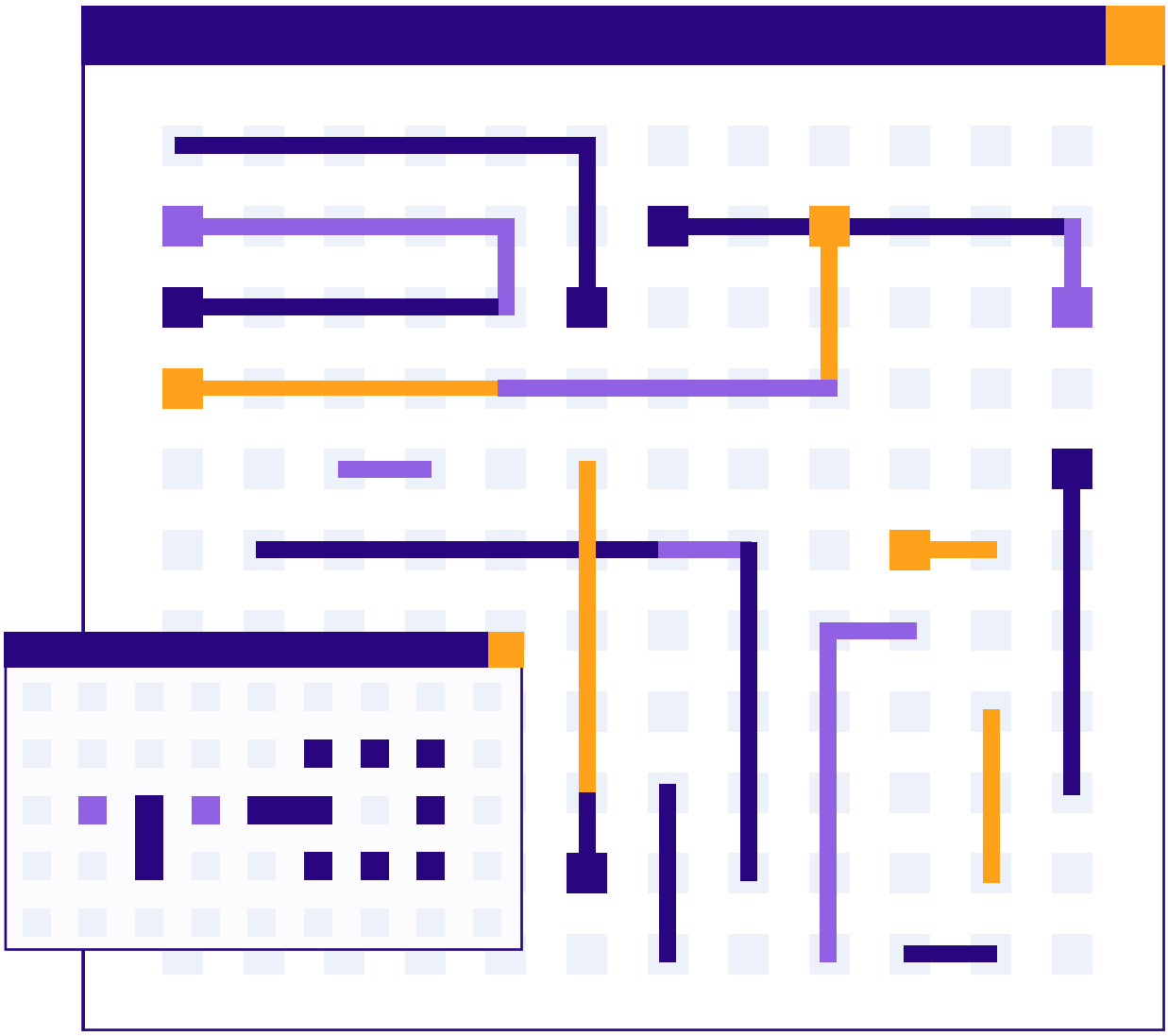
PERCEPÇÕES SOBRE CRIPTOGRAFIA E INVESTIGAÇÕES CRIMINAIS NO BRASIL

mapeamento e análise



INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

apoio:

