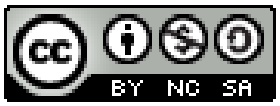
O MOSAICO LEGISLATIVO DA CRIPTOGRAFIA NO BRASIL: UMA ANÁLISE DE PROJETOS DE LEI

Equipe de pesquisa:
André Ramiro (coord.)
Mariana Canto
Paula Côrte Real
José Paulo Lima
Thaís Aguiar

IP.rec
INSTITUTO DE PESQUISA EM DIREITO & TECNOLOGIA DO RECIFE

O presente estudo foi realizado pelo **Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec**, centro independente de pesquisa e atuação política focado nos impactos sociais, éticos e jurídicos relativos ao desenvolvimento tecnológico.

O trabalho do Instituto teve início em 2017 e, desde então, sua equipe atua na elaboração de estudos científicos, análises de caso, campanhas, eventos e ações que contribuam para a construção de conhecimento e de senso crítico sobre o funcionamento das redes digitais.



**PROJETO GRÁFICO,
CAPA E DIAGRAMAÇÃO**
Jeporu - web criativa

Os autores agradecem as revisões e valiosas contribuições de Marina Pita (Intervozes), Sérgio Amadeu (UFABC), Gustavo Rodrigues (Instituto de Referência em Internet e Sociedade), Verónica Arroyo (Access Now) e Pedro Luiz Barreto (C.E.S.A.R).

https://ip.rec.br

@ip.rec @institutoiprec

ÍNDICE

1 _ Apresentação

As disputas que permeiam a garantia do sigilo e as políticas de vigilância sobre as comunicações simbolizam boa parte da história em torno dos direitos digitais. Programas de monitoramento da sociedade cada vez mais amplos são revelados e as justificativas para sua existência são renovadas a cada novo fato político que possa ser traduzido em "ameaça à segurança pública". Com esse avanço, técnicas, políticas, estudos, campanhas e outras reações se apresentam, procurando oferecer maior autonomia tecnológica e privacidade aos usuários da Internet. A criptografia assume papel central nessas disputas.

O projeto "Encriptação: liberdade e tensões no Brasil" - do qual este estudo faz parte - procurou catalisar os aspectos históricos, políticos, tecnológicos e legais que giram em torno da criptografia, na tentativa de fornecer subsídios à formulação de políticas públicas e, de alguma maneira, problematizar possíveis restrições à criptografia no país. O que se passa no cenário brasileiro é resultado e, ao mesmo tempo, motor de transformações em políticas tecnológicas em outras regiões. Com isso, pretendemos contribuir com informações e análises que sejam aproveitadas em favor de uma governança global da Internet - e, por que não, da própria criptografia.

O debate em torno da criptografia no plano nacional ganhou destaque nos últimos anos devido à sucessão de bloqueios de aplicativos de trocas de mensagem[1]. O grau de sigilo oferecido pela criptografia gerou reações das agências de investigação, que alegam ver suas operações prejudicadas por não possuírem mais as capacidades de interceptação e acesso às comunicações. Além disso, os desafios processuais relativos à requisição, por parte das autoridades de investigação, de conteúdos de comunicações aos provedores de aplicação sediados no exterior também deram novos contornos jurisdicionais aos embates no cenário brasileiro.

De toda forma, as características desses conflitos encontram semelhanças onde são postos. Nos Estados Unidos, onde as disputas sobre a criptografia já alcançam maiores contornos, são presenciadas sucessivas investidas em favor do acesso "excepcional" ao conteúdo encriptado de mensagens e de aparelhos celular. Esse movimento também abriu espaço para a criação de novas narrativas como forma de reenquadrar o significado da própria criptografia. Para as autoridades de investigação norte-americanas, por exemplo, a criptografia que preveja brecha que permita explorar o conteúdo encriptado passa a se chamar "encriptação responsável" (responsible encryption, no original),

1 Uma linha do tempo pode ser encontrada em https://bloqueios.info/

criando uma falsa lógica segundo a qual a criptografia verdadeiramente forte e segura seria irresponsável.[2] A partir dos seus contextos políticos específicos, países acolhem essas narrativas a sua maneira, inaugurando seus próprios conflitos em torno da criptografia e suas próprias formas de tentar enfraquecê-la.

Consequentemente, o cenário brasileiro também apresenta suas formas de traduzir tais tensões através das retóricas e atuações de órgãos de investigação e aplicação da lei, surtindo efeito no plano judicial e legislativo. Decisões são proferidas sem considerações ou ponderações suficientes sobre aspectos técnicos e legais específicos à Internet, inaugurando precedentes problemáticos ao ecossistema tecnológico[3]. Da mesma forma, projetos de leis são propostos em reação a fatos políticos sensíveis, para, por exemplo, criar prevenções contra a ocorrência de atentados, combater organizações terroristas, reprimir o tráfico de drogas ou redes de pedofilia, para citar alguns. Algumas dessas propostas legislativas serão objeto deste estudo.

Devido ao caráter transfronteiriço da Internet, é difícil pensar em uma interferência sobre determinado serviço tecnológico ou recurso de segurança que não resvale em outras características da rede de forma não prevista, indesejada ou até mesmo que afete outros territórios. Isso quer dizer que políticas que atinjam determinada plataforma em um dado país possivelmente encontrarão efeitos em outras localidades onde a tecnologia em questão também está presente. Essas decisões impactariam políticas privadas das empresas que operam a tecnologia e isso, por sua vez, surtiria efeito sobre como o poder público de outras localidades a regulam[4] - e assim por diante. Logo, estamos diante de uma ecologia ou de um ecossistema tecnológico: se há interferência em um de seus elementos, toda sua estrutura é abalada, inclusive avançando sobre fronteiras nacionais e impactando outras jurisdições.

Além disso, ao passo que mais e mais aspectos do cotidiano migram para o ecossistema online, mais dependemos da segurança dessas redes[5]. Dados bancários, operações econômicas, serviços essenciais, comunicações profissionais e pessoais, informações sensíveis sobre gestão governamental, sobre articulações de organizações da

2 PFEFFERKORN, Riana. **The risks of "Responsible Encryption".** Stanford's CIS - Center for Internet and Society, fevereiro de 2018. Disponível em https://cyberlaw.stanford.edu/files/publication/files/2018-02-05%20Technical%20Response%20to%20Rosenstein-Wray%20FINAL.pdf. Acesso em 30 de abril de 2020.

3 KARUNI, Simone. **Bloqueio do WhatsApp deixa rastro de prejuízo pelo país.** Correio Braziliense, maio de 2016. Disponível em https://www.correiobraziliense.com.br/app/noticia/economia/2016/05/04/internas_economia,530305/bloqueio-do-whatsapp-deixa-rastro-de-prejuizos-pelo-pais.shtml. Acesso em 30 de abril de 2020.

4 BUDISH, Ryan; BURKERT, Herbert; GASSER, Urs. **Encryption Policy and Its International Impacts: a Framework for Understanding Extraterritorial Ripple Effects.** Hoover Institution, artigo n. 1804, 2018. Disponível em: https://www.hoover.org/research/encryption-policy-and-itsinternational-impacts. Acesso em 30 de abril de 2020.

5 POLK, Ryan. **Your Day with Encryption**. Internet Society. Outubro, 2019 https://www.internetsociety.org/blog/2019/10/your-day-with-encryption/ Acesso em 30 de abril de 2020.

sociedade civil e outra variedade de camadas da vida em sociedade trafegam em sistemas digitais e são, consequentemente, visadas por agentes maliciosos. Como na realidade offline, estes estão sempre perseguindo formas de explorar vulnerabilidades dos usuários e de infraestruturas críticas.

A segurança da informação, portanto, procura sempre estar à frente dessas ameaças e se encarrega de renovar os melhores recursos que assegurem a confidencialidade, a integridade e a disponibilidade das informações. A criptografia, um dos alicerces da segurança da informação, assume uma função chave na implementação e efetivação de técnicas que busquem garantir a confiabilidade sobre a rede. Portanto, tentativas de relativizar as potencialidades oferecidas pela criptografia afetaria, de forma colateral, a estabilidade e resiliência da Internet, comprometendo a confiança e a segurança de seus usuários. Faria sentido enfraquecer justamente a segurança "em nome da segurança"?

Os casos a serem discutidos servem de pano de fundo para o aprofundamento de questões críticas ao uso livre da criptografia e para a reflexão sobre os impactos de propostas legislativas que procuram alterá-la através de mecanismos processuais e tecnológicos. Algumas dessas iniciativas resgatam ideias conhecidas de interceptação e "custódia de chaves" de decriptação. Outras lidam com propostas, digamos, alternativas de acesso ao conteúdo das comunicações. No entanto, a meta se mantém a mesma: suspender o sigilo do fluxo das comunicações privadas e do armazenamento de dados para proveito de agências de investigação. Os riscos, igualmente, se mantém os mesmos: o crescimento do número de ataques e exploração de vulnerabilidades por terceiros não autorizados, aumentando exponencialmente as possibilidades de comprometimento da rede; maior complexidade para os sistemas de segurança; e maiores chances de abusos por parte de setores governamentais, o que possibilitaria acesso direto e arbitrário às comunicações, afastando ainda mais a fronteira das garantias aos direitos fundamentais.

Este trabalho, por fim, busca contribuir para o entendimento sobre a importância técnica, política e legal da criptografia. Busca, igualmente, resgatar seu histórico recente no Brasil e, assim, contextualizar com desafios encontrados tanto a nível legislativo e judicial, bem como com as disputas narrativas típicas desse debate. As análises, enfim, levam em consideração articulações geopolíticas importantes para se compreender as propostas legislativas a nível nacional e como se localiza a defesa das liberdades e dos direitos digitais no campo da criptografia.

Boa leitura!

2 _ Metodologia

Por meio de um breve panorama introdutório sobre o contexto sócio-político que envolve as políticas em questão, o estudo se propôs a fazer um resgate histórico da evolução técnica da criptografia e das narrativas que se entrelaçam para desenhar o atual contexto brasileiro e mundial sobre o tema. O foco principal do estudo, em seguida, concentra-se no cenário brasileiro composto por quatro Projetos de Lei (PLs) na Câmara dos Deputados.

Considerando a proposta de aprofundamento na compreensão do problema investigado, optou-se pelo tipo de pesquisa qualitativa. As fontes primárias utilizadas foram Projetos de Lei que têm relação direta com liberdades e tensões do uso da criptografia no Brasil. Os critérios utilizados para o apanhado dos PLs foram: a) a atualidade, no que concerne aos projetos que se baseiam em fatos políticos mais recentes com roupagens atuais em suas justificativas; e a relevância, no que diz respeito aos projetos mais antigos, porém de extrema importância para melhor compreender o cenário político-normativo em que a discussão se insere e sugerir interpretações para eventuais propostas da mesma natureza.

Através de um mapeamento de propostas legislativas, foi elaborada uma tabela com referências básicas para o estudo, entre elas: a) o número do Projeto de Lei; b) o principal tema abordado no Projeto de Lei; c) a ementa, com breve resumo da proposta de alteração e/ou criação de normas; d) a justificativa e argumentos utilizados para fundamentá-lo; e) e os dispositivos legais, com destaques da redação de cada proposta legislativa.

Uma vez mapeadas, avançando para a análise dos PLs, o estudo foi estruturado e agrupado em seis diferentes eixos a fim de obter uma análise mais coerente e melhor estruturada. A escolha de cada eixo de análise deu-se devido a recorrência dos temas em diversos PLs, o que justificou o agrupamento em contextos e temas específicos, relacionando diretamente algumas das propostas em um só tópico, por exemplo. Além disso, muitos PLs envolvem mais de um tema, mostrando além de correlações entre eles, grandes interseções entre mais de um eixo de análise proposto.

Os eixos foram escolhidos de acordo com contexto, a profundidade oferecida, suas relações com a geopolítica sobre criptografia e os desdobramentos de possíveis cenários de risco para a garantia de direitos no país. Os eixos se referem a: 1. Antigas narrativas, novas roupagens; 2. Backdoors e restrições à liberdade criptográfica; 3. A subver-

são do devido processo legal contra a criptografia; 4. Monitoramento ativo e riscos ao regime de responsabilidade civil; 5. De volta à imputabilidade da rede; e 6. "Alternativas" ao backdoor e as suas problemáticas.

Como forma de complementar o panorama brasileiro de discussões em políticas de criptografia, também foram objeto de análise duas ações no âmbito do judiciário, atualmente em trâmite no Supremo Tribunal Federal. A Ação de Declaração de Inconstitucionalidade (ADI) nº 5527 e a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403. As ações são relevantes ao estudo uma vez que podem estabelecer precedentes judiciais importantes e discutem especificamente os desdobramentos dos casos de bloqueios de aplicativos ocorridos em território brasileiro, além de instrumentalizarem interpretações da legislação aqui explorada e repercutirem diretamente em consequências para o uso da criptografia no país.

3 _ Criptografia e Sociedade <

_ As dimensões histórica e técnica

A comunicação através de códigos, cifras e a busca pelo sigilo sempre esteve presente, de maior ou menor forma, no desenvolvimento da sociedade moderna. As dimensões da privacidade são cada vez mais aplicáveis à troca de informações e a expansão da Internet tornou isso ainda mais notável. Portanto, técnicas que procuram conferir maior segurança às comunicações, como a criptografia, assumem um papel cada vez mais basilar nas dinâmicas e fluxos de dados na rede.

O estado da arte na criptografia, atualmente, é resultado de séculos de desenvolvimento de códigos e tecnologias que buscam meios de transmitir uma mensagem com a menor possibilidade de interceptação possível. Da Roma Antiga, passando pela Idade Média e pela Guerra Fria[6], até os dias de hoje, sempre houve, com maior ou menor frequência, estudos e aplicações de códigos e técnicas que buscavam afastar o acesso ou compreensão de informações por pessoas não autorizadas. São as origens do aprimoramento da segurança da informação, o que tornou mais efetivo o controle sobre a emissão e recepção de dados e mensagens por meio de computadores[7].

6 KHAN, David. **The Codebreakers: the comprehensive history of secret communications from Ancient Times to the Internet.** Scribner Book Company, 1996; KATZ, Johathan; LINDEL, Yhueda. **Introduction to Modern Cryptography.** CRC Press, 2017. Disponível em https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/Introduction%20to%20Modern%20Cryptography.pdf. Acesso em 30 de abril de 2020.

7 GENCOGLU, Muharrem. **Importance of Cryptography in Information Society.** IOSR Journal of Computer

Durante boa parte do século 20, o uso da criptografia era, na ampla maioria dos casos, conferido a setores estatais. A Segunda Guerra Mundial reforçou a conotação restrita das técnicas de cifragem de comunicações e a Guerra Fria, devido à disputa informacional e tecnológica, levou adiante seu caráter de instrumento militar, o que fez repercutir em limitações à exportação de técnicas de criptografia[8]. Nos Estados Unidos, era listada como munição e o International Traffic in Arms Regulations (ITAR) regulava, entre outros coisas, os produtos que forneciam técnicas de encriptação. Além de sua restrição para exportação internacional, também se buscava a limitação do uso indiscriminado da criptografia mesmo em comunicação entre civis em âmbito doméstico.[9]

Até meados da década de 70, o uso da criptografia era custoso, pois envolvia um sistema de distribuição de chaves privadas, o que dificultava seu uso pelo cidadão comum. Com a criação da criptografia assimétrica, que utiliza um par de chaves (uma pública e outra privada), entre outros fatores, foi facilitada a troca das chaves de forma segura entre duas partes. Atualmente, a criptografia de chave pública está por trás da segurança de grande parte das transações e comunicações realizadas pela Internet.

O jogo de encriptação/decriptação das informações, portanto, carrega o potencial de rearranjar o poder na medida em que possibilita maiores capacidades de decisão sobre quem pode e quem não pode ter acesso a determinado conteúdo. Isso quer dizer que a criptografia sempre foi acompanhada de uma dimensão política, para além de um quebra-cabeça lógico ou matemático[10]. Assim, a partir do momento em que as forças tradicionais que detêm o poder passam a ver desafiado o monopólio sobre a confidencialidade das informações, estruturas sociais e políticas são movidas[11]. Setores antes fragilizados, que não tinham acesso a tecnologias de segurança da informação, agora se veem com acesso facilitado e com mais autonomia e controle sobre sua privacidade e liberdade de expressão. Do outro lado da moeda, o Estado, tradicionalmente observador de comunicações e comportamentos da sociedade, vê restringida sua capacidade histórica e cultural de vigilância sobre os indivíduos.

Engineering, Vol 21. janeiro de 2019, pág 65.

8 DIFFIE, Whitfield; LANDAU, Susan. **The export of cryptography in the 20th century and the 21st.** Handbook of of History of Information Security. Elsevier, 2009. Pág 4. Disponível em https://privacyink.org/pdf/export_control.pdf. Acesso em 28 de abril de 2020.

9 KHEL, Danielle; WILSON, Andi; BANKSTON, Kevin. **Doomed to Repeat History? Lessons from the Crypto Wars of the 1990.** Open Technology Institute. New America, 2015.

10 RANGER, Steve. **Encryption: in the between maths and politics there is only one winner.** ZDnet, julho de 2017. Disponível em https://zdnet.com/article/encryption-in-the-battle-between-maths-and-politics-there-is-only-one-winner/. Acesso em 30 de abril de 2020

11 ROGAWAY, Philip. **The Moral Character of Cryptographic Work**. University of California, 2015. Disponível em: http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf. Acesso em 19 de fevereiro de 2019.

_ As dimensões políticas

Nos últimos anos, a necessidade de avançar com sistemas de segurança da informação e confiabilidade nas aplicações tecnológicas se somou às sucessivas revelações de abusos de poder do Estado, notadamente por amplos programas de vigilância em massa. Essa união deságua, entre outras coisas, na renovação da importância das técnicas criptográficas[12] e em seu crescimento exponencial[13]. A uma só vez, isso significa o desenvolvimento natural das formas de tornar as comunicações mais resistentes a interferências e uma reação aos abusos do Estado.

Para as forças policiais, as empresas cada vez mais adotam arquiteturas de informação que inibem a capacidade do governo obter acesso a comunicações mesmo em situações que se adequem ao devido processo legal. A criptografia seria, supostamente, a marca dessas arquiteturas. Alegam que a defesa da privacidade foi "longe demais" na medida em que a criptografia afastaria a possibilidade de acesso a informações por essas mesmas agências[14]. Essas tensões simbolizam os conflitos em torno da criptografia dos últimos quase trinta anos. Uma diversidade de discursos públicos e testemunhos ao longo dos últimos anos construíram uma marcante defesa do relaxamento da criptografia, sobretudo aquela proveniente das autoridades policiais estadunidenses como o Department of Justice (DOJ) e o Federal Bureau of Investigation (FBI).[15]

Da parte das empresas de tecnologia, o emprego de criptografia ponta a ponta em populares plataformas de mensageria, assim como de criptografia por padrão em discos rígidos de aparelhos celular, significa um aceno, em primeiro plano, ao comprometimento com a segurança dos usuários. Por outro lado, a reputação dos provedores de aplicação vem seguidamente sendo testada em razão das revelações sobre rotinas de colaboração com agências de investigação, fornecendo acesso direto a seus servidores e dados[16]. Logo, em um segundo plano, a ativação de ferramentas de encriptação

12 SNOWDEN, Edward. **Without encryption, we will lose all privacy. This is our new battleground.** The Guardian, outubro de 2019. Disponível em https://www.theguardian.com/commentisfree/2019/oct/15/encryption-lose-privacy-us-uk-australia-facebook. Acesso em 30 de abril de 2020.

