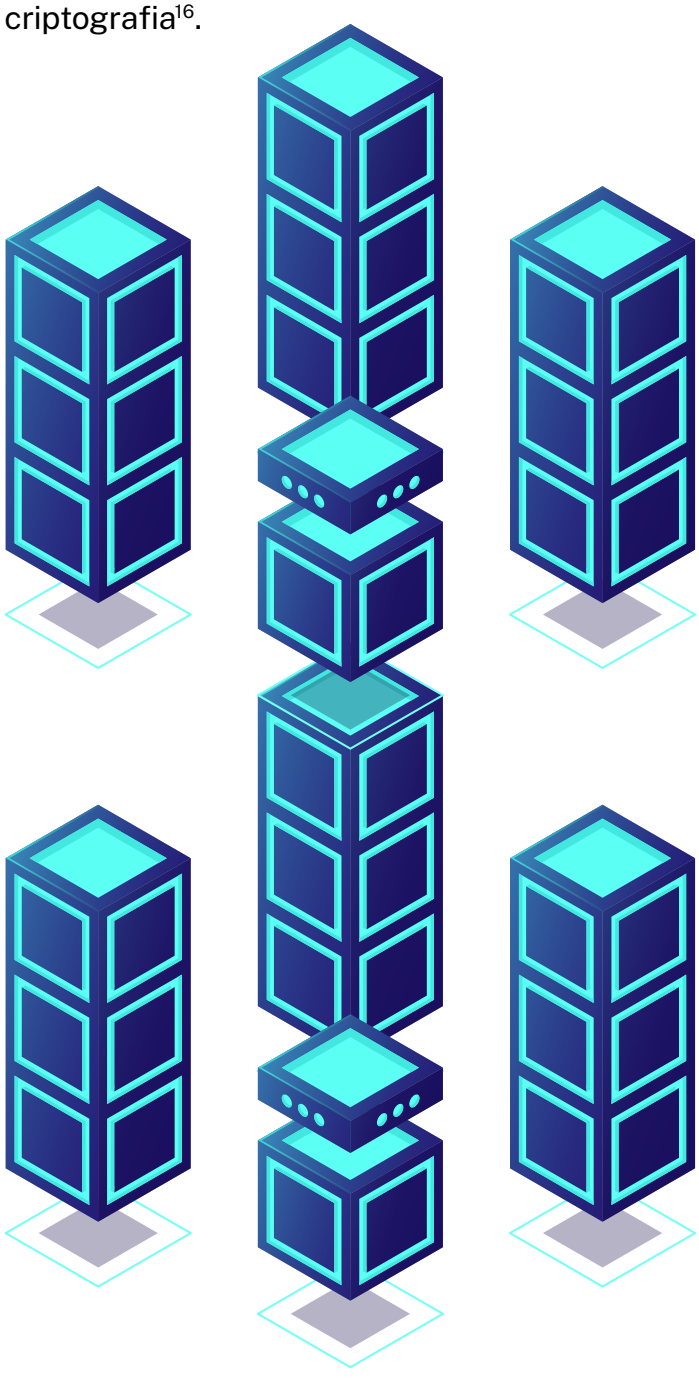
Dessa forma, argumenta que não há suporte jurídico que autorize a suspensão temporária e a proibição do exercício das atividades em caso de descumprimento de ordem judicial de disponibilização do conteúdo de comunicações privadas. As sanções previstas, na verdade, servem para garantir a proteção da privacidade e dos dados do usuário, de modo que usá-las como forma de compelir os particulares a enfraquecer a criptografia vai completamente de encontro à finalidade da lei e, em particular, do dispositivo em questão.

As ordens de bloqueio, concluiu a Ministra, resultaram de uma interpretação equivocada da lei, sem a devida consideração quanto à possibilidade concreta de cumprimento da determinação, além de desconsiderarem a importância da criptografia para a garantia de outros direitos fundamentais[13]. Tratam-se, portanto, de medidas desproporcionais, que acabaram por afetar a vida de inúmeras pessoas usuárias dos serviços da empresa, gerando um verdadeiro caos nas relações pessoais, profissionais e comerciais mediadas pelo provedor.

Por essas razões, a Ministra votou pela improcedência do pedido de declaração de inconstitucionalidade, adotando uma interpretação conforme a Constituição quanto ao art. 10, § 2º para estabelecer que o conteúdo das comunicações privadas apenas poderá ser disponibilizado mediante ordem judicial na forma que a lei estabelecer e para fins de investigação ou instrução processual penal[14].