Internet Society Capítulo Brasil

Internet Society Foundation

PERCEPÇÕES SOBRE CRIPTOGRAFIA E INVESTIGAÇÕES CRIMINAIS NO BRASIL

mapeamento e análise

Autoria

Ana Bárbara Gomes Pereira

Gustavo Ramos Rodrigues

Victor Barbieri Rodrigues Vieira

Consultoria

Lucas Caetano Pereira de Oliveira

Revisão externa

Paulo Renã da Silva Santarém

Raquel Lima Saraiva

Projeto gráfico, capa e diagramação

Felipe Duarte

Como citar em ABNT

PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: dd mmm aaaa.

Esta publicação faz parte do projeto "Privacidade é segurança: comunicando a importância da criptografia para todos", com a parceria da ISOC Brasil e financiamento da ISOC Foundation.

realização: IRIS Instituto de Referência em Internet e Sociedade

apoio: Internet Society Capítulo Brasil; Internet Society Foundation

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

DIREÇÃO

Luíza Couto Chaves Brandão

MEMBROS

Ana Bárbara Gomes / Pesquisadora

Beatriz Fernandes / Estagiária de Comunicação

Felipe Duarte / Coordenador de Comunicação

Gustavo Rodrigues / Coordenador de Políticas Públicas e Pesquisador

Juliana Roman / Pesquisadora

Lahis Kurtz / Coordenadora de Pesquisa e Pesquisadora

Leandro Soares Nunes / Pesquisador

Paloma Rocillo Rolim do Carmo / Vice-diretora e Pesquisadora

Pedro Vilela Resende Gonçalves / Co-fundador e Associado

Victor Barbieri Rodrigues Vieira / Pesquisador

SUMÁRIO

Resumo executivo

Contexto. Desde a segunda metade do século XX, o constante avanço tecnológico no campo das técnicas criptográficas, bem como as perspectivas de massificação do acesso a essas tecnologias por parte da sociedade civil representou um ponto de recorrente conflito argumentativo. Demarcada pelo que se convenciona chamar de *Crypto Wars* – ou Guerras Criptográficas – a disputa envolvendo Estado, indústria e sociedade civil em torno do direito de acesso desta às técnicas de criptografia forte e segura se estende até os dias atuais. De natureza episódica – porém perene – as Guerras Criptográficas adquirem novas dimensões no século XXI, com o exponencial aumento do acesso da sociedade civil à internet e, concomitantemente, com o desenvolvimento e uso de tecnologias investigativas cada vez mais sofisticadas.

No Brasil, a importação da narrativa estadunidense do *Going Dark* – ou "obscurecimento" – culminou também na reprodução desse conflito, materializado inicialmente nos bloqueios do aplicativo WhatsApp no país em 2015 e 2016. Os casos culminaram na ADI 5527 e ADPF 403, impetradas no Supremo Tribunal Federal, que tematizam a constitucionalidade das medidas. Em que pese a conclusão do julgamento de ambas ainda estar pendente, os votos dos relatores dessas ações indicaram o reconhecimento da criptografia como essencial à realização de direitos fundamentais, como privacidade e liberdade de expressão. Similarmente, o Superior Tribunal de Justiça já considerou, nos exames do RMS 60.531 e do RESP 1.872.695, ilícita a aplicação de sanções a provedor de aplicação que descumpre ordem de interceptação por impossibilidade técnica imposta pela criptografia.

Apesar disso, tentativas de introduzir um mecanismo de acesso excepcional na criptografia ainda ocorrem no país e não raramente se tornam objeto de discussão legislativa. O apelidado "Pacote Anticrime" do ex-Ministro da Justiça e Segurança Pública Sérgio Moro, continha previsões que ampliaram os poderes de interceptação estatal e que poderiam implicar numa fragilização da criptografia, por exemplo. Similarmente, a reforma do Código de Processo Penal trouxe novamente à tona o debate sobre a possibilidade de provedores de aplicação serem compelidos à redução da segurança de seus sistemas para realização de interceptações durante a persecução penal. Desse modo, a questão do acesso excepcional e da governança de criptografia permanece urgente e atual no país.