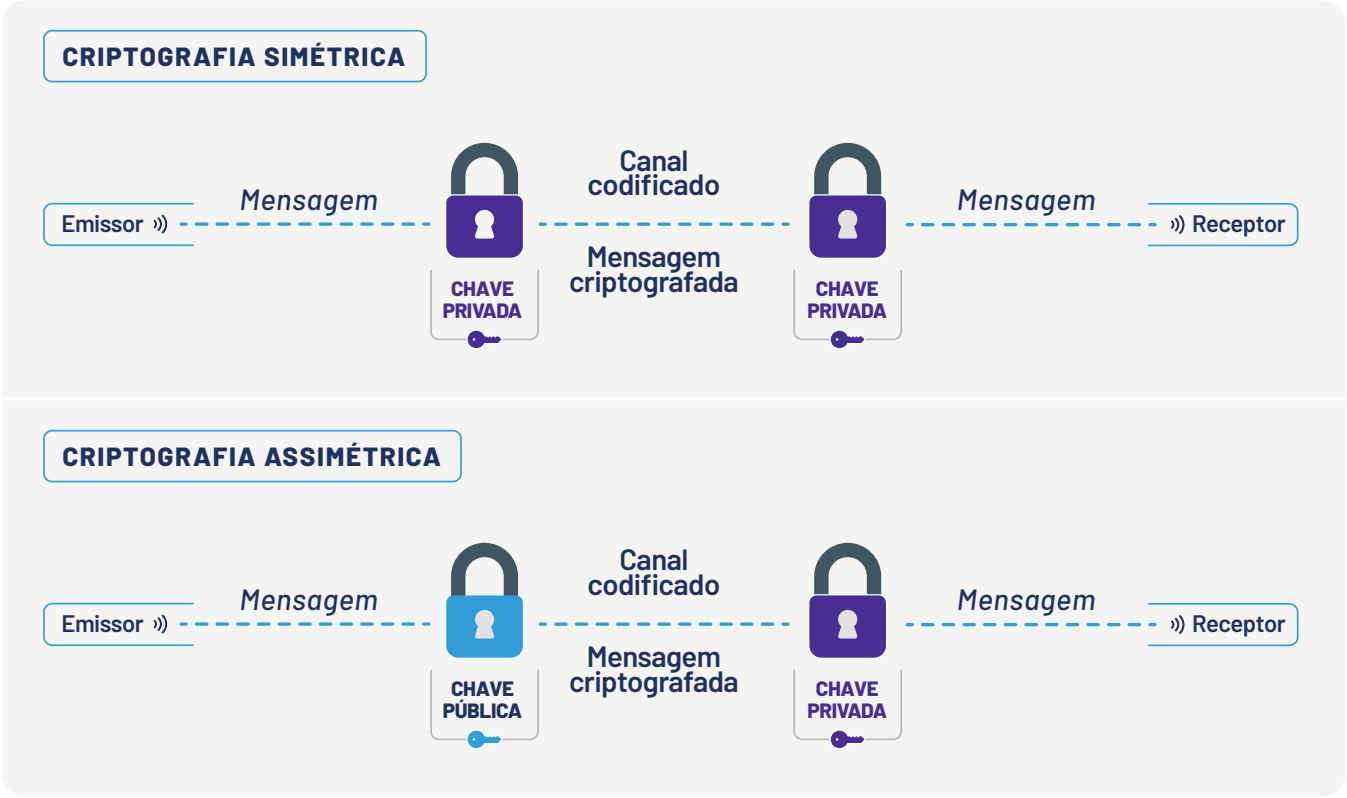
13 LEWIS, James; ZHENG, Denise; CARTER, William. **The Effect of Encryption on Lawful Access to Communications and Data.** CSIS Technology Policy Program. Fevereiro, 2017. Disponível em https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf. Acesso em 27 de abril de 2020.

14 COMEY, James. **Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?** Federal Bureau of Investigation. Brookings Institution, 2014. Disponível em https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acesso em27 de abril de 2020

15 Ver, por exemplo, os discursos e testemunhos das referidas agências em https://search.justice.gov/search?affiliate=justice-ag&query=encryption e https://www.fbi.gov/news/testimony. Acesso em 10 de junho de 2020.

16 FORENSTEIN, Gregory. **Report: NSA collects data direct from servers of Google, Apple, Microsoft, Facebook and more.** Techcrunch, junho de 2013. Disponível em https://techcrunch.com/2013/06/06/report-nsa-collects-

por padrão em seus serviços, afastando possibilidades de acesso e interceptação por meios tradicionais, também acena para uma tentativa de renovação da confiança com seu mercado de usuários[17]. Seria possível assumir, ainda, que uma brecha no sistema de segurança, para fins de "acesso excepcional", levaria a maiores encargos operacionais e grandes prejuízos econômicos decorrentes de eventuais vazamento de dados[18].



CRIPTO-GRAFIA

Conjunto de procedimentos técnicos que protegem o sigilo, a autenticidade e a integridade dos dados e comunicações. Para isso codifica - ou cifra - as informações, dando acesso apenas às pessoas autorizadas.

O mosaico de posicionamentos vai além de um conflito mercadológico e processual-criminal e põe em perspectiva a fundamental representação da comunidade científica de especialistas em técnicas de criptografia. Estudos basilares para as disputas em

-data-directly-from-servers-of-google-apple-microsoft-facebook-and-more/. Acesso em 30 de abril de 2020; SHULZE, Elizabeth. **US, UK sign agreement to access data from tech companies like Facebook.** CNBC, outubro de 2019. Disponível em https://www.cnbc.com/2019/10/04/us-uk-sign-agreement-to-access-data-from-tech-companies-like-facebook.html. Acesso em 30 de abril de 2020.

17 KENT, Gail. **Hard Quetions: Why does Facebook enable end-to-end encryption?** Facebook, maio de 2018. Disponível em https://about.fb.com/news/2018/05/end-to-end-encryption/. Acesso em 30 de abril de 2020;

18 COHNEY, Shaanan. **The costs of corroding cryptography.** Wharton University of Pennsylvania - Public Policy Initiative - Student Blog, julho de 2018. Disponível em https://publicpolicy.wharton.upenn.edu/live/news/2564-the-cost-of-corroding-cryptography. Acesso em 30 de abril de 2020.

torno da criptografia nos últimos anos apontam[19], com algum nível de consenso[20], para uma série de riscos estruturais e em escala caso um cenário de "acesso excepcional" fosse alcançado. Entre alguns dos alertas mais críticos, assume-se que a criação de vulnerabilidades em sistemas de criptografia carregaria maiores chances de vazamentos, facilitando que dados caiam nas mãos de terceiros não autorizados, agentes maliciosos que poriam em risco a segurança dos milhões de usuários (como, historicamente, já acontece[21]). Além disso, a implementação de recursos de acesso excepcional geraria maior complexidade a um sistema, acarretando em maiores possibilidades de falhas: "a complexidade é inimiga da segurança", concordam especialistas[22].

Além disso, em direção oposta aos argumentos originados nos setores das forças policiais, a sociedade civil chama atenção para outra realidade. Ao passo que mais níveis da vida em sociedade avançam em direção aos meios digitais, mais dados do que nunca estão sendo coletados por agências de inteligência e investigação. Em resposta, programas e serviços que objetivam facilitar a autonomia pessoal para criptografar foram precisamente construídos, entre outros finalidades, para afastar a vigilância governamental abusiva[23]; movimentos sociais já foram mobilizados tendo por princípio a defesa da liberdade de encriptar dados e comunicações[24]; e eventos distribuídos mundialmente são construídos colaborativamente com a intenção de democratizar técnicas de criptografia[25]. As expressões sociais são diversas.

Em sentido contrário às narrativas dos poderes de investigação, é possível afirmar que os meios de acesso a informações para fins de persecução criminal nunca fo-

19 ABELSON et al. **Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications**. Cambridge, 2015. Disponível em https://dspace.mit.edu/handle/1721.1/97690. Acesso em 19 de fevereiro de 2019.

20 RUIZ, David. **There is no middle ground on encryption.** Electronic Frontier Foundation, maio de 2018. Disponível em https://www.eff.org/pt-br/deeplinks/2018/05/there-no-middle-ground-encryption. Acesso em 30 de abril de 2020.

21 ALTIERES, Rohr. **Ataque que afetou 74 países usa brecha vazada pelo governo dos EUA.** G1, maio de 2017. Disponível em http://g1.globo.com/tecnologia/blog/seguranca-digital/post/ataque-que-afetou-74-paises-usa-brecha-vazada-do-governo-dos-eua.html. Acesso em 30 de abril de 2020; BIDDLE, Sam. **Leaked NSA malware is helping hijack computers around the world.** The Intercept, maio de 2017. Disponível em https://theintercept.com/2017/05/12/the-nsas-lost-digital-weapon-is-helping-hijack-computers-around-the-world/. Acesso em 30 de abril de 2020;

22 DONEDA. Danilo. **A regulação da criptografia e o bloqueio do WhatsApp.** ConJur, maio de 2017. Disponível em https://www.conjur.com.br/2017-mai-30/danilo-doneda-regulacao-criptografia-bloqueio-whatsapp. Acesso em 30 de abril de 2020.

23 LUMB, David J.. **The Story of Signal.** Increment, outubro de 2018. Disponível em https://increment.com/security/story-of-signal/. Acesso em 08 de maio de 2020; ZIMMERMAN, Phil. **Why I wrote PGP.** PGP User's Guide, 1991. Disponível em https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html. Acesso em 30 de abril de 2020.

24 HUGHES, Eric. **A Cypherpunk's Manifesto.** 1993. Disponível em **https://www.activism.net/cypherpunk/manifesto.html**. Acesso em 30 de abril de 2020.

25 Mais em https://www.cryptoparty.in/.

ram tão facilitados. Metadados[26] não encriptados são fornecidos rotineiramente para autoridades e constroem amplos perfis comportamentais sobre cidadãos; a expansão de dispositivos conectados - ou da Internet das Coisas - confere novos potenciais de captação de informações através de uma ampla variedade de sensores; tecnologias de vigilância e técnicas de hacking governamental já fazem parte das rotinas de investigação e inauguram novos níveis de acesso a dados e comunicações - muitas vezes sem autorização judicial.

As problemáticas aqui expostas, portanto, são transversais à situação da criptografia no cenário brasileiro. Algumas propostas legislativas se apresentam enquanto sintomas dessas tensões e desafiam construções legais pré-existentes, pondo em risco a conjuntura protetiva de direitos fundamentais consagrada pela Constituição e por tratados internacionais como o Pacto de São José da Costa Rica. Propostas de backdoors, responsabilização civil e criminal de provedores, hacking, entres outras, são apresentadas na esteira de formulação de políticas problemáticas e merecem atenção e análise.

Esse estudo pretende, por fim, pôr em perspectiva as relações entre criptografia, sua importância para a sociedade e as iniciativas que carregam o potencial de afetar a cultura tecnológica comprometida com a garantia de direitos. Assim, espera-se poder contribuir para o amadurecimento das políticas sobre tecnologia e ressaltar a importância da criptografia para o Brasil.

26 Para uma explicação mais detalhada, ver ELECTRONIC FRONTIER FOUNDATION. **Why metadata matters.** Agosto de 2015. Disponível em https://ssd.eff.org/pt-br/module/por-que-meta-dados-s%C3%A3o-importantes. Acesso em 10 de junho de 2020.

4 _ Quadro da análise legislativa

Norma	Ementa	Justificativa	Dispositivos legais
PL nº **5.285/2009**[27]	Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal.	Considera a necessidade de maior rigor e controle para regulações sobre o uso de ferramentas de criptografia e interceptação	Art. 21. Constitui crime produzir, fabricar, importar, comercializar, oferecer, emprestar, adquirir, possuir, manter sob sua guarda ou ter em depósito, sem autorização ou em desacordo com determinação legal ou regulamentar, equipamentos destinados especificamente à interceptação, escuta, gravação e decodificação das comunicações telefônicas, incluindo programas de informática e aparelhos de varredura: Pena - reclusão, de dois a oito anos, e multa. Parágrafo único. Incorre na mesma pena quem utiliza a criptografia para proteger comunicação de voz, imagem e dados, em desacordo com as normas expedidas pelo órgão federal competente. (...) Art. 28. A ANATEL – Agência Nacional de Telecomunicações fiscalizará as prestadoras de serviços de telecomunicações exigindo delas o cumprimento das normas técnicas determinadas pelos órgãos competentes. §1º A Agência de que trata o caput, ouvido o Instituto Nacional de Tecnologia da Informação – ITI, disciplinará o padrão tecnológico, os procedimentos relativos à produção, comercialização, importação e o uso da criptografia e de sistemas de interceptação. §2º A chave de acesso de qualquer comunicação criptografada deverá ser previamente depositada na ANATEL, nos termos do regulamento de que trata o parágrafo anterior.

27 Até a data de publicação do presente estudo, a última movimentação em sua tramitação sinalizava que o PL havia sido apensado ao PL 1.258/1995.

Norma	Ementa	Justificativa	Dispositivos legais
PL nº **9.808/2018**[28]	Acrescenta os parágrafos 5° e 6º ao art. 10 da Lei nº 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de internet para fins de persecução criminal, nos casos que especifica.	Afirma ser necessária a limitação aos direitos fundamentais e ao devido processo legal para fins de combate ao crime organizado e ao terrorismo.	Art. 1º - A Lei n° 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, passa a vigorar acrescida dos parágrafos 5o e 6o, com a seguinte redação: "Art.10 (...) § 5º - Encontrando-se o agente em situação flagrante de crimes definidos em lei como hediondo, de tráfico de drogas ou terrorismo, poderá o delegado de polícia acessar, independente de autorização judicial, os dados de registro e conteúdos de comunicação privada de dispositivo móvel, quando necessário à investigação e/ou à interrupção da ação delitiva. § 6º - No caso do parágrafo anterior, em se tratando de dados criptografados, poderá o delegado de polícia requisitar, diretamente aos provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação, o fornecimento de chave criptográfica que permita o acesso aos dados e conteúdos de comunicação privada de dispositivo móvel, sem prejuízo do desenvolvimento e emprego, pelas polícias judiciárias, de técnicas e ferramentas tecnológicas que atinjam esse fim específico, incluindo a utilização de dispositivos que possibilitem o acesso a conteúdo anterior à criptografia por meio de aplicativos, sistemas ou outras ferramentas."

28 Até a data de publicação do presente estudo, a última movimentação em sua tramitação sinalizava que o PL havia sido apensado ao PL 6.960/2017.

Norma	Ementa	Justificativa	Dispositivos legais
PL nº **11.007/ 2018**[29]	Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, define terrorismo, dispõe sobre investigação criminal e meios de obtenção de prova, estabelece políticas e estratégias antiterroristas, medidas de prevenção ao aumento de atores terroristas, diminuição dos riscos de atentado e de seus impactos, medidas de persecução penal a atividades terroristas e altera a Lei nº 13.260, de 16 de março de 2016.	Argumenta ser necessária a atualização da Lei 13.260/2016 (Lei Antiterrorismo), bem como os meios de investigação criminal e obtenção de prova.	Art. 6º - Praticar qualquer ato de colaboração com as atividades ou as finalidades de uma organização, grupo ou elemento terrorista, ou para a prática de qualquer dos delitos previstos nesta lei. Pena- reclusão, de cinco a dez anos e inabilitação para o exercício de cargo, emprego ou função por idêntico período. § 1º - Consideram-se atos de colaboração a informação ou vigilância de pessoas, bens ou instalações, a construção, cessão ou utilização de alojamentos ou depósitos, a ocultação, acolhimento ou traslado de pessoas, a organização de práticas de entretenimento ou assistência a elas, a prestação de serviços tecnológicos, e qualquer outra forma equivalente de cooperação ou ajuda às atividades das organizações ou grupos terroristas, grupos ou pessoas a que se refere o parágrafo anterior. Art. 8º (...) §1º - Em qualquer fase da investigação e da persecução penal, serão permitidos os seguintes meios de obtenção de prova: (...) IV – acesso a registro de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais; V - interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica;

29 Até a data de publicação do presente estudo, a última movimentação em sua tramitação sinalizava que o PL havia sido apensado ao PL 2.462/1991

Norma	Ementa	Justificativa	Dispositivos legais
PL nº **2.418/2019**[30]	Altera a Lei nº 12.965/2014, para criar obrigação de monitoramento de atividades terroristas e crimes hediondos a provedores de aplicações de Internet e dá outras providências.	Considera necessário o monitoramento ativo de conteúdos por parte de provedores de aplicação como forma de coibir atos preparatórios ou ameaças de crimes hediondos.	Art. 1º - Esta Lei altera a Lei no 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, para criar obrigação de monitoramento de atividades terroristas e crimes hediondos a provedores de aplicações de Internet e dá outras providências. Art. 2º - A Lei no 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, passa a vigorar acrescida do artigo 21-A, com a seguinte redação: "Art. 21-A. Os provedores de aplicações deverão monitorar ativamente publicações de seus usuários que impliquem atos preparatórios ou ameaças de crimes hediondos ou de terrorismo, nos termos da Lei no 13.260/2016. § 1º - As publicações mencionadas no caput deverão ser repassadas às autoridades competentes, na forma do regulamento. § 2o As obrigações estabelecidas nesse artigo somente se aplicam a provedores de aplicações que possuam mais de 10.000 (dez mil) assinantes ou usuários. § 3 - Na impossibilidade eventual e justificada de cumprimento do disposto no caput, os provedores de aplicações deverão permitir a instalação de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para o mesmo fim."

30 Até a data de publicação do presente estudo, a última movimentação em sua tramitação sinalizava que o PL aguardava parecer do Relator na Comissão e Combate ao Crime Organizado (SCPCCO)

5 _ Eixos de Análise dos Projetos de Lei

5.1 _ Antigas narrativas, novas roupagens

A forma como as políticas sobre tecnologias são apresentadas ao público estabelecem uma moldura, às vezes bem definida, de compreensão sobre suas qualidades, necessidades, conflitos e propostas que pretendem endereçar. Esses vetores determinam quais valores sociais, legais e técnicos estão sendo priorizados e quais bens jurídicos irão se sobressair tendo em vista o contexto apresentado pelos formuladores de políticas. Às vezes, o formato assumido por esses discursos objetivam a manutenção do status quo e a continuidade da expansão das técnicas de vigilância[31].

É interessante a ideia de "enquadramento"[32] para explorar como as narrativas desenvolvidas por agentes que constroem políticas se apresentam, quais histórias contam e de quais recursos (sejam retóricos ou processuais-legislativos) fazem uso para abordar a defesa da privacidade (ou as ameaças a esta) e da regulação de tecnologias. Partindo da complexidade sobre a governança das novas tecnologias, é interessante observar como essas narrativas se inserem nas dinâmicas geopolíticas, especialmente naquelas que têm por objeto a criptografia.

_ Crypto Wars: a criptografia é inimiga da lei?