Ademais, julgando parcialmente procedente o pedido de interpretação conforme do art. 12, III e IV, da Lei, firmou o entendimento de que as penalidades em questão somente podem ser impostas aos provedores nos casos de violação da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros[15].

Portanto, de forma acertada, afastou qualquer interpretação que amplie a hipótese de incidência dos dispositivos em comento para abarcar o sancionamento por descumprimento de ordem judicial de disponibilização de conteúdo de comunicações, cuja obtenção só seja possível a partir da quebra ou vulnerabilização de mecanismos de proteção como a criptografia[16].



13 Ibidem.

14 Ibidem.

15 Ibidem.

16 Ibidem.

2.2 - ADPF 403 (Edson Fachin)

A Arguição de Descumprimento de Preceito Fundamental nº 403, por sua vez, foi proposta, em caráter incidental, sob o argumento de que a decisão judicial de suspensão do WhatsApp violaria o preceito fundamental da liberdade de comunicação, previsto no art. 5º, inciso IX, da Constituição Federal, afetando de maneira desproporcional a vida de milhares de pessoas que utilizam o serviço.

De maneira semelhante à Ministra Rosa Weber, o relator do caso, Ministro Edson Fachin, ao proferir seu voto, defendeu a importância da criptografia para o exercício dos direitos à privacidade, à liberdade de comunicação, de opinião e de expressão, especialmente diante das possibilidade de violação decorrente da capacidade de vigilância, que pode ser realizada através da Internet[17].

Ademais, destacou a necessidade de garantia do anonimato no ambiente digital, não como uma forma de se eximir pessoas e entidades de eventual responsabilização, mas como uma dimensão essencial do direito à privacidade, relacionada à possibilidade de não ter todos os aspectos da vida pessoal monitorados e analisados[18]. Dessa forma, ressaltou que tanto a criptografia quanto o anonimato são mecanismos fundamentais para a promoção de direitos fundamentais, especialmente em contextos autoritários e censores. Além disso, são essenciais para garantir uma Internet mais segura, reconhecendo este também como direito de todos[19].

17 BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental 403/SE. Relator: Edson Fachin. Brasília, DF. Diário da Justiça Eletrônico, Brasília, DF, 28 mai. 2020. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf . Acesso em: 16 abr. 2025.

18 Ibidem.

19 Ibidem.

Apesar disso, o Ministro admite que a criptografia pode dificultar o trabalho de investigação das autoridades, mas contrapõe a este argumento o fato de que até agora nenhum governo foi capaz de demonstrar que isso não pode ser realizado de outras formas[20]. Além disso, defendeu que permitir o acesso a mensagens criptografadas aos agentes públicos, por meio da implementação de vulnerabilidades no sistema ou até mesmo pela proibição do uso da tecnologia, comprometeria a segurança de todos[21]. Fachin chega até supor a possibilidade de permitir a criptografia apenas para autoridades públicas, mas conclui que essa hipótese não se sustenta tendo em vista que a tecnologia não protege apenas direitos constitucionalmente garantidos, mas também permite o acesso de pessoas em situação de vulnerabilidade[22].

Outro ponto importante que merece destaque no voto em questão é que, conforme observado pelo Ministro, o uso da criptografia forte não implica qualquer isenção de responsabilização das empresas, as quais devem observar a legislação brasileira e cumprir ordens judiciais relativas à entrega de dados, desde que tal cumprimento não comprometa a segurança de seus sistemas[23]. Ademais, o uso da criptografia não exime as empresas da responsabilidade compartilhada na construção de uma sociedade mais justa. Nesse sentido, devem atuar de forma proativa para impedir que seus serviços sejam utilizados para a disseminação de discurso de ódio, a realização de ataques ao sistema democrático e a veiculação de conteúdos ilegais[24].

Em suma, o Ministro entendeu que, mesmo diante da alegada ameaça representada pelo uso da criptografia, não é possível autorizar o acesso excepcional ou a implementação de vulnerabilidades nos sistemas que a utilizam, nem mesmo a sua proibição[25]. Autorizar tais medidas seria um verdadeiro contrassenso frente à busca por uma Internet mais segura, pois comprometeria um dos principais mecanismos de proteção de direitos fundamentais no ambiente digital.

Assim, com o objetivo de afastar qualquer interpretação que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagens criptografada, julgou procedente a Arguição de Descumprimento de Preceito Fundamental para declarar a inconstitucionalidade parcial, sem redução de texto, dos dispositivos previstos no art. 7º, II, e no art. 12, III, do MCI[26].