Metodologia. Nesse contexto, o presente estudo buscou investigar as percepções e opiniões de profissionais envolvidos com o debate público sobre o tema. Foram realizadas 45 entrevistas, das quais 43 foram consideradas válidas, com representantes dos setores governamental, empresarial, terceiro setor e comunidade científica e tecnológica. Os profissionais apresentaram diferentes formações disciplinares e trajetórias profissionais.

Os entrevistados foram selecionados por meio do método de amostragem em bola de neve, em que novos participantes são indicados pelos anteriores, criando uma rede social progressivamente expandida. Uma vez que esse método não gera uma amostragem

representativa de nenhum segmento populacional e é mais sensível a vieses de seleção, o presente estudo não deve ser entendido como uma pesquisa de opinião, mas como um mapeamento empírico e como uma análise dos principais discursos, racionalidades e crenças que permeiam as guerras criptográficas brasileiras.

Após as entrevistas, foi realizada a codificação e análise das percepções e opiniões desses profissionais em relação a quatro tópicos: i) implementação de acesso excepcional em sistemas criptográficos para acesso a dados cifrados para fins de persecução penal; ii) conhecimentos e riscos sobre potenciais alternativas para acesso das autoridades ao conteúdo cifrado sem interferência direta na criptografia; iii) o ambiente regulatório nacional referente à criptografia; e iv) os bloqueios do WhatsApp no Brasil e sua relação com o Marco Civil da Internet. Os resultados dessa análise foram apresentados na forma de reconstruções narrativas dos discursos identificados. Feito esse mapeamento, procedeu-se a uma análise das relações entre as teses identificadas e os contextos factuais com os quais se relacionam.

Resultados. Em relação ao acesso excepcional, constatou-se dois discursos principais em torno do tema. O discurso favorável à medida entende existir hoje um conflito essencial entre privacidade e segurança pública e supõe a primazia desse último valor sobre o primeiro. Ainda, entende existir no direito brasileiro um dever legal de garantir as condições para que as interceptações ocorram por parte daqueles que podem ser compelidos à sua realização nos termos da lei. Paralelamente, o discurso contrário ao acesso excepcional considera a medida desproporcionalmente danosa, pois ela atingiria todos os usuários do sistema, comprometendo sua segurança informacional e seus direitos fundamentais, além de prejudicar a confiança no ambiente digital. Além disso, questiona tanto a necessidade efetiva da medida quanto sua eficácia alegada, sugerindo que a criminalidade migrará das plataformas comprometidas.

Quanto a possíveis alternativas para o acesso a dados sem violação da criptografia, as principais alternativas citadas foram a apreensão e desbloqueio dos dispositivos das pessoas investigadas, hacking governamental desses dispositivos, análise de metadados, *client side-scanning*, inserção de um usuário fantasma e o acesso a dados armazenados em serviços de nuvem. Com relação às soluções baseadas no comprometimento da segurança do dispositivo individual, foi apontado um risco de violação dos direitos do investigado, haja vista a possibilidade de acesso a qualquer conteúdo do dispositivo, inclusive aqueles irrelevantes para a investigação. Quanto às soluções de *client-side scanning* e inserção de um usuário fantasma, a suposição de que tais soluções não interfeririam na criptografia foi objeto de questionamento e crítica. Nesse sentido, uma percepção frequente foi de que haveria um comprometimento principiológico da criptografia mesmo sem uma interferência direta no algoritmo criptográfico ou no sistema de gerenciamento de chaves.