Na história recente, recursos de encriptação sobre informações e comunicações, no contexto da Internet, têm sido "enquadrados" por agências de investigação enquanto obstáculos à efetividade das persecuções penais e, portanto, como ferramentas associadas ao cometimento de ilícitos. As expressões criminosas suscitadas pelas forças de investigação caracterizam comumente figuras contra as quais não há oposição na opinião pública e, consequentemente, supostamente justificariam restrições ao uso de recursos tecnológicos usados por esses criminosos. Entre as figuras[33], o combate a redes

31 MURPHY, Maria Helen. **Surveillance and the Law: language, power and privacy.** Routledge Focus, 2019. Pág 2.

32 BENNETT, Colin, **The Privacy Advocates: resisting the spread of surveillance**. The MIT Press, 2008.The Privacy Advocates: resisting the spread of surveillance. The MIT Press, 2008. Pág 26.

33 Não à toa, o termo "Cavaleiros do Infocalipse" foi cunhado para designar narrativas utilizadas com frequência para enquadrar uma dada tecnologia no uso desvirtuado, ilegal ou ilegítimo. Usualmente, apostam na sensibilidade desses fenômenos para que sejam alcançadas políticas excepcionais que resvalam na garantia de direitos. Mais em SCHNEIER, Bruce. **Scaring people into supporting backdoors.** Schneier on Security (website). Disponível em https://www.schneier.com/blog/archives/2019/12/scaring_people_.html; MAY, Timothy C. **The Cyphermonicon.**

de pedofilia, tráfico de drogas, cibercrimes, terrorismo, entre outros, são utilizados por agências de investigação para legitimar propostas de restrição tecnológica – em geral aquelas que objetivam a proteção ao sigilo e à privacidade[34] -, bem como para legitimar a operação de aparatos de vigilância e monitoramento

No centro dos conflitos entre políticas de restrição à privacidade[35] ou ao sigilo[36] das comunicações versus propostas para democratizar tecnologias cuja função é alcançar a privacidade, a criptografia é fundamentalmente representativa. Criptógrafos promovem, incansavelmente, avanços técnicos e buscam tornar computacionalmente mais distantes as possibilidades de decriptação por um agente não autorizado. Da mesma forma, defensores da privacidade e ativistas articulam movimentos e coalizões[37] para fortalecer a criptografia enquanto ferramenta necessária à efetivação dos direitos fundamentais. Por outro lado, outras coalizões e campanhas a favor de brechas em sistemas criptográficos, acessos excepcionais e exploração de vulnerabilidades são encampadas por representantes das forças de investigação no Brasil[38] e em diversos outros países[39].

Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ; e CAREY, Robert F.; BURKEL, Jacquelyn **A. Revisiting the Four Horsemen of the Infocalypse: representations of anonymity and the internet in Canadian newspapers.** First Monday, julho de 2007. Disponível em https://www.firstmonday.org/ojs/index.php/fm/article/view/1999/1874;

34 PFEFFERKORN, Riana. **The EARN IT Act: How to ban end-to-end encryption without actually banning it.** Stanforford's CIS - The Center for Internet and Society, janeiro de 2020. Disponível em http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it**.** Acesso em 27 de abril de 2020; KOCH, Richie. **Here are all the countries where the government is trying to ban VPNs** ProtonVPN, outubro de 2018. Disponível em: https://protonvpn.com/blog/are-vpns-illegal/. Acesso em 27 de abril de 2020.

35 O ex-Procurador Geral Adjunto dos Estados Unidos, Rod Rosenstein, alega a existência de uma suposta "privacidade absoluta" possibilitada pela criptografia. Ver ROSENSTEIN, Rod. **Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy.** Department of Justice, 2017. Disponível em https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval. Acesso em 27 de abril de 2020. Na realidade, sempre houve espaços inalcançáveis à vigilância policial e não seria papel do cidadão facilitar o acesso a suas comunicações.

36 O Procurador Geral dos Estados Unidos, William Barr, alega haver um "sigilo impenetrável" tornado possível pela criptografia. Ver BARR, William. **Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security.** Department of Justice. New York, 2019. Disponível em https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber. Acesso em 27 de abril de 2020. Seria, então, igualmente irrazoável sugerir que todos os espaços de comunicação devam ser penetráveis ao proveito do Estado.

37 Ver, por exemplo, HALL, Joseph Lorenzo. **Open Letter: Facebook's and-to-end encryption plans.** Center for Democracy and Technology (CDT). Outubro de 2019. Disponível em https://cdt.org/insights/open-letter-facebooks-end-to-end-encryption-plans. Acesso em 27 de abril de 2020; ACCESS NOW. **Global coalition from five nations demands "Five Eyes" respect encryption.** Access Now, Junho de 2017. Disponível em: https://www.accessnow.org/83-organizations-experts-5-nations-demand-five-eyes-respect-strong-encryption/. Acesso em 27 de abril de 2020.

38 Ministério da Justiça. Brasil. **Declaração do Going Dark Brasil.** I Simpósio Going Dark Brasil. Disponível em https://www.justica.gov.br/news/collective-nitf-content-1550010028.2/documentos/declaracao-do-going-dark-brasil.pdf. Acesso em 27 de abril de 2020.

39 G7. **Combating the use of the Internet for terrorists and violent extremist purposes.** G7 France, Biarritz, 2019. Disponível em http://www.g7.utoronto.ca/justice/2019-internet.pdf. Acesso em 27 de abril de 2020.

A década de 1990 foi exemplar no que se refere ao conflito entre essas expressões políticas e ilustra bem o mote narrativo que pretende justificar políticas públicas de "acesso excepcional" a comunicações encriptadas. O caso conhecido como Clipper Chip[40] – episódio em que o governo estadunidense pretendeu implementar um chip cujo objetivo era fornecer encriptação às comunicações telefônicas dos cidadãos, ao tempo em que era posta em "custódia"[41] uma chave de decriptação, à disposição das agências de investigação – carregava a narrativa de combate ao tráfico de drogas e ao terrorismo[42]. O episódio se tornou o epicentro do que ficou conhecido, até os dias de hoje, como "Crypto Wars"[43].

As Crypto Wars foram, então, renovadas como consequência das investigações sobre o tiroteio em San Bernardino. Em 2016, o FBI buscou a ajuda da Apple para ter acesso ao iPhone pertencente a um dos responsáveis pelo atentado. A empresa, então, recusou-se a cumprir com o pedido. Uma longa batalha jurídico-política foi estabelecida e o FBI buscou carimbar o rótulo "Going Dark"[44] para se referir às dificuldades que as agências de investigação estavam enfrentando para obter acesso a provas e evidências na persecução de crimes como o de San Bernardino. Tentou-se, aí, estabelecer uma narrativa predominante que girasse em torno das dificuldades investigativas – das quais a garantia de direitos fundamentais e à segurança das redes não passavam de ponderações[45].

_ A importação da narrativa estadunidense

Nos projetos de lei brasileiros, o conjunto de propostas de interceptação às comunicações encriptadas, por sua vez, reenquadram a mesma situação, ajustando ao

40 LEVY, Steven. **Battle of the Clipper Chip.** The New York Times Magazine, 1994. Disponível em https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html. Acesso em 27 de abril de 2020.

41 ABELSON, Hal et al. **The risks of key recovery, key encryption and trusted third-party encryption.** Disponível em https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf. Acesso em 27 de abril de 2020.

42 SCHULTZ, Matthias. **Clipper meets FBI vs. Apple - a comparison of the cryptography discourses from 1993 and 2016.** COGITATIO, Media and Communication, vol. 5, 2017, pag 57. Disponível em https://www.cogitatiopress.com/mediaandcommunication/article/view/805. Acesso em 10 de junho de 2020.

43 KHEL, Danielle; WILSON, Andi; BANKSTON, Kevin. **Doomed to Repeat History? Lessons from the Crypto Wars of the 1990.** Open Technology Institute. New America, 2015.

44 A própria escolha do rótulo *Going Dark* em si já carrega um elemento psicológico, apostando no medo do escuro para a correlação do termo com os desafios que as agências de investigação enfrentam. Além disso, a expressão *Crypto Wars* também pode apontar para uma direção em que o Estado tenha mais legitimidade para acionar medidas excepcionais, afinal a defesa e a segurança nacional, em tempos de exceção, é responsabilidades das forças estatais. Ao reafirmar um estado de "guerra", seria possível reforçar essa narrativa. Essa análise é melhor explorada em PFEFFERKORN, Riana. **The rhetoric of responsible encryption.** Stanford's CIS - Center of Internet and Society. Outubro de 2017. Disponível em https://www.justsecurity.org/46102/rhetoric-responsible-encryption/. Acesso em 27 de abril de 2020.

45 COMEY, James. **Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?** Federal Bureau of Investigation. Brookings Institution, 2014. Disponível em https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acesso em27 de abril de 2020.

contexto investigativo, criminal e político nacional. No PL nº 11.007/2018, por exemplo, proposta de substitutivo à Lei 13.260/2016 (Lei Antiterrorismo em vigor), procura-se justificar que há incompatibilidade entre as atuais formas de combate ao terrorismo e os recursos dos quais o terrorismo faz uso. O projeto afirma que afastar a vigilância de órgãos de segurança pública e de inteligência estatal é uma das bases do terrorismo, o qual

> "possui como nota diferencial a clandestinidade, no sentido de que procuram manter suas atividades fora do radar de vigilância de órgãos de segurança pública e de inteligência. A violência terrorista, por sua vez, não é secreta nem aspira a sê-lo como outros delitos"

A comunicação, portanto, segundo o Projeto de Lei nº 11.007/2018, seria um elemento logístico essencial para o preparo, execução e sucesso de um ato terrorista. Reflexo de uma mudança de lógica entre os dois modelos de dispor sobre o combate ao terrorismo é o fato de que, na lei em vigor, a palavra "comunicação" aparece uma única vez, enquanto o PL nº 11.007/2018 conta com oito menções ao longo dos artigos e justificativa - com ênfase nos meios eletrônicos.

Na mesma linha de raciocínio, em artigo publicado por oficiais da Agência Brasileira de Inteligência (ABIn) sobre "o processo de radicalização e ameaça terroristas no contexto brasileiro a partir da Operação Hashtag"[46], foi apontado que a comunicação de jovens em mídias sociais foi central, entre as características particulares nacionais, para facilitar a expansão do Estado Islâmico no país. Quanto mais radicais eram os indivíduos, mais rapidamente abandonavam grupos de discussão em redes sociais e partiam em direção a "aplicativos móveis criptografados". A partir destes, comunidades iam se formando e, consequentemente, mais progressivamente os discursos iam se radicalizando e células extremistas tomariam forma.

A criptografia seria enquadrada enquanto ferramenta essencial à integração de agentes terroristas e criaria terreno à radicalização dos discursos. No entanto, apesar de haver indícios de uso de plataformas populares de criptografia por grupos extremistas, dados apontam para usos alternativos de encriptação, como de sistemas de fabricação própria - como no caso do Estado Islâmico[47], guiados pela fuga de plataformas associa-

46 A, Thiago; O, Augusto; S, Allan. **O processo de radicalização e a ameaça terrorista no contexto brasileiro a partir da Operação Hashtag**. Revista Brasileira de Inteligência: Abin, n. 12, dezembro de 2017. Pág. 13. Disponível em http://www.abin.gov.br/conteudo/uploads/2018/05/RBI12-Artigo1-O-PROCESSO-DE-RADICALIZA%C3%87%C3%83O-E-A-AMEA%C3%87A-TERRORISTA-NO-CONTEXTO-BRASILEIRO-A-PARTIR-DA-OPERA%C3%87%C3%83O-HASHTAG.pdf. Acesso em 04 de abril de 2020.

47 AHLBERG, Christopher. **How Al-Qaeda Uses Encryption Post-Snowden (Part 2).** Recorded Future. Agoto de 2014. Disponível em https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/. Acesso em 27 de

das à indústria ocidental - e mesmo de aparelhos de comunicação de curta vida útil, como telefones descartáveis, os chamados burner phones[48]. Aponta-se que em ataques terroristas recentes de grande relevo na geopolítica internacional - como em Mumbai, Londres, Boston, San Bernardino, Paris ou Bruxelas – nenhum indício sugere que a criptografia tenha assumido uma função determinística para o sucesso desses incidentes[49].

Além de tudo, o terrorismo não é o único fenômeno que depende da troca sistemática de informações para existir e produzir efeitos. Movimentos sociais são exemplos de manifestações de legítimo interesse, traços democráticos que ativam transformações sociais e valorizam medidas de precaução, autocuidado, administração de grupos em redes sociais, sigilo e, portanto, meios de comunicação seguros. Atualmente, portanto, a criptografia, é apontada como recurso essencial para o exercício da liberdade de expressão, reunião e associação[50].

Interessa, portanto, fazer a correlação do PL nº 11.007/2018 com o contexto político nacional tendo em vista outros projetos que também já foram propostos em momento anterior[51] e que fazem parte de uma série de medidas tomadas por parlamentares que visam alterar a definição de "atos terroristas" no cenário brasileiro. Necessário lembrar que, nas disputas político-legislativas vivenciadas à época da atual Lei Antiterrorismo, entre 2013 e 2016, houve grande problematização da abrangência da definição de "atos terroristas". Setores de defesa dos direitos humanos classificam essas articulações como tentativas de criminalização de movimentos sociais, com o intuito de ofuscar protestos na medida em que iam de encontro ao exercício de direitos políticos[52].

---

abril de 2020.

48 MOODY, Glyn. **Paris terrorists used burner phones, not encryption, to evade detection.** Arstechnica, março de 2016. Disponível em https://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/. Acesso em 27 de abril de 2020.

49 LEWIS, James A; ZHENG, Denise E.; CARTER, William A. **The Effect of Encryption on Lawful Access to Communication and Data**. CSIS - Center for Strategic and International Studies, fevereiro de 2017. Disponível em https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf. Acesso em 27 de abril de 2020.

50 ANISTIA INTERNACIONAL. **Encryption: a matter of human rights.** Anistia Internacional, março de 2016. Disponível em https://www.amnesty.org/download/Documents/POL4036822016ENGLISH.pdf. Acesso em 27 de abril de 2020.

51 BRASIL. Senado Federal. **Projeto de Lei do Senado de nº 272**, de 2016. Altera a Lei nº 13.260, de 16 de março de 2016, a fim de disciplinar com mais precisão condutas consideradas como atos de terrorismo. do Senado. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/126364. Acesso em 27 de abril de 2020. Interessante notar que os discursos que criminalizam os movimentos sociais voltaram com toda força com a presidência de Jair Bolsonaro, que fez referência direta de apoio ao projeto de lei aqui mencionado. Disponível em SARDINHA, Edson. **Bolsonaro defende Lei Antiterrorismo vetada por Dilma temida por movimentos sociais.** Congresso em Foco, janeiro de 2019. Disponível em https://congressoemfoco.uol.com.br/governo/em-meio-a-ataques-no-ceara-bolsonaro-defende-lei-antiterrorista-vetada-por-dilma-e-temida-por-movimentos-sociais/. Acesso em 27 de abril de 2020.

52 ARTIGO 19. **As restrições ao direito de protesto no Brasil.** Disponível em https://artigo19.org/5anos-de2013/. Acesso em 27 de abril de 2020.

5.2 _ Backdoors e restrições à liberdade criptográfica

Diante da desconfiança construída em relação às iniciativas e considerando as narrativas de setores de investigação, ampliar a tipificação sobre "atos de colaboração", como quer o art. 6º, §1º do PL 11.007/2018, leva à possível leitura de que plataformas que ofereçam criptografia ponta a ponta poderiam ser responsabilizadas.

> Art. 6o. Praticar qualquer ato de colaboração com as atividades ou as finalidades de uma organização, grupo ou elemento terrorista, ou para a prática de qualquer dos delitos previstos nesta lei
>
> (...)
>
> § 1o. *Consideram-se atos de colaboração* a informação ou vigilância de pessoas, bens ou instalações, a construção, cessão ou utilização de alojamentos ou depósitos, a ocultação, acolhimento ou traslado de pessoas, a organização de práticas de entretenimento ou assistência a elas, a *prestação de serviços tecnológicos, e qualquer outra forma equivalente de cooperação ou ajuda às atividades das organizações ou grupos terroristas, grupos ou pessoas a que se refere o parágrafo anterior*. (grifo nosso)

A tentativa de enquadrar intermediários como responsáveis por facilitar condutas terroristas e outras categorias de crimes também não é exatamente nova. Em Audiência Pública convocada pelo STF[53], em 2017, o Secretário de Cooperação Internacional da Procuradoria Geral da República (PGR), Vladimir Aras, afirma que o WhatsApp

> "serve como meio para prática de infrações penais e sanções sobre pessoas jurídicas estão presentes, também, por exemplo, na Lei Anticorrupção Empresarial, art. 19, quando pessoas jurídicas são utilizadas para essas práticas ilícitas também podem ser dissolvidas ou ter suas atividades suspensas".

53 SUPREMO TRIBUNAL FEDERAL. **STF inicia audiência pública que discute bloqueio judicial do WhatsApp e Marco Civil da Internet.** STF Notícias, junho de 2017. Disponível em http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=345369. Acesso em 27 de abril de 2020.

O paralelo de responsabilização com as práticas previstas na Lei Anticorrupção deixam claro que a narrativa de responsabilizar pessoas jurídicas (no caso, provedores), como intermediários para o cometimento de ilícitos, como a preparação de atos terroristas, de fato habita os discursos. O fornecimento de técnicas de sigilo, exemplificados pela encriptação ponta a ponta das mensagens, é potencialmente caracterizado como o próprio comportamento ilícito.

Em sucessivos discursos de representantes do FBI e do Departamento de Justiça dos Estados Unidos (DOJ), encontram-se, igualmente, sistemáticas retóricas que sugerem a responsabilização, se não penal, moral das plataformas de criptografia. A tradição do DOJ em chamar o acesso excepcional de "encriptação responsável"[54] (responsible encryption, no original) leva a crer que a criptografia ponta a ponta seria irresponsável.[55] As narrativas governamentais são fabricadas de forma a garantir o direcionamento do debate exatamente para onde as autoridades querem que se encaminhe – caminho este que pode ser identificado como a criminalização da criptografia - mais uma vez enquadrando a disputa.

Importar para o Brasil a narrativa da ameaça terrorista implica em uma tradução bastante delicada na medida em que há uma profunda diferença de realidades sociopolíticas. E, como visto, a possibilidade de que a "prestação de serviços tecnológicos" seja encarada enquanto cooperação ou ajuda ao terrorismo pode ser interpretada como o ânimo político necessário para se atingir a responsabilização das plataformas em casos de comunicações entre seus usuários nestas circunstâncias - algo inviável do ponto de vista da garantia aos direitos fundamentais, do princípio da inimputabilidade de intermediários[56] e do potencial de inovação tecnológica - ou mesmo pressão política para se alcançar o acesso excepcional através de acordos público-privados.

Ao longo das últimas décadas, as narrativas das quais as autoridades de investigação lançam mão, ainda que assumam variadas roupagens, apontam para a mesma finalidade: atingir o enfraquecimento da criptografia e acessar o conteúdo das comunicações dos usuários. Portanto, é necessário equacionar as propostas legislativas com discursos governamentais e identificar a vontade política para além das agendas aparentes - como o combate ao terrorismo, ao tráfico de drogas ou à pedofilia - e contextualizar com a realidade sobre o exercício de direitos fundamentais no Brasil e com o ecossistema de segurança da rede.