Para Fachin, o inciso II do art. 7º inclusive representa "a ponte que atualiza e adapta o alcance do direito à privacidade ao mundo digital", refletindo diretrizes tanto nacionais quanto internacionais sobre a importância de garantir a privacidade no fluxo de informações[27]. Quanto ao art. 12, III, da lei afirma, de maneira similar a Ministra Rosa Weber, que a sanção de suspensão das atividades somente pode ser aplicada nos casos em que houver violação ao direito à privacidade[28]. Além disso, sustentou, com base na Lei Geral de Proteção de Dados (LGPD), que caberia à Autoridade Nacional de Proteção de Dados, e não ao Poder Judiciário, a imposição dessa penalidade[29].

20 Ibidem.
21 Ibidem.
22 Ibidem.
23 Ibidem.
24 Ibidem.
25 Ibidem.
26 Ibidem.
27 Ibidem.
28 Ibidem.
29 Ibidem.

Dessa forma, concluiu que não é possível obrigar os provedores de aplicação a quebrar a criptografia, uma vez que enfraquecê-la implica, necessariamente, tornar a Internet um lugar menos seguro.

3. OS RISCOS DA REVERSÃO DOS VOTOS JÁ PROFERIDOS

Como exposto nos votos dos Ministros, a criptografia constitui um mecanismo essencial para a segurança das pessoas nos dias atuais, assegurando as condições necessárias ao exercício de direitos fundamentais. Em ambos os casos, ficou evidente a importância das contribuições técnicas e especializadas apresentadas durante a audiência pública, que desempenharam papel fundamental na elucidação de questões complexas e na fundamentação das decisões.

Em contextos autoritários e ditatoriais, o direito à privacidade, à liberdade de comunicação, de expressão e de opinião tornam-se particularmente fragilizados, colocando em risco indivíduos em situação de maior exposição, como jornalistas, ativistas, artistas e acadêmicos que se opõem a tais regimes e atuam pela defesa dos direitos humanos.

Esse cenário se agrava face à intensificação da coleta de dados pessoais, impulsionada pela plataformização da Internet e pela ascensão de um novo modelo de negócio baseado no perfilamento dos indivíduos e de análises preditivas. Nosso comportamento online atualmente é constantemente monitorado, analisado e precificado, fenômeno este que Shoshana Zuboff (2021) denomina de "Capitalismo de Vigilância"[30].

Nessa fase do capitalismo global, em que a extração massiva de dados se torna regra, o anonimato, como destaca o Ministro Fachin, constitui uma aspecto essencial do direito à privacidade. O direito de não ser visto é o que tem permitido o exercício pleno e sem constrangimentos de liberdades constitucionalmente garantidas, indispensáveis à vida democrática, especialmente em contextos opressores.

Diante dessa nova conjuntura, não cabe ao Estado retroceder na proteção desses direitos, sobretudo quando novos mecanismos, como a criptografia, surgem justamente para garanti-los. **Permitir exceções à criptografia para fins de investigação, como demonstrado, compromete a segurança não apenas de indivíduos sob suspeita, mas de toda a cole-**

30 ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021.

tividade. Como exposto nos votos, os ônus em fragilizar ou até mesmo proibir o uso da criptografia superam os seus possíveis benefícios.

É preciso que se reconheça que a maioria das pessoas utiliza serviços criptografados por razões legítimas. A quebra do sigilo das comunicações, assim como dos registros telegráficos, deve ser, portanto, medida excepcional, justificada por indícios concretos e dentro dos limites constitucionais. Enfraquecer a criptografia de ponta-a-ponta para apurar eventuais ilícitos expõe, entretanto, indiscriminadamente toda a base de usuários. Nesse contexto, não é demais reforçar que uma Internet segura, conforme salienta o Ministro Fachin, não é apenas um direito apenas das autoridades e agentes públicos, mas sim de todas as pessoas.

Criar brechas deliberadas em sistemas criptográficos significa comprometer a segurança geral e, em outras palavras, inverter a lógica da proteção constitucional e trocar a exceção pela regra. Em nome da tentativa de se alcançar potenciais criminosos, colocaria-se todas essas pessoas em risco, sendo a quebra da criptografia muito mais prejudicial ao interesse público do que a busca por outras alternativas que viabilizem a solução de eventuais crimes na Internet.