Quanto ao ambiente regulatório relativo à criptografia no Brasil, uma percepção frequente foi de ambivalência: a criptografia seria simultaneamente valorizada e ameaçada. A

valorização adviria de normas como a Lei Geral de Proteção de Dados, o Marco Civil da Internet e o Decreto nº 8771/2016, as quais são percebidas como incentivos ao uso desse recurso pela sociedade, mesmo na ausência de referência expressa no caso das duas leis. Similarmente, os votos dos relatores das ações sobre o tema no STF e a jurisprudência do STJ foram citados como indicadores de um reconhecimento da importância da criptografia na institucionalidade brasileira. Por outro lado, o caráter inconcluso do julgamento das ações no STF e as tentativas recorrentes de introduzir acesso excepcional foram vistas como sinais de que a criptografia permanece ameaçada no país.

Nesse ponto, dois discursos distintos sobre a questão da regulação da criptografia emergiram. Um deles defende a introdução de garantias explícitas na legislação, seja por meio de uma afirmação legal expressa de que o emprego de criptografia por cidadãos e empresas é lícito, seja pela conversão dos incentivos atuais ao emprego de criptografia em um dever vinculativo aplicável a certos provedores e aplicações. Por outro lado, o segundo discurso questiona se a referência legal expressa à criptografia seria positiva, entendendo que tal abordagem contraria o ideal de neutralidade tecnológica da regulação e pode representar uma interferência indevida no avanço científico do campo da segurança da informação.

Com relação aos bloqueios do WhatsApp e sua relação com o Marco Civil da Internet, por fim, três teses foram aventadas. A primeira entende que os bloqueios foram ilegítimos, seja por considerar seu impacto desproporcional ou por avaliar que as sanções previstas no Marco Civil da Internet seriam inaplicáveis. Essa inaplicabilidade poderia se dar em razão da impossibilidade técnica de cumprimento da ordem cuja desobediência ocasionou as sanções e/ou devido à interpretação de que as sanções previstas no Marco Civil da Internet estão reservadas a casos de violação dos direitos à privacidade e à proteção de dados dos usuários.

A segunda tese, por sua vez, entendeu que os bloqueios foram legítimos, uma vez que o Marco Civil da Internet preveria a aplicação das sanções na ocorrência de descumprimento da legislação brasileira. Uma vez que as ordens judiciais se fundamentam na legislação brasileira, seu descumprimento implicaria em violação de nosso ordenamento. A terceira, por fim, entendeu que a licitude dos bloqueios independeria da redação do Marco Civil da Internet em si, pois os magistrados podem determinar medidas cautelares atípicas na ausência de uma medida legalmente prevista suficiente para o caso concreto – o chamado poder geral de cautela.

Cumpre destacar, ainda, o entendimento comum de que as causas concretas dos bloqueios foi um conflito político entre a empresa Facebook e as instituições do sistema de justiça criminal brasileiro. Desse modo, o episódio teria dimensões econômicas e políticas que extrapolariam a controvérsia jurídica específica.

Análise. Quanto à inserção de um mecanismo de acesso excepcional, não é evidente que a partir da obrigação de condução de interceptações, nas hipóteses e termos da lei, seja

possível deduzir uma aptidão de alteração na arquitetura do sistema a fim de tornar a interceptação viável. No que tange às implicações da medida, há consenso científico no campo da segurança informacional sobre a impossibilidade de garantir que a exploração do mecanismo seja realizada apenas de forma lícita. Ainda, há indícios empíricos de que regulações que enfraqueçam a criptografia causam danos econômicos. Por fim, estudos sobre o ambiente político e jurídico brasileiro têm indicado a ocorrência de processos de supressão das liberdades democráticas e uso da tecnologia para viabilização de medidas autoritárias – fenômeno por vezes designado como tecnoautoritarismo.

Quanto às alternativas ao acesso excepcional, cada uma apresenta implicações distintas. O compelimento judicial do usuário, por meio de sanções, à entrega de senha de desbloqueio do dispositivo foi recentemente considerado ilícito pelo Superior Tribunal de Justiça no julgamento do RHC nº 580.664 - RJ, com fundamento na vedação constitucional à autoincriminação, o que implica na ilicitude desse expediente. No tocante ao hacking governamental, cumpre destacar que tais práticas têm sido objeto de críticas da sociedade civil e de organismos internacionais, que notam seu potencial excessivo para o abuso e sugerem que quaisquer práticas dessa natureza somente sejam admitidas em casos excepcionais, observados requisitos de legalidade, necessidade, proporcionalidade, finalidade legítima, supervisão judicial, entre outros.