---

54 ROSENSTEIN, Rod. **Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy.** Department of Justice, 2017. Disponível em https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval. Acesso em 27 de abril de 2020..

55 PFEFFERKORN, Riana. **A response to "responsible encryption".** Stanford's CIS - Center for Internet and Society, outubro de 2017. Disponível em http://cyberlaw.stanford.edu/blog/2017/10/response-%E2%80%9Cresponsible-encryption%E2%80%9D. Acesso em 27 de abril de 2020.

56 O conceito será melhor explicado no capítulo "De volta à imputabilidade da rede".

_ O caso do acesso excepcional

Independentemente da narrativa adotada ou dos rótulos escolhidos para a mesma disputa, a corrida política e regulatória encampada pelas agências de investigação aponta, na maioria das vezes, para um mesmo objetivo: o acesso através de uma chave reservada para tal finalidade.

Historicamente, o "acesso excepcional" foi[57] - e é[58] - a proposta de solução número um para os desafios relacionados à criptografia que enfrentavam as agências de investigação. Consta em criar vulnerabilidades em sistemas criptográficos que permitam o acesso excepcional mediante uma chave guardada sob custódia de uma entidade de confiança - em geral do governo ou de um ente privado designado previamente[59]. A vulnerabilidade explorada por essa chave mestra teria como consequência um backdoor (ou uma "porta dos fundos"). O sistema de custódia de chaves, também conhecido como key escrow foi, por exemplo, proposto à época do Clipper Chip, mencionado acima, e guarda semelhança com propostas legislativas recentes.

Formas de introduzir mecanismos de interceptação e acesso a mensagens encriptadas aparecem ora de maneira mais tímida, ora de maneira mais explícita em projetos de lei no Brasil. Das propostas mais recentes, a apresentada pelo PL nº 9.808/2018 é a que mais se aproxima de uma tentativa explícita de impor uma obrigatoriedade, aos provedores de aplicação, de acesso a comunicações encriptadas via backdoor. O PL propõe a inserção dos parágrafos 5º e 6º no art. 10 do Marco Civil da Internet. Em seu parágrafo 6º, estabeleceria que

> "No caso do parágrafo anterior[60] em se tratando de dados criptografados, poderá o delegado de polícia requisitar, diretamente aos provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação, o fornecimento de chave criptográfica que permita o acesso aos

57 LEVY, Steven. **Battle of the Clipper Chip.** The New York Times Magazine, 1994. Disponível em https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html. Acesso em 27 de abril de 2020.

58 VENTURA, Felipe. **Proposta que banir WhatsApp e Telegram se não quebrarem sigilo no Brasil.** Tecnoblog, janeiro de 2019. Disponível em https://tecnoblog.net/274333/whatsapp-telegram-quebra-sigilo-proposta-cnj/. Acesso em 28 de abril de 2020; RINALDI, Camila. **"Pacote Anticrime" de Moro quer facilitar interceptação de conversas no WhatsApp.** Olhar Digital, fevereiro de 2019. Disponível em https://olhardigital.com.br/noticia/-pacote-anticrime-de-moro-quer-facilitar-interceptacao-de-conversas-no-whatsapp/82687. Acesso em 28 de abril de 2020.

59 ABELSON, Hal et al. **The risks of key recovery, key encryption and trusted third-party encryption.** Maio de 1997. Disponível em https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf. Acesso em 27 de abril de 2020.

60 Sobre acesso a dados de registro e conteúdo de comunicação privada independente de autorização judicial. Essa passagem será analisada mais adiante neste estudo.

> dados e conteúdos de comunicação privada de dispositivo móvel"

Apesar da variedade de terminologias e hipóteses confusas - tal como a requisição de chaves criptográficas à provedores de conexão (não se vislumbra em que situação isso seria necessário ou mesmo estaria de acordo com a realdade sobre a encriptação/interceptação de comunicações em serviços OTT[61]) ou a autores de aplicativos (figura não condizente com a literatura sobre provedores[62], tampouco com o Marco Civil da Internet) - esta parte do estudo irá se ater, principalmente, à requisição aos provedores de aplicação.

A análise do fluxo procedimental sobre interceptações e acesso a dados armazenados passa pela observação de um conjunto de previsões baseadas, por um lado, no direito à inviolabilidade das comunicações e na privacidade e, por outro, no procedimento legal e hipóteses para se atingir a interceptação.

O parâmetro basilar para o acesso às comunicações, no âmbito de procedimentos investigativos e processuais, é encontrado no art. 5º, inciso XII, da Constituição Federal:

> "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

A passagem sobre regulamentação legal foi contemplada com a Lei 9.296/1996 (Lei de Interceptações), a qual prevê os requisitos necessários à suspensão do sigilo, entre eles, haver indícios razoáveis, ser estritamente necessário o recurso à obtenção das provas e a imprescindibilidade de uma ordem judicial. A Lei dispõe, em seu Art. 1º, §1º, que a regulamentação também diz respeito "à interceptação do fluxo de comunicações em sistemas de informática e telemática."

A Lei de Interceptações toma forma e sentido, principalmente, se aplicável à infraestrutura de telefonia. Essa infraestrutura, por sua vez, é acompanhada por resoluções da Agência Nacional de Telecomunicações (ANATEL) que, tornam possível ou

61 Ou *Over-the-top,* aqueles que operam na camada de aplicações da Internet, ou seja, onde os usuários da Internet produzem, acessam e trocam informações. Mais em CASTRO, Oona. **Serviços over-the-top: conceitos em disputa podem ter consequências para sua regulação.** PoliTICS, junho de 2018. Disponível em https://politics.org.br/edicoes/servi%C3%A7os-over-top-conceitos-em-disputa-podem-ter-consequ%C3%AAncias-para-sua-regula%C3%A7%C3%A3o. Acesso em 28 de abril de 2020.

62 SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet: construção e aplicação.** Juiz de Fora: Ed. Editar, 2016. Págs. 67-69.

habilitam o procedimento previsto para a violação do sigilo das comunicações em telefonia[63]. Portanto são obrigadas, as prestadoras de serviços de telecomunicações, a manterem mecanismos em seus sistemas que os tornem passíveis de interceptação. Devem possuir a habilidade para tal.

Pode-se dizer que o Marco Civil da Internet (Lei nº 12.965/2014), por sua vez, abrange a necessidade de que provedores de conexão sejam hábeis a guardar registro de conexão pelo prazo de um ano (art. 13), bem como que provedores de aplicação de Internet guardem, ou seja, tornem acessíveis ou mesmo sejam hábeis a disponibilizar os registros de conexão às aplicações por um prazo de seis meses (art. 15). Aqui, o sigilo pode ser quebrado mediante ordem judicial e, mais, deve ser possível o acesso, cumpridas as exigências procedimentais e legais.

O art. 7 do Marco Civil da Internet, por sua vez, dispõe, precisamente sobre a inviolabilidade e sigilo dos fluxos de comunicações pela Internet (inciso II) – dados em trânsito, como aqueles percebidos no meio-tempo em que uma conversa está ocorrendo em determinada aplicação - e das comunicações privadas armazenadas (inciso III) - dados em repouso, como aqueles armazenados em servidores após a comunicação já haver ocorrido, dados armazenados em nuvem ou em um disco rígido de celular. No caso de ambos os incisos, é prevista possibilidade de suspensão da inviolabilidade mediante ordem judicial.

> O caso de acesso a metadados é, na grande maioria das vezes, compreendido erroneamente como menos grave. Ainda que não seja viável, na maioria das vezes, encriptar ponta a ponta os metadados (já que os serviços necessitam, por uma questão de protocolos técnicos, processar essas informações para viabilizar o serviço prestado, a exemplo de uma aplicação de mensagem), isso não quer dizer que essas informações não devam ser protegidas por altos padrões de sigilo, respeitado o devido processo legal. Padrões comportamentais podem ser extraídos apenas dessas informações "menos sensíveis" e perfis podem ser traçados para fins de vigilância abusiva, violando a privacidade e criando narrativas comprometedoras aos titulares desses dados

É fácil perceber que nos casos de a) requisição de interceptação dos conteúdos das comunicações havidas por meio de telefonia, b) requisição de registros de conexão à provedores de Internet e c) requisição de registros de acesso à provedores de aplicação, a habilidade de fornecer os dados é necessária e regulada por disposições ora encontradas na Lei de Interceptações, respaldadas em resoluções da ANATEL, ora na disciplina do Marco Civil da Internet. No entanto, para o caso da suspensão da regra de inviolabilidade do conteúdo das comunicações, tal habilidade não é regulamentada ou exigida aos provedores de aplicação[64].

63 ABREU, Jacqueline. **Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação.** Revista Brasileira de Políticas Públicas, Vol 7, nº 3, 2017. Pág. 34.

64 ABREU, Jacqueline. **Op cit.**

Por um lado, nada impede que uma ordem judicial seja emitida para que uma plataforma forneça as comunicações de seus usuários. Caso não carregue mecanismos de criptografia, a medida judicial poderá ser eficaz. Ainda, caso a plataforma tenha criptografia, porém, por razões de política privada, guarde chave de decriptação para uso excepcional – ou seja, disponibilize um backdoor em seu sistema - a ordem também poderá ter sucesso.

É válido ressaltar que o Decreto 8.771/2016, que procurou regulamentar o Marco Civil da Internet, trouxe a defesa do uso de técnicas de encriptação como diretriz de padrão de segurança na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas por parte dos provedores de conexão e de aplicação, para que garantam a inviolabilidade dos respectivos dados visando a proteção e segurança de informações dos usuários.

Por outro lado, a legislação nacional não proíbe que políticas privadas dos provedores de aplicação decidam por implementar um sistema de encriptação ponta a ponta, dando robustez aos mecanismos de segurança de informação e autonomia ao usuário para decidir sobre o fornecimento do conteúdo de suas comunicações. Afinal, não são obrigadas a construir a habilidade de decriptação, ainda que um procedimento processual exista para prever a possibilidade de suspensão do direito ao sigilo das comunicações.

A proteção possibilitada pela criptografia ponta a ponta não é limitada - e nem deveria ser - pelo ordenamento jurídico, sequer há obrigatoriedade dos provedores serem capazes de revertê-la. Sendo assim, o cenário jurídico e regulatório brasileiro tornaria, em parte, ineficazes as propostas do PL nº 9.808, sobretudo em situações em que os

Amplamente referenciado nesta área, o estudo Keys Under Doormats, elenca pelo menos três principais pontos em razão dos quais propostas de acesso excepcional ao conteúdo encriptado trariam ainda mais graves riscos de segurança, inibiriam a inovação e ameaçariam os direitos humanos:

1. Seriam um grande retrocesso na implementação de recursos de segurança na Internet, incluindo forward secrecy – quando chaves de decriptação são deletadas imediatamente após o uso. Assim o roubo de uma chave de decriptação não comprometeria mensagens anteriores;

2. Aumentaria a complexidade de um sistema de segurança – cada novo recurso interage com os outros, criando novas vulnerabilidades. A gestão desse acesso "pontual" às mensagens seria muito mais complexo do que os recursos de vigilância utilizados atualmente por governos.

3. Haveria a concentração de ataques nas entidades ou órgãos que administrariam as chaves. Consequentemente, um agente malicioso que conseguisse acesso às chaves ganharia o mesmo privilégio de acesso às comunicações, fugindo do controle das autoridades

órgãos de investigação estivessem diante de comunicações encriptadas ponta a ponta. As disputas jurídicas levadas a diante com base em um suposto apoio nessa proposta

apenas gerariam insegurança jurídica às empresas e fragilizariam, de forma estrutural, a segurança e a privacidade dos usuários.

_ O caso da regulação da criptografia

Mesmo que, atualmente, esteja presente de forma rotineira nas mais diversas aplicações, - desde comunicações pessoais a transações bancárias, armazenamento de dados, comércio online, entre outros - a criptografia já foi estritamente regulada e limites eram postos (e ainda são, em alguns países[65]) a sua fabricação, exportação e uso[66].

No Brasil, o desenvolvimento da criptografia não sofreu embargos, regulações ou restrições normativas. Pelo contrário, a Infraestrutura Brasileira de Chaves Públicas (ICP-Brasil), órgão público instituído pela Medida Provisória nº 2.200-2/2001, estabelece quais são os algoritmos e padrões mínimos de segurança recomendados para o emprego de tecnologias de criptografia em território nacional[67]. Se não há regulação, há uma agenda que promove o emprego de técnicas progressistas e cada vez mais avançadas.

> A criptografia é cada vez mais presente em normas que valorizam a segurança da informação em território nacional. A Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222/2020), por exemplo, cita a criptografia 9 vezes em suas recomendações e diretrizes, e afirma "o uso adequado de recursos criptográficos comprovadamente habilita uma camada de segurança adicional de extrema relevância para atingir os níveis desejados de proteção de dados em repouso ou em trânsito". E diz mais: "Recomenda-se, nesse sentido, o investimento na busca de soluções inovadoras em novos tipos de criptografia, de forma a considerar seu potencial variado de aplicabilidade e seu valor estratégico para a segurança da informação e para a segurança cibernética do País."

Ainda em 2009, no entanto, foi apresentado o PL nº 5.285/2009, fruto da CPI de Escutas Telefônicas Clandestinas ou "CPI do Grampo"[68], que ocorreu entre 2007 e 2009 para investigar denúncias de escutas ilegais. A iniciativa procura regulamentar o Art. 5º, inc. XII da Constituição Federal e, consequentemente, renovar a Lei de Interceptações. Como resultado do que foi debatido em audiências públicas no âmbito da

65 Ver, por exemplo, STILGHERRIAN. **The Encryption Debate in Australia.** Carnegie Endowment for International Peace, maio de 2019. Disponível em https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217. Acesso em 28 de abril de 2019.

66 O capítulo "Criptografia e Sociedade" deste estudo apresenta um histórico sobre a situação da criptografia durante o século 20, a regulação à qual era submetida, suas limitações de exportação e seu processo de mudança de condição para um uso mais generalizado pela sociedade.

67 ICP-BRASIL. Infraestrutura de Chaves Públicas Brasileira. **Padrões e Algoritmos Criptográficos da ICP-Brasil.** ICP-Brasil, outubro de 2019. Disponível em https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/01.1/DOC-ICP-01.01_-_v.4.2_PADROES_E_ALGORITMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL.pdf. Acesso em 28 de abril de 2019.

68 ESTADÃO. **Com base em denúncia, Câmara cria CPI do Grampo Telefônico.** Outubro de 2007. Disponível em https://politica.estadao.com.br/noticias/geral,com-base-em-denuncia-camara-cria-cpi-do-grampo-telefonico,69557. Acesso em 10 de junho de 2020.

CPI, o projeto pretende, entre outras disposições, prever mecanismos de fiscalização e maior rigor na autorização judicial para a interceptação, como, por exemplo, a notificação do Ministério Público. Por outro lado, também procura criar responsabilidades criminais para o uso de ferramentas de encriptação e decriptação:

> Art. 21. Constitui crime produzir, fabricar, importar, comercializar, oferecer, emprestar, adquirir, possuir, manter sob sua guarda ou ter em depósito sem autorização ou em desacordo com determinação legal ou regulamentar, equipamentos destinados especificamente à interceptação, escuta, gravação e decodificação das comunicações telefônicas, incluindo programas de informática e aparelhos de varredura:
>
> Pena - reclusão, de dois a oito anos, e multa.
>
> Parágrafo único. *Incorre na mesma pena quem utiliza a criptografia para proteger comunicação de voz, imagem e dados, em desacordo com as normas expedidas pelo órgão federal competente.* (grifo nosso)

Caminhar pelo terreno da criminalização - ou regulação - do uso de ferramentas de encriptação ou decriptação é bastante delicado. Deve-se levar em consideração, por um lado, a crítica necessária à importação e exportação de ferramentas de vigilância para uso não regulado[69] ou distante da apreciação judicial. Por outro, a importância do princípio da "inovação sem necessidade de permissão" (permissionless innovation, no original), basilar à expansão das redes conectadas e à liberdade de criar tecnologias - "o mais importante ativo da Internet", segundo Vint Cerf, um dos criadores do Protocolo TCP/IP[70].

De início, a decriptação de sistemas de comunicação, em alguma medida, faz parte de rotinas de criptoanálise[71] de especialistas em cibersegurança. Essas rotinas, aliadas ao avanço computacional, são responsáveis pelo avanço dos esquemas cripto-

69 CANTO, Mariana. **Quanto vale um segredo? Dilemas éticos no mercado do *lawful hacking*.** IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, abril de 2020. Disponível em https://ip.rec.br/2020/04/23/quanto-vale-um-segredo-dilemas-eticos-no-mercado-do-lawful-hacking/. Acesso em 08 de maio de 2020.

70 HUIZER, Erik. **Permissionless inovation, a cornerstone of a successful Internet.** Internet Society, março de 2015. Disponível em https://www.internetsociety.org/wp-content/uploads/2017/08/huizer-permissionless-innovation-1.pdf. Acesso em 29 de abril de 2020.

71 SILVA, Gabriel Leite Batista. **Criptoanálise.** UFRJ, 2010. Disponível em https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/gabriel/cript.htm. Acesso em 08 de maio de 2020.

gráficos menos sofisticados para modelos criptográficos de complexidade matemática elevada.

Considerado o contexto em que foi proposto, o PL nº 5.285/2009 aponta para a criação de mecanismos que criminalizem a escuta ilegal - ou clandestina[72] - como é observado no caput do Art. 21, porém de forma desproporcional. Além disso, o parágrafo único também avança sobre o que pode ser chamado direito à criptografia[73] ao querer criar condições ou amarras com base em novas normativas. Leva a crer que as "normas expedidas pelo órgão federal", no parágrafo único do artigo acima, se referem à ANATEL e as suas resoluções que estabelecem determinações sobre os procedimentos que efetivam, atualmente, a interceptação telefônica. Sobre essas regras, o PL propõe que:

> Art. 28. A ANATEL – Agência Nacional de Telecomunicações fiscalizará as prestadoras de serviços de telecomunicações exigindo delas o cumprimento das normas técnicas determinadas pelos órgãos competentes.
>
> §1º A Agência de que trata o caput, ouvido o Instituto Nacional de Tecnologia da Informação – ITI, disciplinará o padrão tecnológico, os procedimentos relativos à produção, comercialização, importação e o uso da criptografia e de sistemas de interceptação.
>
> §2º A chave de acesso de qualquer comunicação criptografada deverá ser previamente depositada na ANATEL, nos termos do regulamento de que trata o parágrafo anterior. (grifos nossos)

Parece haver uma possível correlação entre os "padrões, procedimentos de produção, comercialização importação e uso" e a responsabilidade penal no uso da criptografia em encontrada no parágrafo único do Art. 21. O projeto induz a compreensão de que a encriptação de comunicações por meios técnicos que não houvesse recebido, previamente, o aval da ANATEL acarretaria no comprometimento da boa-fé sobre o uso.