Além dessas ameaças, é importante destacar os potenciais impactos comerciais e econômicos decorrentes da quebra da criptografia[31]. A confiança na integridade e na segurança das comunicações é um dos pilares fundamentais do ambiente de negócios contemporâneo. Setores como o de sistemas bancários, comércios eletrônicos e os serviços financeiros digitais dependem diretamente de mecanismos criptográficos robustos para garantir a proteção das transações, dados sensíveis e informações sigilosas de clientes. A introdução de brechas intencionais em tais sistemas colocaria em risco a segurança de operações financeiras, expondo consumidores a fraudes, extorsões e perdas, além de comprometer a estabilidade do setor como um todo.

Do mesmo modo, infraestruturas críticas — como redes elétricas, sistemas de telecomunicações e serviços de abastecimento de água — utilizam criptografia para assegurar a sua operação contínua e resistente a intervenções externas. Fragilizar essas proteções aumentaria os riscos de sabotagem, ataques e falhas sistêmicas, com consequências graves para a segurança pública. Em última instância, a erosão da confiança digital poderia gerar retração de investimentos, fuga de empresas de tecnologia e impactos diretos sobre a competitividade do país no cenário internacional.

Ademais representaria um retrocesso na proteção dos instrumentos que hoje garantem a efetivação de direitos individuais, especialmente para os grupos que mais necessitam de proteção, e ampliaria os riscos de ataques, fraudes e outros crimes que poderiam ser prevenidos com o uso adequado da tecnologia. Nesse cenário, os usuários se tornariam ainda mais vulneráveis à vigilância estatal intrusiva, à exploração comercial de seus dados por empresas privadas e à ação de agentes maliciosos.

É importante destacar, ainda, que enfraquecer a criptografia não solucionará problemas complexos como a desinformação, a disseminação de discursos de ódio, os ataques à democracia ou o fortalecimento de câmaras de eco. Nem, como exposto por Fachin, exime as empresas de trabalharem de forma que seus serviços não sejam desvirtuados para finalidades escusas ou ilícitas.

31 COALIZÃO DIREITOS NA REDE. A importância social e econômica da criptografia. Disponível em: <https://cartilhacriptografia.direitosnarede.org.br/cartilhacriptografia.pdf>. Acesso em: 17 abr. 2025.

Esses desafios, por outro lado, exigem uma regulação robusta, com obrigações claras para as plataformas, especialmente no que diz respeito à transparência sobre algoritmos e parâmetros utilizados, sobre à publicidade veiculada em seus serviços e o impulsionamento de conteúdo realizado, além do estabelecimento de mecanismos de prestação de contas e auditoria para empresas.

Em todos os casos, é preciso considerar as diferentes funções intermediárias dos serviços regulados. Além disso, é fundamental proteger os direitos dos usuários, com o estabelecimento de garantias, como a do devido processo e do contraditório na moderação de conteúdo, como também levar em conta iniciativas estruturadas de educação midiática e letramento digital.

Reverter, portanto, o entendimento firmado nos votos significaria ignorar as contribuições técnicas e jurídicas oferecidas por especialistas e entidades, não apenas durante a audiência pública realizada no contexto das ações[32] [33] [34] [35], como citadas nos respectivos votos, mas também nas discussões contemporâneas sobre o tema, em claro prejuízo da sociedade como um todo.

32 BRASIL. SUPREMO TRIBUNAL FEDERAL. Audiência Pública do Supremo Tribunal Federal - Bloqueio Judicial do Whatsapp e Marco Cívil da Internet (MCI) - Parte 1. TV Justiça. 02 jun. 2017. Disponível em: https://youtu.be/3TNsQCNIOO0?si=Mw8JFTtER_bRrWmQ. Acesso em 17 abr. 2025.

33 BRASIL. SUPREMO TRIBUNAL FEDERAL. Audiência Pública do Supremo Tribunal Federal - Bloqueio Judicial do Whatsapp e Marco Cívil da Internet (MCI) - Parte 2. TV Justiça.02 jun. 2017. Disponível em: https://youtu.be/qN9w_BuKfCA?si=Ku2jmG4H8zxvPV7r. Acesso em 17 abr. 2025.

34 BRASIL. SUPREMO TRIBUNAL FEDERAL. Audiência Pública do Supremo Tribunal Federal - Bloqueio Judicial do Whatsapp e Marco Cívil da Internet (MCI) - Parte 3. TV Justiça. 05 jun. 2017. Disponível em: https://youtu.be/Bvq4JSr6uCo?si=40U_6Zh9RsNS417n. Acesso em 17 abr. 2025.