Com relação à proposta de inserção de usuário ou chave fantasma nas comunicações, sua implementação exige interferência no procedimento de distribuição de chaves, o que implica na conclusão incontroversa de que a medida representa um enfraquecimento da criptografia. Assim sendo, seus riscos são similares àqueles identificados no acesso excepcional implementado por meios mais convencionais, como a custódia de chaves.

Quanto ao *client-side scanning*, a ausência potencial de interferência direta no sistema criptográfico implica que a aferição da existência de violação da criptografia é mais controversa. Independentemente dela, contudo, cabe destacar que há necessária redução da segurança do sistema em decorrência da ampliação da superfície de ataque, o que implica na possibilidade de produção de falsos positivos por meio do comprometimento da base de dados utilizada para comparação. Ainda, a possibilidade de desvirtuamento de função do sistema representa um risco democrático que vem suscitando críticas da sociedade civil organizada.

No tocante aos bloqueios do WhatsApp e sua relação com o Marco Civil da Internet, por fim, cumpre reiterar primeiramente que a suposição de que há um dever de aptidão à realização de interceptações não apenas carece de fundamentação, como também contraria a jurisprudência supracitada do Superior Tribunal de Justiça. Quanto ao debate sobre a redação do Marco Civil da Internet, está pendente a deliberação do plenário do Supremo Tribunal Federal, porém a tese de que a aplicação das sanções estaria restrita à violações da privacidade e da proteção de dados pessoais foi acolhida pelos relatores das ações sobre o tema. No que tange ao poder geral de cautela do juiz, o reconhecimento do dano excessivo causado pelo bloqueio do aplicativo implica na ausência do requisito de proporcionalidade necessário ao exercício do poder geral de cautela.

Por essas razões, conclui-se patente que os bloqueios do WhatsApp foram ilícitos independentemente do que deliberar o Supremo Tribunal Federal sobre a aplicabilidade das sanções previstas no Marco Civil da Internet. São ilícitos em razão da impossibilidade técnica de cumprimento da ordem de entrega de dados em virtude de obstáculo fático representado pela criptografia – conforme entendimento do STJ. Ainda que fossem lícitos, conclui-se também que não poderiam ser fundamentados no poder geral de cautela do juiz em razão do impacto desproporcional em relação aos objetivos almejados – conforme as ordens de suspensão dos bloqueios reiteradamente reconheceram.

Conclusões. A análise apresentada evidenciou a complexidade e heterogeneidade de dimensões e perspectivas que caracteriza as guerras criptográficas. Na impossibilidade de um exame exaustivo de todos esses aspectos, o mapeamento de racionalidades conduzido neste estudo permitiu visibilizar premissas jurídicas e fáticas cujo mérito é passível de aferição acadêmica, o que pode contribuir significativamente para o amadurecimento do debate. Paralelamente, demonstrou a existência de racionalidades sociotécnicas e disputas políticas mais profundas que subjazem os pontos de vistas dos atores, o que reforça a perenidade das guerras criptográficas para além de controvérsias sobre premissas específicas.

1. Introdução

A criptografia, ao longo das últimas décadas, tem evoluído para se tornar uma das ferramentas mais importantes para garantir a segurança no meio digital. Conforme se difundiu o uso da internet como ferramenta para os mais variados tipos de serviços, concomitantemente aumentou a demanda para que esses serviços fossem prestados de forma segura. Por isso, o uso de criptografia foi progressivamente difundido na sociedade durante a segunda metade do século XX e início do século XXI. Algumas das principais aplicações presentes desse recurso incluem plataformas de mensageria privada, transações eletrônicas, serviços bancários digitais, sistemas de saúde e mecanismos de controle de tráfego aéreo.