Limitações à liberdade de encriptar seriam pouco práticas. Atingiriam ainda mais os usuários finais da rede, afinal, agentes maliciosos facilmente obteriam acesso

72 BRASIL. Câmara dos Deputados. **CPI das Escutas Clandestinas mantém relatório original.** Agência Câmara Notícias, maio de 2019. Disponível em https://www.camara.leg.br/noticias/128754-cpi-das-escutas-clandestinas-mantem-relatorio-original/. Acesso em 29 de abril de 2020.

73 Information Technology and Innovation Foundation - **Protecting the Freedom to Encrypt.** U.S. Capitol Visitor Center, 28 de junho de 2018 Disponível em https://www.youtube.com/watch?v=JR7TsE81qCQ&feature=emb_title. Acesso em 10 de junho de 2020.

a técnicas clandestinas de encriptação e de decriptação de sistemas vulneráveis. Caso o poder regulador ultrapasse o nível de recomendações observado nas normas da ICP-Brasil, haveria uma fragilização ao cenário nacional de variadas formas: se nivelados por cima os padrões e algoritmos de encriptação, seria possível que outros serviços com menos capacidade criptográfica e econômica fossem prejudicados devido ao desafio de implementar ou adaptar seu modelo de negócio às exigências, afetando o potencial de inovação tecnológica; se nivelados por baixo, com padrões menos avançados, a segurança da informação veria seu progresso anulado em troca da possibilidade de acesso.

Havendo regulações prévias ao uso de técnicas de encriptação de dados e comunicações, surgiria um cenário de políticas restritivas de direitos típicas de países antidemocráticos[74], ou mesmo um retorno à regulação prévia observada em meados do século 20, realidade mais característica de tensões geopolíticas de exceção e menos condizente com desafios técnicos e investigativos domésticos atuais.

5.3 _ A subversão do devido processo legal contra a criptografia

Sucessivas foram - e são - as tentativas de afastar a intermediação judicial em processos penais pautados em relações de Internet. O arcabouço normativo brasileiro, entretanto, conta com robusta disciplina que reafirma a importância do princípio do devido processo legal. A intermediação necessária de uma ordem judicial simboliza, nacional e internacionalmente[75], o devido processo tanto enquanto princípio processual fundamental, como enquanto requisito básico para a garantia de outras liberdades constitucionais, dando legitimidade de uma ação estatal e respeitando o princípio da legalidade[76].

As garantias constitucionais ao devido processo legal foram referenciadas suficientemente no Marco Civil da Internet, representadas, por exemplo, pela necessidade de ordem judicial para guarda e acesso à registros de conexão, aplicação, conteúdo de comunicações (Art. 7, II e III; Art. 10, §§1º e 2º; Art. 15, §1º), bem como na regra básica da responsabilidade civil de provedores de aplicação (Art. 19). A Lei de Interceptações

74 Como nos casos do Paquistão, Iran e Turquia. Mais em KAYE, David. **Encryption and Anonimity follow-up report.** Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, junho de 2018. Disponível em https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acesso em 05 de maio de 2020.

75 Organização dos Estados Americanos - Convenção Americana de Direitos Humanos. **Pacto de São José da Costa Rica.** 1969. Disponível em http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm. Acesso em 01 de maio de 2020.

76 CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pelegrini; DINAMARCO, Cândido Rangel. **Teoria Geral do Processo.** São Paulo: Malheiros Editores, 2006. pág 88.

igualmente reafirma, em seu art. 3, §3º, a necessidade do crivo judicial na suspensão da garantia ao sigilo das comunicações. Sobretudo, as disposições valorizam o direito à privacidade e à liberdade de expressão em um ecossistema de telecomunicações e Internet – os quais podem carregar protocolos e arquiteturas que dão margem à violação de direitos. Sendo assim, o critério judicial teria o poder de ponderar, caso a caso, se o interesse público estaria acima do interesse do indivíduo cuja privacidade poderia ser suspensa - o que não significa validar qualquer espécie de enfraquecimento da criptografia ponta a ponta.

Além de outras conhecidas tentativas[77] de relativizar ou criar exceções à mediação de uma autorização judicial para o acesso direto a dados e comunicações, mais uma proposta é encontrada no PL nº 9.808/2018. A proposição procura modificar o Marco Civil da Internet para, entre outras disposições, acrescentar os parágrafos 5º e 6º ao Art. 10 da Lei. No primeiro deles, dispõe que

> § 5º - Encontrando-se o agente em situação flagrante de crimes definidos em lei como hediondo, de tráfico de drogas ou terrorismo, *poderá o delegado de polícia acessar, independente de autorização judicial, os dados de registro e conteúdos de comunicação privada de dispositivo móvel, quando necessário à investigação e/ou à interrupção da ação delitiva* (grifo nosso).

Há uma subversão da regra de autorização judicial enquanto elemento legitimador da quebra do sigilo e, portanto, violação à construção legislativa protetiva da privacidade. Rompe, portanto, o equilíbrio da relação entre o setor de provedores de aplicação, usuário e Estado, dando margem a novas camadas de riscos à segurança e abuso de autoridade. Essas são precisamente algumas das situações que a criptografia procura coibir.

Ainda que diga respeito a comunicações telefônicas, episódio notável na história das interceptações ilegais no Brasil ficou conhecido como o Caso Escher. No mês de maio de 1999, linhas telefônicas de cooperativas do Movimento Sem Terra (MST) foram grampeadas por 49 dias, sob requisição de um oficial da Polícia Militar do Estado do Paraná e sob autorização judicial não fundamentada e sem oitiva do Ministério Público,

77 Ver, por exemplo, o Projeto de Lei nº 5074/2016, da Câmara dos Deputados (propõe que o delegado de polícia ou o Ministério Público possa requerer diretamente aos provedores de conexão e aplicação dados relativos a suspeitos de cometer crimes pela Internet). Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1452538&filename=PL+5074/2016. Acesso em 09 de maio de 2020.

contrariando o procedimento constitucional e da Lei de Interceptações. A Corte Interamericana de Direitos Humanos (CIDH) da Organização dos Estados Americanos (OEA) condenou o Brasil pelas interceptações ilegais de trabalhadores rurais[78].

A perseguição de movimentos sociais dissidentes torna notável o viés político do episódio e faz romper a rede de confiança entre cidadãos e governo: se há transgressão relativa à interceptação telefônica ilegal, possivelmente haveria transgressão em relação ao acesso às comunicações eletrônicas encriptadas. E mais: se, mesmo respeitando a regra do devido processo legal, já se abre larga margem para a existência de ordens judiciais infundadas, o que dirá caso a própria ordem judicial não seja exigida. Ou seja, o juízo sobre a necessidade recairá sobre quem não foi legitimado ou não tem a fé pública para tal, gerando grandes chances de arbitrariedades.

A inclinação das forças investigativas a uma expansão de culturas de vigilância e o encurtamento da distância entre as autoridades policiais e as comunicações da população são cada vez mais nítidos.[79] Importante relacionar com práticas abusivas de acesso a conteúdos se valendo da coerção física e moral para desbloqueio de celulares. O acesso a informações armazenadas em celulares por meio de batidas policiais[80] – de forma invisível à justiça, pois ocorridas em sua maioria em regiões periféricas – afastada a necessidade constitucional de mandado judicial, pode aprofundar violências estruturais e já institucionalizadas pelo Estado, como o racismo.

Assim, muito embora projetos de lei como o PL nº 9.808/2018 exijam "situação flagrante de crimes definidos em lei como hediondo, de tráfico de drogas ou terrorismo" para o acesso às informações do suspeito sem autorização judicial, a possível arbitrariedade na atuação das autoridades faz com que o dispositivo se torne mais um instruento de perpetuação de desigualdades sociais[81]. Ainda, o agir discricionário do Estado nas

78 Organização dos Estados Americanos - Côrte Interamericana de Direitos Humanos. **Caso Escher e outros vs. Brasil.** Sentença de 6 de julho de 2009. Disponível em http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em 01 de maio de 2019.

79 Ver GRAMPOLÂNDIA. A república da escuta. Disponível em: https://grampo.org/. Acesso em: maio de 2020.

80 Levantamento bastante interessante sobre como os Tribunais de Justiça vêm encarando a legalidade da prova obtida por autoridades policiais através do acesso a dados armazenados em celular pode ser encontrado em FRAGOSO, Nathalie; LUCIANO, Maria. ***Sigilo de pés descalços: avaliação judicial do acesso a celulares por policiais em abordagens e flagrantes***. InternetLab, junho de 2019. Disonível em https://www.internetlab.org.br/pt/privacidade-e-vigilancia/sigilo-de-pes-descalcos-avaliacao-judicial-do-acesso-a-celulares-por-policiais-em-abordagens-e-flagrantes/. Acesso em 01 de maio de 2020.

81 A própria figura do tráfico de drogas presente no PL já traz uma grande carga problemática diante do histórico do encarceramento seletivo no Brasil. Ver, por exemplo, MARTINS, Helena. **Lei de drogas tem impulsionado encarceramento no Brasil.** Agência Brasil, junho de 2018. Disponível em https://agenciabrasil.ebc.com.br/geral/noticia/2018-06/lei-de-drogas-tem-impulsionado-encarceramento-no-brasil. Acesso em 09 de junho de 2020. Caso a lógica seja aplicada ao acesso a informações encriptadas armazenadas, não surpreenderia que a mesma vítima da seletividade penal, ou seja, o jovem negro, seria a principal atingida pelo Projeto de Lei em questão

investigações termina por ameaçar outro direito processual penal importante: o de não produzir provas contra si mesmo.

O entendimento sobre a ilegalidade da interceptação de comunicações e dados telefônicos sem ordem judicial encontra amplo respaldo a nível internacional. Interessante notar precedente do Canadá: no caso R. v. TELUS Communications Co. (2013) foi assentado que a legislação sobre interceptação telefônica se aplicaria às mensagens de texto (SMS), pois seriam comunicações eletrônicas privadas e, portanto, exigiriam autorização judicial para serem acessadas. Nos Estados Unidos, no caso Timothy Ivory Carpenter v. United States, foi julgado, por maioria, que acessar dados de telefone celular que registrem histórico de localizações físicas sem mandado judicial violaria a 4ª Emenda Constitucional (relativa à proteção contra buscas e apreensões arbitrárias), por revelarem alto grau de detalhamento de informações sobre a pessoa. Por fim, no México, a Suprema Corte de Justiça da Nação entendeu que todas as formas existentes de comunicação devem seguir a regra da inviolabilidade, ou seja, o acesso a quaisquer espécies de dados, sejam texto, áudio, imagem ou vídeo, deve se ancorar na autorização judicial, sob pena de ilegalidade[82].

São diferentes camadas de situações que dizem respeito ao acesso a comunicações e elementos que constróem a mesma racionalidade: a valorização do princípio da inviolabilidade do sigilo dos dados e comunicações por meio do devido processo legal. Em casos de acesso a dados criptografados, não seria modificada a chave de leitura: o resultado do julgamento sobre a relevância dos conteúdos requeridos, no âmbito de uma investigação criminal, apenas é facultado à autoridade judicial. As relações havidas por meios digitais não se diferenciam de outros ambientes de interação social no que diz respeito às diretrizes de garantia aos direitos constitucionaish. Uma possível distinção poderia gerar ruídos ou conflitos desnecessários no âmbito do direito penal e processual brasileiro.[83]

82 SUPREMO TRIBUNAL FEDERAL. **Interceptação de dados telefônicos sem mandado judicial.** Pesquisa de Jurisprudência Internacional, fevereiro de 2019. Disponível em http://www.stf.jus.br/arquivo/cms/jurisprudenciaBoletim/anexo/Pesquisa19Interceptaodedadostelefnicossemmandadojudicialpdf.pdf. Acesso em 01 de maio de 2020.

83 O Comitê Gestor da Internet (CGI.br) recomenda que, em relação ao ambiente legal e normativo relativo à Internet no Brasil, seja preservado "o espírito da Lei 12.965/2014, assegurando os direitos e garantias constitucionais aí inseridas, sobretudo a liberdade da expressão, a inviolabilidade da intimidade e da vida privada, a inviolabilidade e o sigilo do fluxo de suas comunicações pela Internet e de suas comunicações armazenadas, salvo por ordem judicial em estrita observância ao devido processo legal nos termos da Constituição Federal, sob o risco de aumentarem as possibilidades de vazamento, abuso e uso político de dados de terceiros." Mais detalhes em COMITÊ GESTOR DA INTERNET. **Resolução CGI.br/RES/2015/013.** Disponível em https://www.cgi.br/resolucoes/documento/2015/013. Acesso em 01 de maio de 2020.

5.4 _ Monitoramento ativo e riscos ao regime de responsabilidade civil

Longo debate já foi travado no Brasil sobre quais seriam as regras mais benéficas ao funcionamento da rede para os casos de responsabilização civil dos provedores de aplicação[84]. Vários eixos de análise foram levados em consideração, entre eles: a necessidade de resposta diligente à vítima de um eventual dano; a teoria do risco inerente à atividade prestada pelos provedores; os impactos à inovação tecnológica e a segurança jurídica das empresas; bem como a liberdade de expressão do usuário e a necessidade de se evitar mecanismos de censura prévia. Duas teorias se bifurcam, respectivamente, a partir do seguinte elemento: se diante da desobediência a uma mera notificação extrajudicial de retirada de conteúdo, por parte do usuário, seria gerada responsabilidade civil ao provedor – ou se apenas a desobediência a uma ordem judicial poderia implicar na responsabilização.

A tese afirmada e reafirmada no Marco Civil da Internet, especialmente no Art. 19, valoriza a segunda linha interpretativa, ou seja, a importância da mediação judicial para que seja gerada obrigação de retirada de conteúdo, preservando a liberdade de expressão e evitando a censura. Essa não é uma especificidade brasileira. As melhores práticas aplicadas globalmente sobre responsabilidade civil de provedores se assemelham – e têm como referência – à regra do MCI[85]. Atualmente, a aplicação da tese é respaldada pelo Superior Tribunal de Justiça[86].

Para o ex-Relator Especial da Organização das Nações Unidas (ONU) para a promoção e a proteção do direito à liberdade de opinião e expressão, Frank La Rue, o debate sobre responsabilização de intermediários está intrinsecamente relacionado ao exercício da liberdade de expressão. Chama a atenção para os aspectos positivos de legislações de países como Brasil, onde a possibilidade de responsabilização apenas é gerada após apreciação do pedido pelo Poder Judiciário[87]. O atual relator, David Kaye,

84 TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. **Responsabilidade civil de provedores na rede: da aplicação do Marco Civil da Internet pelo Tribunal Superior de Justiça.** Revista IBERC, v.1, n. 1, 2019. Págs 17-21.

85 Ver os Princípios de Manilla. Disponível em https://www.manilaprinciples.org/pt-br. Acesso em 01 de maio de 2020.

86 A tese é respaldada pelo STJ: "A jurisprudência do STF, em harmonia com o art. 19, §1º, da Lei 12.965 (Marco Civil da Internet), entende necessária a notificação judicial ao provedor de conteúdo ou de hospedagem para retirada do material apontado como infringente, com a indicação clara e específica da URL; Não se pode impor ao provedor de internet que monitore o conteúdo produzido pelos usuários da rede, de modo a impedir, ou censurar previamente, a divulgação de futuras manifestações ofensivas contra determinado indivíduo." Mais em SUPERIOR TRIBUNAL DE JUSTIÇA, 3ª Turma, REsp 1.568.935 - RJ, Relator Ministro Ricardo Villas Bôas Cueva, julgado em 05 de abril de 2016.

87 DE LA RUE, Frank. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.** Assembléia Geral das Nações Unidas, maio de 2011. Disponível em https://

vai além e afirma que governos não devem se valer de empresas de Internet e redes sociais enquanto seus representantes para restringir a liberdade de expressão,[88] representação esta que pode ser compreendida como programas e políticas de monitoramento das publicações e comunicações. Em paralelo, declaração conjunta de entidades como a própria Relatoria da ONU, a Organização dos Estados Americanos (OEA), a Organização para a Segurança e Cooperação na Europa (OSCE) e a Comissão Africana para os Direitos Humanos e dos Povos, alerta para os desafios postos à liberdade de expressão nos próximos dez anos, afirmando, entre outros pontos, que o controle privado sobre o discurso deve ser afastado como forma de respeitar os direitos humanos e a moderação transparente de conteúdos. Ao mesmo tempo, recomenda que os Estados se abstenham de impor restrições ao uso da criptografia[89].

Mesmo assim, é possível identificar propostas legislativas que avançam em busca da expansão da vigilância sobre as comunicações. O PL nº 2.418/2019 propõe alterar o Marco Civil da Internet para "criar obrigação de monitoramento de atividades terroristas e crimes hediondos a provedores de aplicações de Internet e dá outras providências". Propõe acrescentar o Art. 21-A, que assim dispõe:

> "Art. 21-A. Os provedores de aplicações deverão monitorar ativamente publicações de seus usuários que impliquem atos preparatórios ou ameaças de crimes hediondos ou de terrorismo, nos termos da Lei nº 13.260/2016.
>
> § 1º. As publicações mencionadas no caput deverão ser repassadas às autoridades competentes, na forma do regulamento. § 2º As obrigações estabelecidas nesse artigo somente se aplicam a provedores de aplicações que possuam mais de 10.000 (dez mil) assinantes ou usuários.
>
> § 3º. Na impossibilidade eventual e justificada de cumprimento do disposto no caput, os provedores de aplicações deverão permitir a instalação

www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf; Acesso em 01 de maio de 2020.

88 TIWARI, Soymya. **Social media platforms cannot act as government's proxy for censorship: UN Special Rapporteur David Kaye.** Medianama, novembro de 2019. Disponível em https://www.medianama.com/2019/11/223-united-nations-online-hate-speech/. Acesso em 01 de maio de 2020.

89 Organization of American States; United Nations Special Rapporteur on Freedom of Opinion and Expression; Organization for Security and Co-operation in Europe; African Comission on Human and People's Rights. **Joint Declaration: Challenges to Freedom of Expression in the Next Decade**. Julho de 2019. Disponivel em https://www.osce.org/files/f/documents/9/c/425282.pdf. Acesso em 09 de junho de 2020.

de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para o mesmo fim."

Ainda que o PL não trate de suspender a criptografia nas comunicações, mas de monitorar publicações, parece ser mais uma peça no mosaico legislativo que avança em forma de propostas de acesso a conteúdos produzidos pelos usuários. Além disso, guarda semelhança com articulações internacionais que afetam a criptografia através de políticas de monitoramento em aplicações e que vêm causando reações em redes de especialistas e ativistas.

Em 2018, o governo indiano propôs alterações às regras de responsabilização de intermediários no país. Caso aplicada a nova norma para as Information Technology (Intermediary Guidelines) Rules, provedores deveriam passar a monitorar ativamente o conteúdo das comunicações de seus usuários e possibilitar que seja rastreada a origem de um dado conteúdo quando determinado pela agência governamental responsável[90]. A medida vai ao encontro de queixas do governo indiano sobre a crescente concentração de poder por parte das grandes empresas de tecnologia, as quais teriam limitada responsabilidade legal[91], e sobre a necessidade de perseguir responsáveis por atividades ilegais na rede[92], em narrativa muito parecida com as existentes no Brasil no âmbito do combate às fake news.[93]

Claramente, as regras não poderiam ser aplicadas em plataformas com criptografia ponta a ponta, já que não permitem o acesso ao conteúdo a não ser pelos emissores e receptores da comunicação. Isso significaria que as plataformas teriam que enfraquecer a criptografia para possibilitar o monitoramento. As reações às mudanças sobre regras de responsabilidade foram diversas e alertam que para obedecer às regras os provedores teriam que introduzir backdoors ou desativar os recursos de criptografia

90 SINGH, Manish. **Over two dozen encryption experts call on India to rethink changes to its intermediary liability rules.** TechCrunch, janeiro de 2020. Dísponível em https://techcrunch.com/2020/01/09/over-two-dozen-encryption-experts-call-on-india-to-rethink-changes-to-its-intermediary-liability-rules/. Acesso em 10 de junho de 2020.