35 BRASIL. SUPREMO TRIBUNAL FEDERAL. Audiência Pública do Supremo Tribunal Federal - Bloqueio Judicial do Whatsapp e Marco Cívil da Internet (MCI) - Parte 4. TV Justiça. 02 jun. 2017. Disponível em: https://youtu.be/t1WJLIa5nV8?si=PlIbiXNIwxzu87of. Acesso em 17 abr. 2025.

4. A INEFICÁCIA DA QUEBRA DA CRIPTOGRAFIA DE PONTA A PONTA: FUNDAMENTOS TÉCNICOS E JURÍDICOS

A proposição de obrigar plataformas digitais a implementar mecanismos que fragilizem, contornem ou viabilizem a quebra de seus sistemas de criptografia de ponta a ponta parte da premissa de que o acesso excepcional ao conteúdo de comunicações de determinados usuários permitiria às autoridades competentes elucidar ilícitos penais com maior celeridade e eficácia. No entanto, tal premissa ignora, por um lado, os limites técnicos e a complexidade operacional das investigações digitais no cenário contemporâneo, e, por outro, os graves riscos sistêmicos que decorrem da imposição de tais obrigações às empresas provedoras de serviços digitais.

A criptografia de ponta a ponta é um mecanismo de proteção da confidencialidade das comunicações digitais que garante que apenas os dispositivos das partes diretamente envolvidas na troca de mensagens detenham as chaves criptográficas necessárias para codificar e decodificar o conteúdo transmitido. Essas chaves são geradas e armazenadas localmente nos dispositivos dos usuários, sem qualquer tipo de acesso, mesmo técnico, por parte dos provedores do serviço de comunicação — como é o caso das plataformas de mensageria. Como consequência, **nem mesmo os próprios provedores possuem acesso ao teor das comunicações**, pois não detêm as chaves criptográficas necessárias à sua decodificação.

Essa arquitetura técnica impede que tais empresas forneçam o conteúdo das mensagens, mesmo quando compelidas por ordem judicial. Não se trata, pois, de resistência injustificada à atuação estatal, mas de uma impossibilidade material: o conteúdo solicitado simplesmente não se encontra sob a guarda ou domínio do provedor.

Qualquer tentativa de obrigar tais empresas a alterar a arquitetura do sistema, a fim de permitir o acesso por terceiros a conteúdos criptografados — como as autoridades estatais —, exigiria a criação de uma espécie de "chave mestra" ou mecanismo oculto de acesso (comumente denominado backdoor), capaz de romper a proteção criptográfica e revelar os dados protegidos.

Entretanto, o argumento segundo o qual seria possível implementar mecanismos que permitissem o acesso seletivo e controlado às comunicações, restrito a ordens judiciais, esbarra em um consenso técnico consolidado no campo da segurança da informação: **a criação de qualquer mecanismo de acesso excepcional necessariamente compromete a integridade de todo o sistema criptográfico**. Isso porque, a partir do momento que tal mecanismo é criado, ainda que sob o fundamento de uso controlado, o sistema deixa de oferecer garantias de inviolabilidade. O simples fato de haver um ponto de acesso vulnerável — mesmo que tecnicamente protegido — transforma o sistema em um vetor de ataque que pode ser acessível não apenas ao poder público, mas também a agentes maliciosos, como cibercriminosos, governos estrangeiros, organizações de espionagem ou mesmo atores internos com acesso privilegiado.

A criação de uma vulnerabilidade intencional — ainda que sob supervisão estatal — enseja riscos permanentes e imprevisíveis, pois tal brecha pode ser descoberta, explorada ou vazada, como já demonstrado em diversos casos de ferramentas estatais que foram utilizadas para fins ilícitos. Em suma, **não existem *backdoors* seguros ou restritos**.