A propagação do uso de criptografia na sociedade, contudo, não é livre de controvérsia. Nas últimas décadas, autoridades do setor de persecução penal vêm adotando uma retórica crítica ao emprego de certas aplicações criptográficas, notavelmente o uso de criptografia forte[1] para a proteção das informações armazenadas ou comunicadas por indivíduos. Para essas instituições, a massificação da criptografia forte em dispositivos pessoais e plataformas de comunicação se tornou um obstáculo para o exercício de suas funções, pois dificulta ou impede a produção de informações necessárias à prevenção e repressão da atividade criminosa. Tais atores por vezes utilizam o termo "obscurecimento" (*Going Dark*) para designar o alegado fenômeno de que a criptografia tornaria as comunicações digitais ilegíveis à autoridade policial, o que favoreceria o cometimento de ilícitos[2].

Em consonância a essa percepção, tentativas estatais de restringir ou limitar o desenvolvimento e o emprego de criptografia forte são observadas em diversos países, como Brasil, Estados Unidos, Reino Unido, Rússia e Austrália[3]. Em geral, tais esforços se associam à demanda pela introdução de um mecanismo que faculte à autoridade estatal o acesso às informações cifradas. Essas propostas frequentemente encontram resistência de especialistas em segurança da informação e ativistas dos direitos digitais, que as contrapõem com alegações de que tal mudança reduziria a segurança dos sistemas e submeteria os cidadãos a potenciais abusos de poder[4].

---

1 Um algoritmo criptográfico é considerado forte ou computacionalmente seguro quando sua segurança não puder ser quebrada em tempo hábil com os recursos computacionais disponíveis no presente ou no futuro. Ver SCHNEIER, Bruce. **Applied Cryptography**: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. New Jersey: John Willey & Sons, 1996, p. 30.

2 Ver BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (BERKMAN). **Não Entre em Pânico**: Avançando no debate sobre "obscurecimento" (Going Dark). 2018. Tradução pelo Instituto de Tecnologia e Sociedade do Rio. Disponível em: https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf. Acesso em 02/08/2021.

3 RODRIGUES, G. R. A controvérsia cifrada: o Clipper e o mito da derrota estatal nas guerras criptográficas dos anos 1990. Em: ALVES, Marco Antônio Sousa. NOBRE, Marcio Rimet. (orgs.). **A sociedade da informação em questão**: o direito, o poder e o sujeito na contemporaneidade. Belo Horizonte: D'Plácido, 2019.

4 RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

Comumente designadas como guerras criptográficas (*Crypto Wars*), tais controvérsias assumiram importância crescente na agenda de debates sobre políticas de governança da internet na década de 2010. As guerras criptográficas evocam considerações de segurança da informação sobre os impactos de arranjos infraestruturais particulares, questões jurídicas referentes às obrigações e sanções aplicáveis a provedores de serviços de internet, conflitos políticos entre atores estatais e empresas globais de tecnologia e disputas simbólicas sobre os significados do conceito de segurança e sua relação com a privacidade. Dessa forma, mobilizam as perspectivas de diversos atores, como representantes da justiça criminal, gestores de empresas privadas de tecnologia, ativistas dos direitos digitais, especialistas em segurança da informação, juristas dedicados às questões tecnológicas, entre outros.

Com o objetivo geral de compreender as racionalidades técnicas, jurídicas, políticas e econômicas que orientam os diferentes atores envolvidos na construção dos debates sobre esse tema no Brasil, o presente trabalho intentou mapear especificamente seus argumentos, crenças e percepções sobre as relações entre criptografia, privacidade, segurança pública, segurança da informação e direitos. Para tanto, foram realizadas entrevistas qualitativas com mais de 40 profissionais especializados ou engajados com o debate sobre os referidos temas. Os entrevistados foram selecionados por meio do método de amostragem em bola de neve. As transcrições das entrevistas foram, em seguida, codificadas e submetidas à análise qualitativa sistemática de conteúdo com o auxílio do software Atlas.ti 7.0. Com base na análise, seus argumentos e pontos de vista foram reconstruídos narrativamente e apresentados neste trabalho.