91 MOHANTY, Bedavyasa. **The encryption debate in India.** Carnegie Endowment for International Peace, maio de 2019. Disponível em https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213. Acesso em 10 de junho de 2020.

92 Uma orientação direta pode ser acessada nesse tweet do Ministry of Electronics and Information Technology da Índia, disponível em https://twitter.com/GoI_MeitY/status/1081505492059467776. Acesso em 04 de maio de 2020.

93 Coalizão Direitos na Rede. **PL das fake news: identificação e criminalização em massa dos usuários.** Junho de 2020. Disponível em https://direitosnarede.org.br/2020/06/20/pl-das-fake-news-relatorio-estabelece-identificacao-e-criminalizacao-em-massa-de-usuarios.html. Acesso em 10 de junho de 2020.

ponta a ponta, comprometendo a segurança digital de forma drástica e, consequentemente, a privacidade e a liberdade de expressão[94].

As duas propostas - a brasileira e a indiana - apontam para a mesma resposta política: a necessidade de monitoramento ativo das atividades dos usuários como meio supostamente necessário ao auxílio das investigações e consequente acesso. É, portanto, necessário contextualizá-las geopoliticamente enquanto movimentos governamentais correlacionados que sinalizam formas de pressão contra as regras de responsabilidade de intermediários e que resvalam diretamente nos direitos fundamentais dos usuários.

Não são exatamente novas as sugestões de enfraquecer a criptografia para possibilitar o mapeamento do compartilhamento de conteúdos ilegais. Várias foram as manifestações que questionavam a criptografia de aplicativos de mensagem enquanto suposta responsável pela impunidade dos responsáveis pelos mecanismos de desinformação, sobretudo nas últimas eleições presidenciais, em 2018[95]. Caso essa leitura política seja cruzada com as motivações do PL nº 2.418/2019, já suficientemente problemático, a realidade da proposta legislativa indiana encontraria terreno fértil em território nacional.

Enquanto a proposta indiana aponta para a responsabilização civil em caso de descumprimento do dever de monitoramento, a brasileira aposta em outro artifício: em caso de descumprimento ou na impossibilidade de monitorar as publicações, geraria a permissão para que o Estado interfira diretamente na arquitetura do serviço. Além de se relacionar com alternativas problemáticas e que desafiam a resiliência da criptografia, já exploradas nesse estudo, viola o princípio da proporcionalidade[96]. Ou seja, a solução é inadequada: não garante a eficácia de que todas as comunicações suspeitas serão filtradas (outras redes e outros serviços de comunicação e divulgação de conteúdos podem ser buscados por agentes maliciosos); é desnecessária: há outros mecanismos de combate mais efetivos e que não atingem/ameaçam a criptografia e vulnerabilizam o

94 Access Now e outros: **International coalition of organizations and experts call on the Ministry of Electronics and Information Technology to withdraw the draft amendments proposed to the Information Technology (Intermediary Guidelines) Rules**. Março de 2019. Disponível em https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_-_Indias_Intermediary_Guidelines_-_March_15_2019.pdf. Acesso em 05 de abril de 2020.

95 Mais recentemente, a criptografia vem recebendo críticas por, supostamente, facilitar campanhas de desinformação veiculadas pelo WhatsApp. Exemplos dessa abordagem podem ser encontradas em TARDÁGUILA, Cristina. **Criptografia ou capacidade de viralização? O WhatsApp precisa enxergar esse paradoxo.** Revista Piauí, dezembro de 2018. Disponível em https://piaui.folha.uol.com.br/lupa/2018/12/03/artigo-epoca-criptografia-whatsapp/; e SILVA, Victor Hugo. **WhatsApp diz que não vai quebrar a criptografia para monitorar fake news.** Tecnoblog, agosto de 2018. Disponível em https://tecnoblog.net/257255/whatsapp-criptografia-fake-news/. Acessos em 10 de junho de 2020.

96 ÁVILA, Humberto. **Teoria dos Princípios: da definição à aplicação dos princípios jurídicos. S**ão Paulo: Editora Malheiros, 4ª Ed, Pág 116-125

usuário final; e é desproporcional: busca resultados através do monitoramento excessivo, fragilizando direitos individuais.

Abrir as portas para legislações que obriguem o monitoramento de publicações em redes sociais abre caminho político que poderá desaguar em leis que podem obrigar ao monitoramento ativo das comunicações. Consequentemente, essa vigilância privada ou, alternativamente, pública, como aponta o PL nº 2.418/2019, acende o alerta para futuras restrições à criptografia, como percebido nas novas regras de responsabilidade de intermediários no caso indiano.

Enfim, a regra brasileira de responsabilidade de intermediários afasta a necessidade de monitoramento das comunicações e publicações por parte dos provedores. Esse possível cenário, se tornado factível, geraria um ônus tecnológico às empresas – que deveriam implementar ainda mais algoritmos de moderação de conteúdos e empregar ainda maior quantidade de capital humano na tarefa – além de implicar no risco de uma censura prévia por receio de responsabilização posterior. Paralelamente, o usuário veria sua liberdade de expressão ainda mais afetada, seu acesso a informações reduzido e suas comunicações vigiadas em tempo integral.

5.5 _ De volta à imputabilidade da rede

A interpretação mais progressista sobre responsabilidade de intermediários de Internet significa que, a princípio, não há relação entre os provedores com os atos ilegais praticados por seus usuários. Como demonstrado, um cenário diferente desse abriria espaço para mecanismos de censura e diminuição do potencial de liberdade de expressão nas redes. Se a regra é sedimentada pelo Marco Civil da Internet, também não haveria, em matéria penal, responsabilidade das plataformas por crimes praticados por seus usuários. Como assentado no princípio da inimputabilidade da rede, o combate a ilícitos na Internet deve atingir os responsáveis finais e não os meios de acesso e transporte, como estabelecido nos Princípios para o Uso e Governança da Internet do Comitê Gestor da Internet (CGI.br)[97].

Apesar disso, as narrativas encontradas em meio aos desafios enfrentados pelas agências de investigação flertam com a ideia de uma responsabilidade penal para as plataformas. As retóricas que sugerem mecanismos de responsabilização buscam aproximar, mais e mais, o sigilo proporcionado pela criptografia e o avanço de crimes hediondos. Nesse caminho, plataformas convocariam, literalmente, o criminoso ao uso de seus serviços, pois seriam construídas com a finalidade de impedir a interceptação ou o

97 COMITÊ GESTOR DA INTERNET. **Princípios para a Governança e Uso da Internet.** Comitê Gestor da Internet (CGI.br), junho de 2009. Disponível em https://cryptoid.com.br/banco-de-noticias/declaracao-de-principios-do-cgi-br-para-a-governanca-e-uso-da-internet-completa-10-anos/. Acesso em 04 de abril de 2020.

acesso legal[98]. Partindo desse imaginário[99], caso os intermediários estejam ameaçados judicialmente, seria mais fácil restringir a criptografia ponta a ponta.

Encontra eco no Brasil a construção narrativa que ameaça plataformas de comunicação criptografadas ao aproximá-las da cooperação com o terrorismo. A redação do PL 11.007/2018, por exemplo, é abrangente nas condutas que elenca e, se assimiladas com os discursos das agências de investigação que propõe tornar intermediários responsáveis, abre espaço para a efetivação da criminalização. No tipo penal que pretende ser criado em seu Art. 5º, caput, lê-se:

> Art. 5. Receber, financiar, prover, oferecer, obter, guardar, manter em depósito, solicitar, investir, de qualquer modo, direta ou indiretamente, recursos, ativos, bens, direitos, valores ou serviços de qualquer natureza, para o planejamento, a preparação ou a execução dos crimes previstos nesta Lei.

Diante da generalização de condutas possíveis que poderiam significar a caracterização do crime do artigo, uma das leituras possíveis seria:

> Art. 5. (...) *oferecer* (...) *de qualquer modo, direta ou indiretamente, recursos* (...) *ou serviços de qualquer natureza, para o planejamento, a preparação ou a execução dos crimes previstos nesta Lei.* (grifo nosso)

Esse raciocínio passa, justamente, pela argumentação das agências em questão. Se, para a Polícia Federal, a "cogitação, o preparo, a execução, a consumação e o exaurimento de um crime" são percorridos, atualmente, por meios de aplicativos de comunicação[100] e, para a Agência Brasileira de Inteligência (ABIn), a radicalização de células

98 William Barr, atual General Attorney do Departamento de Justiça dos Estados unidos, satiriza provedores de aplicação que usam criptografia em seus serviços: "Ei, nós podemos te deixar invisível para para as agências de aplicação da lei" (tradução livre). Disponível em https://www.youtube.com/watch?v=WZEcjHXG-1w, em 7 minutos e 6 segundos. Acesso em 04 de abril de 2020.

99 RAMIRO, André. **A Construção de imaginários nas narrativas governamentais sobre criptografia.** Derechos Digitales. Disponível em https://www.derechosdigitales.org/wp-content/uploads/A-Construcao-de-Imaginarios-nas-Narrativas-Governamentais-sobre-Criptografia-final.pdf. Acesso em 20 de junho de 2020.

100 LEAL, Felipe. Polícia Federal do Brasil. **Audiência Pública sobre as Ação Direta de Inconstitucionalidade nº 5.527 e Ação de Descumprimento de Preceito Fundamental nº 403**. Supremo Tribunal Federal. Brasília, 2017. Disponível em http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 1504 de abril de 2020.

terroristas está estritamente ligada ao uso de aplicativos de mensagem criptografada[101], então a confusão entre serviços de criptografia e atividades terroristas seria possível na interpretação contextual do PL 11.007. As plataformas poderiam, portanto, ser indiciadas criminalmente.

A atual Lei Antiterrorismo foi amplamente criticada pela abrangência das condutas passíveis de responsabilidade penal – o que levou grupos de defesa dos direitos humanos a se manifestarem veementemente contrários à Lei e em defesa de movimentos sociais que poderiam ser afetados, como já apontado nesse estudo. E a reforma da lei apresentada pelo PL 11.007 também dá margem a um poder bastante arbitrário e genérico para a justiça:

> Art. 6. Praticar qualquer ato de colaboração com as atividades ou as finalidades de uma organização, grupo ou elemento terrorista, ou para a prática de qualquer dos delitos previstos nesta lei
>
> (...)
>
> § 1º Consideram-se atos de colaboração (...) a prestação de serviços tecnológicos, e qualquer outra forma equivalente de cooperação ou ajuda às atividades das organizações ou grupos terroristas, grupos ou pessoas a que se refere o parágrafo anterior

Qual seria o limite de interpretação sobre o ato de cooperar ou ajudar? Excetuam-se os casos de aplicativos disponíveis ao grande público no mercado? A grosso modo, na utilização de aplicações de mensageria por um grupo de indivíduos associados ao terrorismo, há boas chances de que a mediação seja feita, inevitavelmente, por por um dos inúmeros serviços tecnológicos disponível publicamente. Além disso, caso a empresa responsável pela plataforma não disponibilize a chave criptográfica ou qualquer outra solução de acesso, a ideia de colaboração poderia ganhar força: ou colabora com a investigação policial a partir de uma criptografia mais fraca, ou com a atividade terrorista. Uma encruzilhada legal produzida por uma construção narrativa e legislativa desproporcional.

---

101 A, Thiago; O, Augusto; S, Allan. **O processo de radicalização e a ameaça terrorista no contexto brasileiro a partir da Operação Hashtag**. Revista Brasileira de Inteligência: Abin, n. 12, dezembro de 2017. Pág. 13. Disponível em http://www.abin.gov.br/conteudo/uploads/2018/05/RBI12-Artigo1-O-PROCESSO-DE-RADICALIZA%C3%87%C3%83O-E-A-AMEA%C3%87A-TERRORISTA-NO-CONTEXTO-BRASILEIRO-A-PARTIR-DA-OPERA%C3%87%C3%83O-HASHTAG.pdf. Acesso em 04 de abril de 2020.

Os parágrafos 2º e 3º do mesmo Art. 6º qualificam o crime de colaboração:

> § 2º. As penas previstas neste artigo aumentam-se da metade se:
>
> (...)
>
> II – a conduta envolver a difusão de serviços ou conteúdos acessíveis ao público através de meios de comunicação, internet, por meio de serviços de comunicação eletrônicas ou mediante o uso de tecnologias de informação.
>
> § 3º. Se o crime for praticado na modalidade culposa:
>
> Pena – reclusão, de três a seis anos.

A referida "conduta", no caso, é a própria natureza da existência das plataformas. Pelo simples fato de terem o propósito comunicativo, base tecnológica e serem difusas na rede, provedores de aplicação estariam no escopo da proposta. O inciso II gera uma rede de responsabilidade ampla, sobretudo àqueles que não dão possibilidade de acesso aos dados e comunicações para as autoridades policiais.

Igualmente chama atenção a modalidade culposa de colaboração. Quer dizer, por agirem com imprudência, negligência ou imperícia, terminariam por concorrer para um resultado. Partindo da definição de terrorismo trazida pelo PL 11.007, as atividades criminosas requerem o elemento vontade. Se não houver intenção ou alinhamento ideológico, em quais tipos de situações, por faltar com o dever de cuidado e incorrer em um resultado não desejado, estaria-se colaborando com atividades ou finalidades de uma organização terrorista? Esse cuidado significaria prever um backdoor? A falta de cuidado significaria uma criptografia ponta a ponta? Em termos práticos, é possível afirmar que a norma, prevendo colaboração culposa para prestadores de serviços de tecnologia, criaria uma abrangência suficiente para envolver qualquer cidadão ou aplicação que oferecesse serviços tecnológicos eventualmente usados por grupos terroristas. Ainda que sem intenção ou vontade, poderiam ser responsáveis criminalmente por colaboração com o terrorismo.

Esses são alguns dos cenários provocados pela diluição da regra de responsabilidade dos intermediários. Invariavelmente, ao ampliar as chances de que as plataformas

respondam por crimes praticados por seus usuários, não só são provocadas inseguranças, mas também essas injustiças são repassadas ao usuário final, que será afetado pelas mudanças que porventura as plataformas serão levadas a realizar em seus serviços.

5.6 _ "Alternativas" ao backdoor e as suas problemáticas

_ Lawful hacking

Apesar da atual desobrigação para os provedores de aplicação em fornecer chaves de decriptação, percebe-se uma movimentação no âmbito do legislativo brasileiro - e de outros países - em torno de projetos de lei que buscam alcançar o acesso a conteúdos criptografados por supostos novos meios. Assim, cada vez mais, agentes governamentais encontram técnicas de invasão para ter acesso ao conteúdo de comunicações sigilosas - o que se convencionou chamar de "lawful hacking" ou "government hacking" (hacking estatal ou amparado pela lei).

A técnica é defendida por diversos especialistas uma vez que, ao invés de forçar as empresas a criarem backdoors ou fornecerem chaves criptográficas, a aplicação da lei poderia explorar as brechas de segurança existentes[102], sem comprometer, em tese, a segurança alcançada pela criptografia. O desenvolvimento legislativo de uma estrutura legal que possibilite o lawful hacking no Brasil é visto por muitos como uma alternativa viável para que autoridades policiais continuem aptas a investigar crimes graves[103].

É o caso do PL nº 9.808/2018, que propõe a inclusão de dois parágrafos no artigo 10º do Marco Civil da Internet. O primeiro deles propõe que:

> "em se tratando de dados criptografados, poderá o delegado de polícia requisitar, diretamente aos provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação, o fornecimento de chave criptográfica que permita o acesso aos dados e conteúdos de comunicação privada de dispositivo móvel, sem prejuízo do desenvolvimento e emprego, pelas polícias judiciárias, de técnicas e ferramentas tecno-

102 COHEN, Justin. **Lawful Hacking: A Temporary Solution to the "Going Dark" Challenge.** Fevereiro 2019. Disponível em https://journals.library.columbia.edu/index.php/stlr/blog/view/109

103 ANTONIALLI, Dennys; ABREU Jacqueline. **E quando o policial vira hacker?** Internetlab, julho de 2017. Disponível em https://www.internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/ Acesso em 30 de abril de 2020.

lógicas que atinjam esse fim específico, incluindo a utilização de dispositivos que possibilitem o acesso a conteúdo anterior à criptografia por meio de aplicativos, sistemas ou outras ferramentas."

Embora o lawful hacking pareça uma solução viável, autorizar e incentivar autoridades a explorar vulnerabilidades em sistemas digitais pode gerar efeitos indesejados. Um maior uso governamental de exploração de inseguranças aumentaria o risco de vazamento dessas vulnerabilidades e o risco da sua exploração por terceiros. Também é preciso considerar os danos colaterais que algumas alternativas eventualmente trariam para toda a comunidade de usuários e, também, a realidade geopolítica na qual o Marco Civil da Internet surge[104].

Por falta de instrumento legal específico para legitimar o lawful hacking, salvaguardas apropriadas devem ser perseguidas para garantir que as invasões sejam feitas apenas quando absolutamente necessário. Além de uma autorização judicial, o governo deve garantir que a evidência buscada não possa ser alcançada por outro meio menos invasivo. Em novembro de 2019, a organização não-governamental Privacy International chamou a atenção para a proposta legislativa de government hacking da Suécia[105]. De acordo com a entidade, o projeto é problemático por diversos motivos, dentre eles: o escopo de aplicação da proposta sueca é injustificadamente amplo e a autorização judicial não é necessária em alguns casos.

Além disso, é preciso apontar também o dilema ético que o lawful hacking cria um para o governo. Para que a tática funcione, autoridades não poderiam informar às empresas sobre as vulnerabilidades descobertas, sob risco de ter sua invasão frustrada:Seria preciso manter a rede e os usuários inseguros e expostos à exploração por outros agentes maliciosos.

A questão se torna ainda mais delicada uma vez que o uso destas brechas não se restringe ao combate de crimes, mas também à perseguição de defensores de direitos humanos. Foi revelado, por exemplo, que ativistas marroquinos foram perseguidos por meio de um software produzido por um grupo israelense especializado em explorar vulnerabilidades de sistemas operacionais de smartphones[106]. De acordo com uma

104 GREENWALD, Glenn; MACASKILL, Ewen. **NSA Prism program taps into user data of Apple, Google and others**. The Guardian 7, no. 6, 2013, p. 1-43.; BERGHEL, Hal. Through the PRISM darkly. Computer 46, no. 7, 2013, p. 86-90.

105 Privacy International. **New Swedish draft proposal for government hacking powers violates human rights standards.** Novembro, 2019 https://privacyinternational.org/news-analysis/3291/new-swedish-draft-proposal-government-hacking-powers-violates-human-rights Acesso em 30 de abril de 2020.