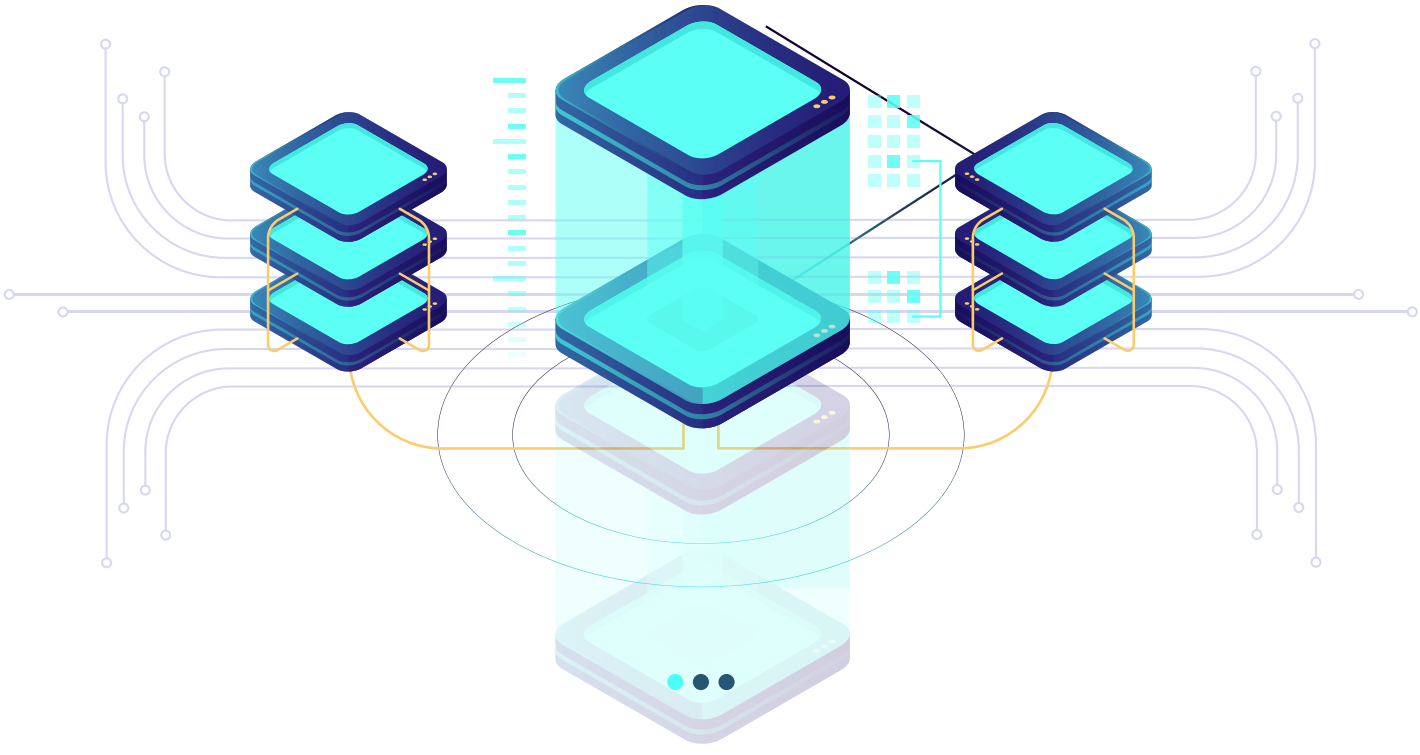
Assim, essa medida comprometeria de forma massiva e indiscriminada não apenas alvos legítimos de investigação, mas toda a base de usuários do sistema, abrangendo a segurança de jornalistas, advogados, ativistas, médicos, parlamentares, empresários e cidadãos em geral que dependem da confidencialidade das comunicações digitais para o exercício de suas funções e da vida privada.

Além disso, ainda que fosse possível, do ponto de vista técnico, a criação de mecanismos de acesso à criptografia, e que tais mecanismos fossem exigidos de empresas estabelecidas sob a jurisdição brasileira, a medida não alcançaria os fins pretendidos, pois a tecnologia da criptografia está amplamente disseminada e disponível em softwares de código aberto, redes descentralizadas e aplicativos alternativos que operam fora do alcance regulatório nacional, esvaziando a eficácia operacional da ação.

A imposição de restrições a determinados sistemas e serviços, portanto, apenas desloca a prática ilícita, sem resolvê-la. Cria-se, assim, uma falsa sensação de controle, ao mesmo tempo em que expõe a população geral a riscos significativos, sem gerar efetividade investigativa relevante.

Do ponto de vista jurídico, **a adoção de medidas que impliquem no enfraquecimento estrutural da criptografia ofende diretamente o princípio da proporcionalidade, pois os impactos dessa medida extrapolam o âmbito da persecução penal e incidem de forma desproporcional sobre o exercício de direitos fundamentais**. No caso do Whatsapp, a supressão de garantias criptográficas afeta indiscriminadamente milhões de usuários legítimos, impactando o exercício de atividades econômicas, profissionais e pessoais que dependem da integridade das comunicações digitais, ao passo que os supostos ganhos investigativos são marginais e de eficácia efêmera, considerando as múltiplas vias alternativas de comunicação segura disponíveis.