A relevância desta pesquisa justifica-se tanto pela atualidade e importância política, já descritas, de seu objeto quanto pela novidade de sua abordagem, uma vez que estudos interdisciplinares de impacto que abordem empiricamente as diferentes percepções dos envolvidos na controvérsia são pouco conhecidos ou inexistentes na academia nacional. A abordagem jurídica tem predominado no país, em geral por meio de estudos[5] que examinam os bloqueios sofridos pelo aplicativo WhatsApp à luz do ordenamento legal brasileiro, analisam e comparam diferentes modelos regulatórios ou discutem as relações entre a criptografia e os direitos fundamentais. Nesse cenário, o trabalho carrega o potencial para uma contribuição inovadora a partir da qual se poderá extrair uma agenda de pesquisa futura que examine de forma aprofundada as teses e percepções levantadas neste trabalho.

O texto apresenta 6 seções, incluída esta introdução, e duas peças em anexo (apêndice). Na seção 2, apresentamos uma breve contextualização das guerras criptográficas nos

5 Ver, por exemplo, KURTZ, Lahis P.; MENEZES, Victor. A.. Entre o direito e a força na sociedade da informação: bloqueio judicial do WhatsApp e ADI nº 5.527. In: Fabrício Bertini Pasquot Polido; Lucas Costa dos Anjos; Luiza Couto Chaves Brandão. (Org.). **Tecnologias e conectividade**: direito e políticas na governança das redes. 1ed. Belo Horizonte: 2018, v. 1, p. 15-30.; CARVALHO, Thaís B.. **O bloqueio judicial do WhatsApp no território brasileiro no contexto do Estado Democrático de Direito.** 2017. 69 f. Monografia de graduação no curso de Direito - Universidade Federal de Lavras, Lavras, 2017; ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42.; DONEDA, Danilo. MACHADO, Diego. (coords.) **A criptografia no direito brasileiro**. São Paulo: Thompson Reuters - Revista do Tribunais, 2019.

Estados Unidos e no Brasil, recordando alguns dos processos e episódios históricos que marcaram a história do debate nesses contextos. Na seção 3, detalhamos a metodologia da pesquisa, elaborando de forma pormenorizada os processos de seleção dos entrevistados, realização das entrevistas e codificação e análise dos dados.

Na seção 4, apresentamos os resultados da pesquisa, indicando as percepções dos entrevistados sobre os seguintes temas: i) acesso excepcional em sistemas criptográficos para persecução penal; ii) possíveis alternativas para acesso das autoridades ao conteúdo decifrado sem interferência direta na criptografia, bem como seus riscos; iii) avaliação fática e normativa sobre o ambiente regulatório nacional referente à criptografia; iv) opinião sobre os bloqueios do WhatsApp no Brasil e sua relação com o Marco Civil da Internet.

Em seguida, na seção 5, os resultados são discutidos pelos autores, considerando aspectos contextuais e referências importantes para o debate. Por fim, as conclusões são apresentadas na última seção, seguida dos apêndices - onde se encontram informações adicionais sobre o percurso metodológico da pesquisa.

2. Contexto - as Guerras Criptográficas

Conforme evoluíram as técnicas criptográficas, tornou-se cada vez mais evidente a aplicabilidade estratégica dessa tecnologia para a confecção de ferramentas de diversas naturezas – inclusive para aplicações militares –, o que, por sua vez, valorizou a criptografia aos olhos de governos ao redor do mundo. Concomitantemente, o avanço técnico nessa área do conhecimento, combinado com a perspectiva de exportação e facilitação do acesso a técnicas avançadas de criptografia para países terceiros e até mesmo para a sociedade civil, motivaram um protecionismo por parte dos governos que detinham conhecimentos mais avançados na área da criptografia.[6] [7]