106 Amnesty International. **Moroccan human rights defenders targeted using malicious NSO Israeli spyware.** Outubro, 2019. Disponível em https://amnesty.org/en/latest/news/2019/10/moroccan-human-rights-defen-

série de entidades comprometidas com a defesa dos direitos humanos no ambiente digital, a prática vem se popularizando e gerando grandes margens de lucro por meio de produtos chamados de "software de interceptação legal" e produzidos por empresas privadas com sedes no Reino Unido e Alemanha (FinFisher), Itália (Hacking Team) e Israel (NSO Group)[107].

Em 2018, pesquisadores descobriram que um desses softwares foi utilizado em 45 países[108], incluindo o Brasil. A Polícia Federal, no entanto, negou o uso e explicou que o software tinha sido utilizado "apenas em um teste de conceito", procedimento em que o produto é testado nos aparelhos de policiais.[109] Não se sabe, contudo, se foi o "teste de conceito" o responsável pelo rastro captado pelos pesquisadores no Brasil.

Percebe-se que a falta de transparência quanto ao funcionamento e adoção dessas ferramentas por governos e autoridades não é exclusividade do panorama brasileiro. É importante ressaltar que, em relatório publicado no mês de junho de 2019, o relator especial das Nações Unidas sobre liberdade de opinião e expressão, David Kaye, pediu a moratória imediata da venda, transferência e uso da tecnologia de vigilância até que estruturas regulatórias compatíveis com os direitos humanos sejam construídas[110].

A realidade trazida pela criptografia não justifica que novas rotinas de invasão de dispositivos eletrônicos sejam praticadas por agentes estatais de forma simplista. Um debate técnico e jurídico responsável deve preceder a exploração de vulnerabilidades em sistemas de segurança pela polícia, tanto em função dos riscos aos direitos fundamentais dos usuários - gerados por possíveis arbitrariedades desses agentes - quanto devido às potenciais novas brechas de segurança que poderiam ser causadas de forma estrutural à infraestrutura da rede. O projeto de lei, portanto, passa por cima da construção de entendimento jurídico sobre a criptografia e sugere novas legitimidades, de forma descuidada, às agências de investigação.

---

ders-targeted-using-malicious-nso-israeli-spyware/ Acesso em 30 de abril de 2020

107 GALPERIN, Eva; COHN, Cindy. **Private Companies, Government Surveillance Software and Human Rights.** Electronic Frontier Foundation. Outubro 2019. Disponível em https://www.eff.org/deeplinks/2019/10/applying-human-rights-framework-sale-government-surveillance-software

108 MARCZAK, Bill; SCOTT-RAILTON, John; MCKUNE, Sarah; RAZZAK, Bahr Abdul; DEIBERT, Ron. **HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.** The Citizen Lab. Setembro 2018. Disponível em https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/. Acesso em 10 de junho de 2020.

109 Época. **A chegada ao Brasil do Pegasus, estrela do submundo da espionagem**. Julho 2019. Disponível em https://epoca.globo.com/brasil/a-chegada-ao-brasil-do-pegasus-estrela-do-submundo-da-espionagem-23815778

110 KAYE, David. **UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools.** Junho 2018. Disponívvel em https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

_ Chave fantasma como solução?

Além da contratação de empresas especializadas em quebra de criptografia[111], uma outra alternativa que governos ao redor do mundo vem buscando é a adoção de soluções ghost key ou ghost user.

Surgida no Reino Unido, a proposta exigiria que os provedores de serviços com criptografia ponta a ponta "minassem" os seus mecanismos de forma a permitir que funcionários do governo obtivessem acesso ao conteúdo criptografado. De acordo com a proposta, o Estado - no caso do Reino Unido, o Government Communications Headquarters - poderia exigir que os serviços de mensagens criptografadas adicionassem uma nova chave, de propriedade da polícia, às conversas de um suspeito sem informar aos participantes da conversa; em seguida, uma atualização do software seria oferecida ao usuário alvo de investigação para que este passe a usar uma versão acessível à polícia, que poderia se infiltrar, por exemplo, em um grupo ou chamada sem ser notada. Seria uma forma de adicionar mais uma "ponta" na criptografia "ponta a ponta".

Apesar daqueles que afirmam que a proposta de chaves fantasmas não "tocaria" na criptografia[112], isto não é verdade. Os processos de distribuição, autenticação e as próprias chaves são partes integrais de todo o sistema criptográfico. Alterações no software seriam necessárias a fim de suprimir, por exemplo, as notificações e todas as indicações da interface do usuário que normalmente distinguem os chats individuais dos chats em grupo (por exemplo, um chat entre duas pessoas e um ghost user deve parecer um chat único). Ou seja, um dos pilares da criptografia, a autenticidade, seria comprometido. Além disso, os fornecedores precisariam modificar o software de seus serviços - possivelmente através de uma atualização do aplicativo - para criar um mecanismo em que fosse possível a ativação destas funções em dispositivos específicos em resposta às demandas do governo.

A eficácia da medida sequer é garantida. Se as pessoas que usam aplicativos de criptografia ponta a ponta para coordenar atividades criminosas souberem que os provedores de serviços foram forçados a implementar uma solução de ghost key, será relativamente fácil, para eles, simplesmente recusar a atualização da versão do aplicativo ou migrar para outra plataforma. Para especialistas como Nate Cardozo[113], da Electronic

111 FORBES. **FBI contrata hackers para quebrar criptografia de empresas de tecnologia.** 21 de abril de 2016. Disponível em https://forbes.com.br/negocios/2016/04/fbi-contrata-hackers-para-quebrar-criptografia-de-empresas-de-tecnologia/ Acesso em 8 de maio de 2020

112 LEVY, Ian; ROBINSON, Crispin. **Principles for a more informed excepcional access debate.** Lawfare, novembro de 2018. Disponível em: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate. Acesso em 09 de maio de 2020.

113 CARDOZO, Nate. **Give Up the Ghost: A Backdoor by Another Name.** Just Security. Janeiro, 2019. Disponível em: https://www.justsecurity.org/62114/give-ghost-backdoor/

Frontier Foundation, a proposta apresentaria as mesmas ameaças que a implementação de uma backdoor põe à segurança e privacidade dos usuários de uma forma geral[114].

6 _ Dois retratos da criptografia em juízo <

As decisões judiciais que determinaram os bloqueios de aplicativos de mensageria em todo território nacional - e às vezes com reverberações em países vizinhos[115] - geraram uma série de repercussões ao redor do país. Claros exemplos disso são as ações que tramitam atualmente no Supremo Tribunal Federal relacionadas à matéria.

_ Ação Direta de Inconstitucionalidade (ADI) nº 5527

Iniciada pelo Partido da República (PR), agora Partido Liberal (PL), a Ação Direta de Inconstitucionalidade (ADI) nº 5527 trata do requerimento de suspensão imediata e, ao final, a declaração de inconstitucionalidade dos incisos III e IV do art. 12 da Lei n. 12.965/14 (Marco Civil da Internet) - que prevê sanções como "suspensão" e "proibição" das atividades mencionadas no art. 11[116] - como também do art. 10, §2º, sobre a disponibilização de conteúdo de mensagens mediante ordem judicial.

Em sua petição inicial, o PR discute o caráter de aplicações de Internet, optando por classificar os aplicativos de troca de mensagens pela Internet como comunicação telefônica. Assim, a quebra de sigilo somente pode ser autorizada por ordem judicial para fins de persecução penal. O Partido busca defender também que os aplicativos de troca de mensagem são um serviço prestado por particular, mas que deve receber proteção do Estado em razão do interesse da sociedade na continuidade de suas atividades.

---

114 É importante salientar que a solução *ghost key* é diferente daquilo que é definido como "infiltração policial virtual". Enquanto a primeira se dá mediante a alterações no sistema criptográfico e acontece por meio da presença oculta de uma terceira pessoa, a segunda se configura a partir das ações de um agente infiltrado que assume uma nova identidade e se insere em um determinado grupo de forma visível.

115 CAPUTO. Victor. **Bloqueio no Brasil tira WhatsApp do ar na Argentina e no Chile.** Revista Exame, dezembro de 2015. Disponivel em https://exame.abril.com.br/tecnologia/bloqueio-no-brasil-tira-whatsapp-do-ar-na-argentina-e-chile/. Acesso em 05 de abril de 2020.

116 "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros."

Dessa forma, os proponentes se utilizam ainda de dois artigos relacionados à livre comunicação no ordenamento jurídico brasileiro: o art. 5º, IX, da CF que afirma: "É livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença" e o artigo 13 da Convenção Americana de Direitos Humanos, que diz que o direito à liberdade de pensamento e de expressão inclui a liberdade de "procurar, receber e difundir informações e ideias de qualquer natureza, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer meio de sua escolha". Assim, para eles, o art. 12, III e IV, do Marco Civil da Internet seria inconstitucional pois fere a CF ao tornar possível a suspensão temporária e a proibição dos serviços de aplicativos de troca de mensagens.

A ADI chega a argumentar que as penalidades previstas no art. 12, III e IV, do MCI, ao atingirem pessoas estranhas aos fatos apenados, violariam os princípios da intranscendência e da individualização da pena. Além disso, utilizam-se também de argumentos econômicos ao citar a migração em massa de usuários do WhatsApp ao Telegram. De acordo com o PR, a perda ou a conquista de usuários foi fator externo à dinâmica concorrencial do mercado. Sendo assim, a demanda passou a ser ditada pela atuação do Poder Judiciário, ferindo a livre concorrência entre os atores econômicos e o disposto no artigo 170 da Constituição Federal (princípios para a garantia da ordem econômica no Brasil).

Os incisos III e IV do Art. 12 do Marco Civil da Internet, no entanto, não representam uma norma inconstitucional. Nesse caso, importante destacar o entendimento da AGU[117] e do Senado Federal[118], respaldada pela posição já previamente publicizada[119] pelo Comitê Gestor da Internet no Brasil (CGI.br): o art. 12 prevê sanções para descumprimento de normas de proteção de registros, dados pessoais e comunicações privadas e não de casos de descumprimento de ordem judicial. Não se observa qualquer empecilho na previsão abstrata das sanções de suspensão e proibição de atividades nos casos determinados na letra da lei uma vez que estes estão relacionados aos direitos à privacidade, à proteção dos dados pessoais, ao sigilo das comunicações privadas e dos registros de usuários. Caso essas previsões sejam declaradas inconstitucionais, haveria o risco de interesses econômicos de provedores prevalecerem em relação a direitos fundamentais de usuários.

---

117 Advocacia Geral da União. **AÇÃO DIRETA DE INCONSTITUCIONALIDADE N° 5527**. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=560715474#23%20-%20Peti%E7%E3o%20de%20apresenta%E7%E3o%20de%20manifesta%E7%E3o%20(32914/2016)%20-%20Peti%E7%E3o%20de%20apresenta%E7%E3o%20de%20manifesta%E7%E3o. Acesso em 09 de maio 2020.

118 Senado Federal. **OFÍCIO N° 061/2016-PRESID/ADVOSF (Processo SF nº 00200.007278/2016-27)**. Brasília, 6 de junho de 2016. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=556977343#21%20-%20Presta%E7%E3o%20de%20informa%E7%F5es%20(30041/2016)%20-%20Presta%E7%E3o%20de%20informa%E7%F5es. Acesso em 09 de maio de 2020.

119 Ibidem.

Durante a ação, ainda foi observado que a fundamentação legal utilizada para embasar os bloqueios seria o art. 461, §1.º, do Código de Processo Civil de 1973[120]. Dessa forma, uma vez que o Marco Civil não impede outras decisões judiciais que se baseiam em outros diplomas normativos para o bloqueio ou suspensão de aplicativos e sites, a declaração de inconstitucionalidade desse dispositivo na ADI 5527 seria desnecessária e ineficaz.

Em seu voto, a Ministra Rosa Weber, relatora da ADI 5527, buscou seguir o entendimento já consolidado pelos diversos órgãos e especialistas na temática ao atentar que os incisos do art. 12 não representam uma norma inconstitucional já que protegem direitos fundamentais e preveem sanções para descumprimento de normas de proteção de registros, dados pessoais e comunicações privadas - e para casos de descumprimento de ordem judicial. A Ministra declarou improcedente o pedido de declaração de nulidade parcial do art. 12, III e IV, da Lei nº 12.965/2014, por compreender que "a sua hipótese de incidência não abrange o conteúdo que dele se pretende excluir", nesse caso a possibilidade de bloqueios em caso de descumprimento judicial. Assim, as sanções do referido artigo só poderiam ser aplicadas em casos de vazamento de dados pessoais e de conteúdo de comunicações privadas, atos que afrontam direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações e dos registros.

A Ministra ratifica ainda a interpretação conforme do art. 10, §2º, reafirmando que dados de conteúdo de comunicações só podem ser disponibilizados através de ordem judicial e lembra que o Estado não pode compelir aplicativos a oferecerem serviços de forma menos segura com o pretexto de usar vulnerabilidades para acessar dados em investigações criminais. Para ela, o "trade-off não se dá entre segurança pública e privacidade" já que além de violar frontalmente a proteção da liberdade de expressão e a proteção do sigilo das informações, medidas de acesso excepcional como backdoors teriam como consequência "tornar as tecnologias de comunicação menos seguras para todos os seus usuários". Weber considera ainda que alternativas de acesso excepcional são "potencialmente inócuas", já que aqueles que se utilizam de aplicações criptografadas com o intuito de cometer crimes escapariam das forças policiais por meio da simples migração para outros aplicativos fora do alcance das autoridades. O voto da ministra já representa um divisor de águas em termos de entendimento dos tribunais sobre o bloqueio de aplicativos e sobre a importância da criptografia.

Em seu voto, a Ministra aproveita para defender que tornar ilegal ou limitar a criptografia representaria uma "involução" e destaca instrumentos internacionais que

120 Instituto Beta para Democracia e Internet-IBIDEM e e Laboratório de Pesquisa Direito Privado e Internet-LAPIN. **Supremo Tribunal Federal ADI 5527 Amicus Curiae.** Disponível em https://drive.google.com/file/d/0B5yj-Tu1DTF9wUDhyTllsdTZqTVk/view. Acesso em 10 de junho de 2020.

corroboram com essa visão. Utiliza, por exemplo, as considerações de Zeid Raad Al Hussein, do Alto-Comissariado das Nações Unidas para os Direitos Humanos entre 2014 e 2018, elencando os riscos do enfraquecimento da criptografia em relação à segurança de ativistas de direitos humanos, jornalistas, denunciantes e dissidentes políticos. Além dos direitos humanos, a ministra recorre a instrumentos internacionais econômicos como é o caso das Diretrizes para Política de Criptografia adotada pela Organização para a Cooperação e Desenvolvimento Econômico - OCDE em 1997. O documento reafirma que "o direito fundamental dos indivíduos à privacidade, incluindo o sigilo das comunicações e a proteção dos dados pessoais, deve ser respeitado nas políticas nacionais de criptografia e na implementação e uso de métodos criptográficos."

_ Ação de Descumprimento de Preceito Fundamental (ADPF) nº 403

Proposta pelo Partido Popular Socialista (PPS) logo após a execução do segundo bloqueio judicial do aplicativo Whatsapp no Brasil, em maio de 2016, a ação de Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403 requereu a suspensão dos efeitos da decisão da Vara Criminal de Lagarto, no Estado de Sergipe. O juízo penalizou a empresa Facebook Brasil por não atender ordens de interceptação. Entretanto, o bloqueio foi suspenso 24h após a sua determinação pelo Tribunal de Justiça de Sergipe.

Em julho de 2016, após a propositura da ADPF, mais uma decisão judicial determinou o bloqueio do aplicativo. Mais uma vez, em razão do não cumprimento de uma decisão judicial de interceptação da 2ª Vara Criminal de Duque de Caxias. Assim, o PPS requereu, no âmbito da ADPF já proposta, a suspensão do novo bloqueio. O pedido foi analisado de forma liminar pelo ministro Ricardo Lewandowski, que concluiu pela desproporcionalidade da medida e afirmou que, na presente situação, o bloqueio do aplicativo parecia violar a garantia de liberdade de expressão e a legislação sobre o tema.

Em relação à ADPF, a Procuradoria-Geral da República (PGR) e o Ministério da Justiça e Cidadania possuem visões similares. A PGR defende a extinção da ação sem resolução de mérito pelo fato da decisão objeto já ter sido suspensa e por não ter sido indicado ato do poder público lesivo a preceito fundamental, enquanto o Ministério da Justiça e Cidadania segue o entendimento e acredita que o bloqueio em nada violou a liberdade de comunicação dos cidadãos e cidadãs brasileiras. Para o órgão, a decisão de bloqueio foi tida, ainda, como proporcional dada a sua finalidade.

Em relação às cinco instituições que propuseram pedidos de ingresso nas ações como amicus curiae, todas concordam com o argumento de que há violação à liberdade de comunicação (inc. IX, art. 5º da CF) quando há bloqueios ao aplicativo WhatsApp

e pedem a procedência do pedido da ADPF para suspender os bloqueios. Entretanto, percebe-se particularidades em relação à fundamentação legal, pedidos e temas abordados pelas instituições.

A Federação das Associações das Empresas de Tecnologia da Informação (ASSESPRO) adotou uma interpretação mais extensiva que a do PPS. Ela observou que o bloqueio também poderia ser considerado inconstitucional em razão do impedimento ao livre acesso à informação (inc. XIV do art. 5º) e proibição à continuidade do próprio objeto social do WhatsApp (art. 170 da Constituição Federal, parágrafo único, inc. IV). A Associação Brasileira de Defesa do Consumidor - PROTESTE, por sua vez, requereu o impedimento de qualquer decisão judicial que possa vir a ser lesiva aos preceitos fundamentais de liberdade de expressão, comunicação, intimidade e comunicação privada.

Além de tratar da questão dos bloqueios, a Frente Parlamentar pela Internet Livre e Sem Limite requereu a declaração de interpretação do art. 10, caput e §2º do MCI conforme a Constituição Federal. Desse modo, seria inconstitucional a interpretação de um dever irrestrito de guarda de registros de acesso, de conexão e de conteúdos de comunicações. A Frente afirmou que esse dever violaria direitos fundamentais como o direito à intimidade, à vida privada, ao sigilo das comunicações, e ao princípio da proporcionalidade. Assim, como o Instituto de Tecnologia e Sociedade (ITS), a frente também defendeu que, caso seja entendida como necessária a guarda contínua e irrestrita dos dados e conteúdo das comunicações privadas, o STF deveria definir expressamente o art. 12, incisos III e IV, do Marco Civil, como não hábil para fundamentar sanções a empresas que descumpram ordem judicial de apresentação de dados, registros ou comunicações privadas.

Dessa maneira, como já defendido em momento anterior no presente estudo, acredita-se que o artigo 12 do Marco Civil da Internet deveria ser utilizado como forma de compelir que os aplicativos e sites respeitem o direito à privacidade dos usuários e não em favor do cerceamento de preceitos fundamentais de liberdade de expressão e comunicação. Chega-se à conclusão, portanto, de que qualquer interpretação relacionada à imposição de bloqueios por meio de fundamentação legal com base no art. 12 deve ser declarada inconstitucional.