Desse modo, a tentativa de impor sanções a empresas que se recusem a violar seus sistemas de proteção revela incompreensão quanto à limitação técnica envolvida e inverte os princípios da segurança digital. Compelir



um provedor a comprometer sua arquitetura de proteção, a fim de satisfazer determinação judicial, significa exigir que atue contra os próprios deveres legais de proteção à privacidade e à integridade das comunicações, como os estabelecidos na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Tal medida afronta não apenas o ordenamento jurídico nacional, mas posiciona o país em contrariedade aos parâmetros normativos internacionais no campo dos direitos humanos e da governança da Internet.

Conforme bem assinalado nos votos dos Ministros Rosa Weber e Edson Fachin, não se pode, sob qualquer fundamento, transformar a segurança de toda a coletividade em risco colateral. **A fragilização deliberada da criptografia de ponta a ponta representa, simultaneamente, uma resposta ineficaz ao crime, uma medida desproporcional em relação aos direitos em jogo e uma ameaça à segurança digital de toda a sociedade**.

5. RECOMENDAÇÕES

À luz das considerações técnicas e jurídicas expostas ao longo deste documento, conclui-se que a criptografia de ponta a ponta desempenha papel central na garantia da segurança digital e da proteção de direitos fundamentais no ambiente digital. Tal mecanismo, ao assegurar que apenas as partes envolvidas na comunicação tenham acesso ao seu conteúdo, representa não apenas uma medida técnica de proteção de dados, mas um desdobramento direto das garantias constitucionais da inviolabilidade das comunicações (art. 5º, XII, da Constituição Federal) e da proteção à intimidade e à vida privada (art. 5º, X).

Considerando a complexidade da matéria, é de rigor o reconhecimento, como já delineado em parte nos votos proferidos, das seguintes conclusões e recomendações:

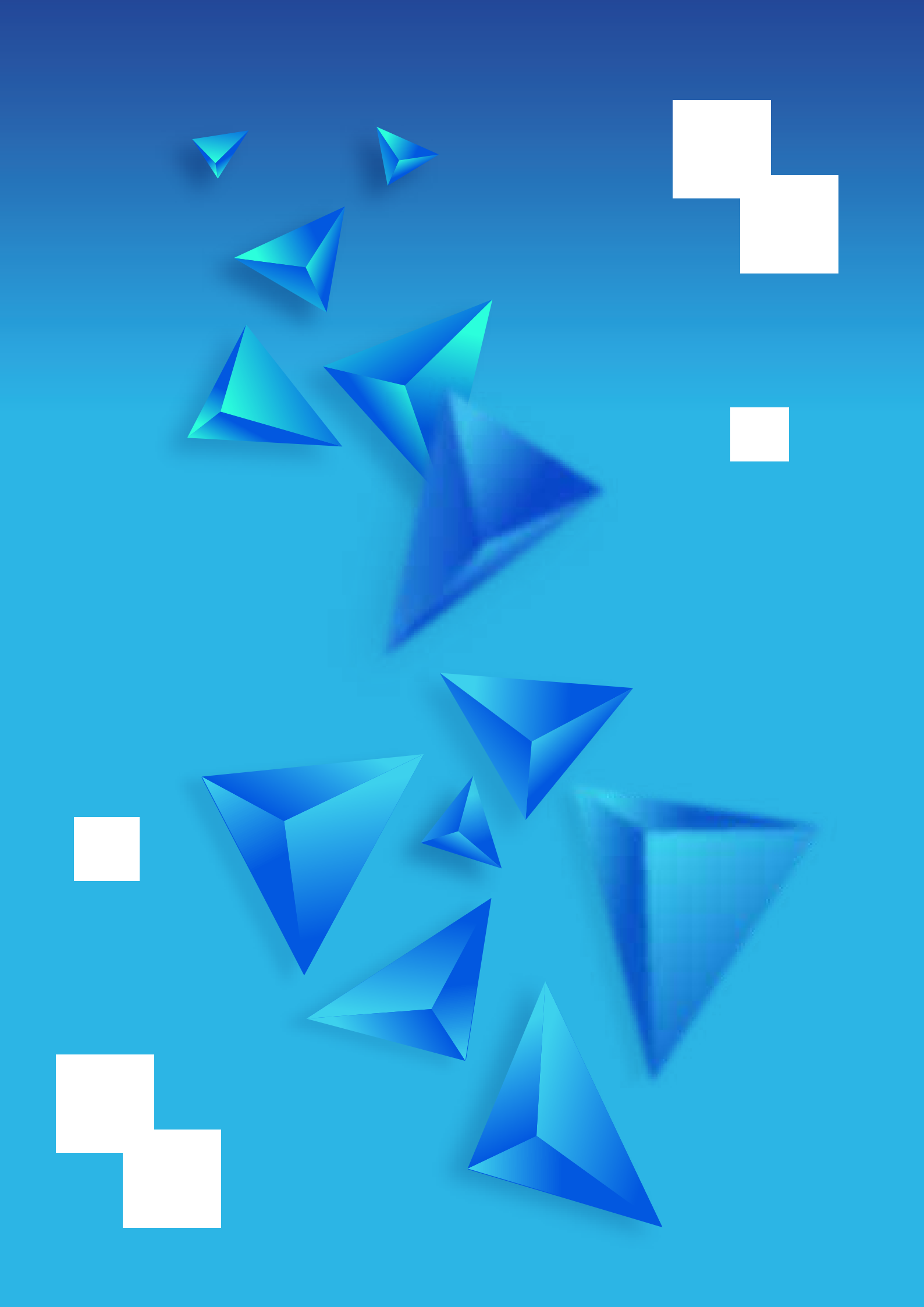
- **Reconhecimento da inviabilidade técnica da quebra seletiva da criptografia ponta a ponta:** Não há, sob a arquitetura atual adotada por diversas plataformas, possibilidade técnica de acesso ao conteúdo das comunicações criptografadas por parte das próprias empresas responsáveis pelos aplicativos. Isso decorre do fato de que as chaves criptográficas são geradas e armazenadas exclusivamente nos dispositivos dos usuários finais, não sendo acessíveis sequer pelas plataformas. Assim, ordens judiciais que demandem tal acesso, ainda que legítimas em sua intenção, esbarram em uma limitação técnica objetiva e incontornável.

- **Rejeição da imposição de mecanismos de acesso excepcional (backdoors):** Qualquer exigência que implique a criação de vulnerabilidades deliberadas nos sistemas de criptografia — como a implementação de backdoors — é desproporcional, inconstitucional e contrária ao interesse público. A introdução de tais mecanismos comprometeria a segurança de todos os usuários, expondo comunicações privadas a agentes mal-intencionados, e colocaria em risco a integridade de dados sensíveis de milhões de pessoas, incluindo cidadãos, empresas e órgãos públicos.

- **Reconhecimento da ineficácia prática da quebra isolada da criptografia como instrumento de persecução penal:** Ainda que fosse tecnicamente possível a obtenção de conteúdos criptografados de um serviço específico, a medida seria, em regra, inócua no médio e longo prazos. Isso porque usuários envolvidos em atividades ilícitas tendem a migrar rapidamente para outras plataformas igualmente protegidas, muitas delas sediadas fora da jurisdição nacional. Assim, a quebra da criptografia em um serviço isolado não resolveria o problema de fundo, ao passo que imporia custos sociais e institucionais elevados.

- **Compromisso com a proteção de direitos fundamentais no ambiente digital:** As decisões judiciais e interpretações normativas sobre o tema devem sempre considerar a centralidade da criptografia como salvaguarda de direitos fundamentais. Esta proteção se estende a múltiplos aspectos da vida digital dos cidadãos, abrangendo não apenas a liberdade de expressão e o sigilo profissional, mas também a proteção contra vigilância indevida, a preservação da privacidade das comunicações pessoais, a garantia da confidencialidade de dados sensíveis, e o estabelecimento de salvaguardas robustas contra potenciais abusos por parte de agentes estatais ou privados.

- **Reconhecimento de que o art. 12, III e IV, do Marco Civil da Internet não autoriza bloqueio de aplicações por descumprimento de ordem judicial,** mas tão somente aplica sanções quando da infração a direitos de privacidade, proteção de dados pessoais e sigilo das comunicações, já que sua interpretação deve ser feita em conjunto com o art. 11, ao qual faz referência explícita.



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife

@I.P.REC

I.P.REC.BR

Internet Society
Capítulo Brasil

@ISOCBRASIL

ISOC.ORG.BR

APOIO: Internet Society Foundation