O relator da ADPF 403, o Ministro Edson Fachin, fez considerações importantes em seu voto não só para a segurança da criptografia no Brasil, mas também para a proteção dos direitos digitais no país. Por meio de afirmações como “os direitos que as pessoas têm offline devem também devem ser protegidos online” e “direitos digitais são direitos fundamentais”, o Ministro deixa clara a sua posição e sai em defesa do direito

à privacidade e à liberdade de expressão nas comunicações. Para ele, estes direitos são fundamentais e condições para o pleno exercício do direito de acesso à internet.

Assim como Rosa Weber, Edson Fachin enfatiza que chega a ser contraditório que em nome da segurança pública busque-se uma Internet menos segura. Ainda afirma que a segurança da rede é um dever do Estado e que este não pode tomar medidas que busquem enfraquecer a criptografia e trazer insegurança a milhares de usuários sem a certeza dos ganhos obtidos em outras áreas. Ele lembra ainda que medidas que restringem direitos fundamentais, como é o caso dos bloqueios, devem ser estritamente "necessárias", mais do que "úteis", "razoáveis" ou "desejáveis", como já sinalizado anteriormente pela Corte Europeia de Direitos Humanos[121] (The Sunday Times v. United Kingdom, julgamento de 26 de abril de 1979, par. 59).

Finalmente, Edson Fachin é assertivo ao afirmar que backdoors apenas para "good guys" não é algo real. Assim, conclui o seu voto optando pelo afastamento de "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." Além de endereçar mecanismos de acesso excepcional, também afirma que a proibição da utilização de criptografia ponta a ponta seria inconstitucional, uma vez que uma ordem como essa impactaria desproporcionalmente aqueles mais vulneráveis. Conclui, por fim, 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".

7 _ Conclusão <

Os níveis de confiabilidade e segurança sobre as redes digitais, envolvendo a proteção de informações sensíveis ao Estado, a cibersegurança, o pleno desenvolvimento econômico, bem como o ecossistema de direitos fundamentais na rede - incluindo suas repercussões sobre a integridade física dos indivíduos - dependem, de forma central, da criptografia. Redes seguras e confiáveis afastam as vulnerabilidades e riscos provocados por terceiros maliciosos, assim como previnem indivíduos e organizações da vigilância abusiva operada muitas vezes pelos próprios Estados.

121 Corte Europeia de Direitos Humanos. **The Sunday Times vs. The United Kingdom.** Julgamento de 26 de abril de 1979, pág 59. Disponível em https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57584%22]}. Acesso em 10 de junho de 2020.

Ainda assim, problematizações à criptografia têm surgido no cenário nacional. Esses processos de construção política assumem ora a forma de proposições legislativas, ora surgem como decisões judiciais que causam repercussões, de forma estrutural, à rede e aos direitos a ela conexos. E, de forma mais contínua, as propostas de enfraquecimento da criptografia habitam as investidas narrativas das forças de investigação, as quais repercutem no parlamento e no judiciário.

Se - com algum otimismo - o debate na esfera judicial no Brasil parece apontar para a consolidação da interpretação sobre a garantia à liberdade de comunicação e expressão, ao sigilo e à privacidade no Marco Civil da Internet e na Constituição Federal, bem como para o entendimento sobre a ilegalidade do bloqueio de aplicações em razão do uso de criptografia ponta a ponta, as articulações entre forças de investigação e o legislativo parecem sugerir um cenário desafiador em termos de liberdade criptográfica. Ao partirem das habituais narrativas dos setores de investigação, os Projetos de Lei elencados neste estudo ilustram as diferentes formas de abordar o tema: buscando mudanças sobre as regras de responsabilidade sobre intermediários, impondo obrigações de monitoramento contínuo dos usuários ou inviabilizando, através da criminalização ou de imposições técnicas e legais, a operação de recursos criptográficos. No entanto, apontam para o mesmo caminho: a facilidade em operacionalizar rotinas de vigilância; da mesma forma, caem na mesma contradição: em nome da ampliação dos poderes de investigação, fragilizam redes de segurança e garantia de direitos ainda mais amplas.

Sendo assim, antes do debate em torno da criptografia significar uma incompatibilidade entre privacidade e segurança - como parte das retóricas a favor de backdoors buscam fazer parecer -, estamos diante de um conflito entre “segurança e segurança”. Tomadores de decisão, parlamentares e representações dos setores de investigação devem agregar conhecimentos, em colaboração e os demais setores de interesse da sociedade, sobre o que está em jogo no âmbito das políticas de criptografia. Isso significa dimensionar os riscos em gerar vulnerabilidades propositais em sistemas de segurança. Como restou demonstrado ao longo do estudo, a existência de vulnerabilidades digitais para fins de investigação não parece apontar para ganhos ao interesse público, mas para o retrocesso ao desenvolvimento tecnológico e aos direitos constitucionais.

Espera-se que este estudo sirva de bússola à análise e escrutínio dos presentes Projetos de Lei e dos futuros, bem como das políticas públicas operadas pelas agências de investigação e das decisões judiciais que potencialmente afetem a criptografia e a segurança da rede. Espera-se, também, que seja instrumento de suporte a parlamentares, às organizações da sociedade civil e à comunidade científica que atuem no interesse da segurança e do respeito aos direitos na rede. E, por fim, que seja mais uma peça

na constante construção de entendimento político, jurídico e técnico sobre a crescente importância da criptografia em uma sociedade cada vez mais conectada.

ANEXO 01

Opiniões de especialistas

Veridiana Alimonti

_ *criptografia e estruturas de vigilância*

"Não precisamos ir muito atrás na história do Brasil e de outros países da América Latina para verificar como estruturas de vigilância das comunicações são utilizadas sem atender a parâmetros adequados de legalidade, necessidade e proporcionalidade, muitas vezes a serviço da perseguição e da preservação de poderes instituídos à revelia de garantias fundamentais de direitos humanos.

Caso revelado no início desse ano na Colômbia ilustra muito bem essa realidade e reacende escândalo de uma década atrás. Em janeiro desse, ano uma investigação jornalística revelou que unidades do exército colombiano realizaram escutas ilegais nos telefones e e-mails de políticos opositores, juízes, jornalistas e organizações da sociedade civil. Algo semelhante já havia sido denunciado em 2009, durante a administração de Álvaro Uribe, o que levou a mudanças nos altos níveis das forças de inteligência do país e a uma reforma legal. Em 2015 vieram a público documentos evidenciando negociações e compra do software espião da empresa Hacking Team por diferentes governos ao redor do mundo. Conforme aponta relatório da organização Derechos Digitales, seu uso na América Latina ocorreu em violação às legislações locais e a padrões internacionais de direitos humanos. No México, oito das dez autoridades que compraram o software não estavam autorizadas a exercer atividades de vigilância. No Equador, a tecnologia foi usada para vigiar um opositor do governo de Rafael Correa. O Brasil está entre os países que negociaram com a empresa e os documentos vazados mostram operações de mais de 60 mil euros. Ainda em 2009, o Estado brasileiro foi condenado pela Corte Interamericana de Direitos Humanos no caso "Escher e outros vs Brasil" pela realização de interceptações telefônicas contra cooperativas de trabalhadores rurais ligadas ao MST sem a devida observância de parâmetros legais e garantias da Convenção Americana. Escutas ilegais também fizeram parte das medidas de vigilância que a empresa de mineração Vale S.A. adotou contra seus funcionários, jornalistas, movimentos sociais, entre outros, denunciada em 2013.

Esses são apenas alguns exemplos que demonstram como a vigilância nas comunicações se associa a um cenário de vulnerabilidade de ativistas, dissidentes, jornalistas, lideranças comunitárias e movimentos sociais. Um cenário em que as violações à privacidade podem significar, e com frequência implicam, um risco real à integridade física e à vida dessas pessoas. Em 2019, o Brasil foi o 4º país em que mais defensores de direitos humanos foram mortos,de acordo com o relatório da organização Front Line Defenders. O país também apresenta número considerável de mortes de jornalistas na última década, conforme levantamento da Unesco. Ainda que esses casos não estejam necessariamente relacionados à "quebra" de criptografia, eles ressal-

tam a importância da privacidade e segurança nas comunicações, preocupação central quando se trata do uso e desenvolvimento de métodos criptográficos. Na verdade, como já ressaltou o Relator Especial para a Liberdade de Expressão da ONU, David Kaye, a criptografia cria uma zona de privacidade que serve como porta de entrada ao exercício de uma série de outros direitos humanos. Investidas contra a criptografia fragilizam direitos políticos, a capacidade de se organizar, de obter, compartilhar, debater e guardar informações de forma segura e íntegra. Essa segurança é fundamental também para o próprio Estado, por exemplo, para conter esforços de espionagem de outros países, ou mesmo para o trabalho de autoridades de investigação.

Iniciativas voltadas a comprometer a criptografia, como a proposta que ficou conhecida como Ghost no Reino Unido ou a lei australiana de acesso e assistência, fragilizam de forma massiva a segurança e a integridade das comunicações, entre outras razões: (i) por intensificar o risco de falha nos sistemas de comunicação que todos usam ao ampliar a superfície vulnerável a ataques; e (ii) pela dificuldade de manter vulnerabilidades criadas (como backdoors) sob controle e fora do alcance de atores maliciosos. Mais do que isso, tais iniciativas partem do pressuposto equivocado que opõe privacidade e criptografia, de um lado, e segurança pública, de outro. Os atributos da criptografia protegem a informação de acessos não autorizados, permitem identificar com segurança a sua origem e garantem que ela não seja modificada sem autorização. A criptografia previne fraudes e roubo de dados. Nas transações financeiras online, ela é fundamental para que informações bancárias sejam transmitidas de forma segura. Em relação a dados armazenados, a criptografia mitiga os danos de vazamentos de dados se aqueles que acessaram o banco não puderem entender seu conteúdo. Ou evita que terceiros tenham acesso a fotos, mensagens, etc, armazenados em um celular roubado, por exemplo, se o dispositivo for criptografado. Investidas contra a criptografia colocam em risco não só a privacidade individual, mas podem causar impactos coletivos, inclusive e destacadamente à segurança de todas e todos."

Veridiana Alimonti. Analista de Políticas Públicas para América Latina, Electronic Frontier Foundation (EFF)

Riana Pfefferkorn

_ *criptografia, vulnerabilidades e efeitos extraterritoriais*

"Como a Internet é transnacional, se um país impõe restrições à criptografia, isso não impede que os residentes desse país tenham acesso a aplicativos de software que fornecem criptografia forte. Eles poderão baixar programas da Internet e carregar esses

aplicativos nos seus telefones (mesmo que as lojas oficiais de aplicativos para Android e iPhone não permitam os aplicativos naquele país). Pesquisas realizadas em 2016 mostram que os fornecedores de software criptografado estão baseados em muitos países do mundo e essas entidades não terão o dever de parar de oferecer seus serviços em seu país de origem, mesmo que outro país imponha restrições. Portanto, as pessoas ainda poderão acessar a criptografia "ilegal", mesmo que seu país imponha restrições; elas apenas terão que trabalhar mais para fazer isso. Isso significa que a pessoa comum não vai se incomodar, então a pessoa comum terá uma segurança pior do que aqueles que se esforçam - o que incluirá os próprios criminosos motivados a atacar essas pessoas comuns.

Outro impacto internacional diz respeito a existência de um efeito dominó. Se um país aprovar leis que restringem a criptografia, ele inspirará outros países a fazerem o mesmo. Estamos vendo isso agora com o Five Eyes: depois que o Reino Unido aprovou a "Snooper's Charter" em 2016, a Austrália aprovou uma Lei modelada na do Reino Unido em 2018 e inspirou autoridades nos EUA a continuar pressionando por uma restrição legislativa à criptografia - que poderemos ter como resultado o Projeto de Lei do EARN IT Act. Quando as chamadas democracias, como a Austrália ou a Índia, normalizam a noção de restringir a capacidade das pessoas de proteger seus dados e se comunicar em particular, torna-se mais politicamente viável que outros países sigam o exemplo."

Riana Pfefferkon. Diretora Associada para Vigilância e Cibersegurança, CIS - Stanford Center for Internet and Society

Jacqueline Abreu

_ *criptografia e grupos vulneráveis*

"Investidas contra a criptografia aparecem sempre que uma técnica nova de criptografia dificulta a realização de atividades de monitoramento e vigilância do Estado que foram normalizadas como se existisse o direito de serem feitas simplesmente porque antes não existia obstáculo fático para que assim o fizessem. Autoridades governamentais acostumaram-se a ser capazes de interceptar comunicações telefônicas; quando migramos em massa para comunicações eletrônicas - dessa vez protegidas com criptografia - implicaram.

As narrativas de combate ao terrorismo, ao crime organizado e às redes de pedofilia para fragilização de técnicas de criptografia estão intimamente ligadas à viabilização de estruturas de vigilância em massa. A razão é simples: o comprometimento do nível de segurança de comunicações à distância pela fragilização da criptografia, sob qualquer narrativa que seja, facilita estruturas de vigilância em massa. Comprometer

criptografia significa facilitar a vigilância; iniciativas contrárias institucionalizadas aplicadas em escala, advindas de esforços políticos, implicariam portanto a facilitação de estruturas de vigilância em massa.

Para discutir quem mais seria sofreria com isso, é preciso ter clareza de que a criptografia que dificulta que a polícia, legitimamente encarregada de conduzir investigações, tenha acesso a comunicações de criminosos é a mesma que garante que ativistas possam fazer denúncias de violações de direitos em países autoritários sem risco de perseguição, que jornalistas possam se comunicar com fontes para receber denúncias de corrupção de forma segura, que protege eu e você de criminosos que querem obter informações privilegiadas nossas para aplicar golpes, praticar extorsões, nos ameaçar, etc. Todos nos tornaríamos mais vulneráveis em certa medida, portanto - mas o peso seria sentido principalmente por aqueles que estão em posições sensíveis pela natureza do seu trabalho, pela sua visibilidade política ou mesmo por fazerem parte de grupos sociais e étnicos que já são mais visados como alvos de políticas de segurança ou de preconceito.

Proteger a criptografia é, nesse sentido, também proteger a segurança dessas pessoas e o exercício de suas liberdades. Do contrário, haveria impacto portanto tanto na privacidade como na liberdade de comunicação e expressão. Em países com instituições democráticas mais frágeis e, no caso do Brasil, com jurisprudência mais fraca quanto a esses direitos e frágil arquitetura de supervisão e responsabilização de autoridades contra abusos, as perspectivas são ainda mais preocupantes."

Jacqueline Abreu. Advogada, doutoranda em Direito na USP e mestra em Direito pela Universidade da Califórnia, Berkeley (EUA).

Fernanda Domingos

_ *criptografia e aplicação da lei*

"Do ponto de vista das forças da Lei é possível dizer sim que a visão com relação à criptografia se alterou.

Num primeiro momento houve um ímpeto de proibição em relação à criptografia ponto-a-ponto, por exemplo, tecnologia desconhecida dos operadores do direito leigos em tecnologia, afinal uma tecnologia estava sendo empregada para obstruir o cumprimento da lei.

A partir do momento em que se tomou consciência a respeito do papel fundamental que a criptografia representa para garantir não apenas a privacidade das pesso-

as, mas também a sua segurança, num mundo que opera virtualmente em praticamente todas as áreas, passou-se a entender que não era possível mais viver sem a criptografia e que proibi-la não era uma opção.

Porém, as forças da lei ainda se deparam com o grande desafio de investigar e obter provas que estão protegidas por essa mesma tecnologia. a implantação de backdoors não deve ser uma opção, pois a fragilização da criptografia não viria em proveito da sociedade. Porém, já alguns países alteram ou estudam alterar suas legislações como forma de obrigar as empresas a providenciarem uma solução para esse impasse em situações muito pontuais e sem colocar em risco a segurança geral que se entende atualmente como indispensável.

Ainda é um desafio equilibrar a privacidade e a segurança das pessoas."

Fernanda Domingos. Procuradora da República, Ministério Público Federal.

Verónica Arroyo

_ *criptografia e direitos humanos*

"A criptografia é importante para proteger informações. Quando enfraquecida ou proibida, qualquer pessoa obtém acesso fácil a essas informações, dando espaço a diversas ações maléficas. Outros interesses obscuros ou ocultos, além da vigilância, são ameaças ou ataques a certos grupos de pessoas. O acesso a certas informações torna muito mais fácil o rastreamento do comportamento e das crenças de alguém. Em governos autoritários, [tal acesso] pode ser usado para atacar e perseguir a oposição. Como uma tática de vigilância em massa, [o acesso a certas informações] pode ser usado para influenciar as pessoas. Como vimos, por meio do uso de técnicas de manipulação orientada a dados, nas últimas eleições no Brasil. Nesse caso, por meio do uso de grupos criptografados de ponta a ponta no WhatsApp. Iniciativas similares podem ser ainda mais prejudiciais caso haja pouca ou nenhuma criptografia.

As pessoas usam a internet para muitos propósitos. Um exemplo são serviços financeiros; se o serviço do banco não estiver bem criptografado, informações confidenciais, incluindo informações de identidade, podem ser facilmente roubadas. Além disso, a falta ou mesmo uma criptografia fraca podem ser especialmente prejudiciais para jornalistas, denunciantes, ativistas, advogados e para a população que vive em países onde os governos criminalizam certos comportamentos ou características, como a comunidade LGBTQ+. Vimos exemplos na América Latina sobre como isso afeta esses grupos de pessoas, por isso, no ano passado, as organizações da sociedade civil da Amé-

rica Latina elaboraram e assinaram uma carta aberta sobre criptografia, alertando para que os governos da região e as empresas não enfraqueçam ou proíbam a criptografia.

A criptografia permite o desenvolvimento de direitos humanos, principalmente dos direitos à privacidade e à liberdade de expressão. Também permite comunicações e transações confiáveis. Essa confiança é algo importante para exercer direitos políticos, como liberdade de reunião, liberdade de associação, direito de eleger e ser eleito. As pessoas precisam confiar em suas atividades e em seus pares. Por exemplo, a criptografia pode ser usada para organizar demonstrações, conduzir campanhas e tomar decisões sensíveis durante o período das eleições. Portanto, a criptografia é importante, mas se torna mais relevante em países onde governos ou poderes de fato controlam a população e limitam seus direitos; nesses contextos, a criptografia se torna uma ferramenta para exercer os direitos humanos.

[Em relação à correlação entre privacidade e segurança pública], estamos acostumados a vê-los como conceitos opostos. Um exemplo é a Lei de Inteligência da Colômbia, que proíbe a criptografia na Colômbia e é renovada a cada quatro anos desde 1993. A proibição foi justificada pelo Tribunal Constitucional, porque seu uso põe em risco a segurança pública. No entanto, um "versus" entre esses conceitos não é uma boa maneira de entender a criptografia. É verdade que a criptografia é uma boa maneira de manter as informações privadas, mas também ajuda a mantê-las seguras e evita que criminosos ou atores externos obtenham acesso a essas informações. A segurança online também é uma questão de segurança pública e, hoje em dia, a segurança digital está se tornando uma prioridade para governos, cidadãos e empresas. Portanto, acredito que ambos os conceitos [segurança e privacidade] são importantes e devem ser vistos como complementares. "

Verônica Arroyo, Associada de Políticas Públicas - América Latina, Access Now.