Essas ações protecionistas são justamente o que se entende pelas Guerras Criptográficas. Em linhas gerais, foram embates entre os setores público e privado, nos quais o Estado buscava interpor barreiras à massificação do uso da criptografia por empresas que, cientes do apelo comercial da tecnologia, almejavam incluí-la em seus produtos. Tradicionalmente, são enumeradas duas ocorrências principais desses eventos – ao final do século XX e a partir de 2013 –, correspondentes à Primeira e à Segunda Guerras Criptográficas[8]. Importa destacar, contudo, o entendimento atual de que as Crypto Wars

6 FROOMKIN, M. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

7 INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. Cryptologi v. 3, n. 3, 129 - 135, 1979.

8 Apesar da enumeração usual das Guerras Criptográficas em duas instâncias, o historiador e criptólogo Craig Jarvis

não se trataram de eventos isolados e compartimentalizados, mas sim de pontos de destaque em um contexto de perene conflito envolvendo interesses estatais, empresariais e civis.[9] A seguir, será apresentado um breve resumo dos principais eventos que marcaram esse conflito e seus principais marcos a fim de contextualizar a leitura.

2.1. Guerras criptográficas no século XX

Houve dois episódios principais que sintetizam a primeira etapa das Guerras Criptográficas, que tem raízes na década de 70 e durou aproximadamente até o fim da década de 1990.

Durante a II Guerra Mundial, mensagens cifradas eram utilizadas para permitir a comunicação por rádio entre forças aliadas, impedindo que estas fossem compreendidas pelo inimigo. Nesse cenário, eram empregados esforços para decifrar as comunicações inimigas e obter uma vantagem estratégica. Aproximadamente nesse período – em decorrência de sua enorme utilidade bélica –, a criptografia passou a ser considerada pelo governo estadunidense como análoga à munição militar.

Nesse contexto, o primeiro momento das Crypto Wars consistiu em uma série de tensões relacionadas às tentativas dos EUA de restringir a disseminação doméstica e exterior da criptografia. No plano externo, isso se deu por meio da interposição de barreiras estritas para a exportação de técnicas criptográficas. Categorizada como forma de armamento, a criptografia foi inserida entre os itens protegidos pelas legislações estadunidenses relativas à exportação de equipamento bélico – a *International Traffic in Arms Regulations* e o *Arms Export Control Act*[10], ambas normas de 1976.

No plano doméstico, por sua vez, a atuação da NSA se voltava a inibir a difusão da criptografia forte no setor privado e na sociedade civil. Destaca-se, nesse ponto, a tentativa governamental de determinar o algoritmo criptográfico a ser utilizado pelo setor privado, o *Data Encryption Standard* (DES), desenvolvido pela NSA e pela Agência Nacional de Padrões[11]. Em 1977, o governo federal do país selecionou uma versão revisada desse padrão, o algoritmo LUCIFER, desenvolvido pela IBM, como padrão nacional. A implementação do LUCIFER/DES foi objeto de críticas da comunidade técnica e do setor privado, pois impunha um limite severo sobre o tamanho das chaves criptográficas[12].

argumenta em favor do reconhecimento de ao menos mais um desses eventos. Segundo Jarvis, a Primeira Guerra Criptográfica teria ocorrido entre os anos de 1966 e 1981, englobando eventos como a criação do primeiro algoritmo criptográfico aprovado pelo governo dos EUA (o chamado DES, ou "*Data Encryption Standard*"), o qual foi acusado por diversos criptólogos de ter sofrido alterações em seu funcionamento para permitir acesso extraordinário da NSA às comunicações cifradas. A Primeira Guerra Criptográfica, segundo o autor, também teria incluído a tentativa do governo estadunidense de impedir a publicação da obra *The Codebreakers*, de David Kahn. Para mais informações, conferir: JARVIS, Craig. **Crypto Wars**: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. CRC Press, 2020.

9 AULA 4 - Criptografia: experiências regulatórias e debates internacionais com Diego Canabarro. Belo Horizonte: Instituto Iris, 2021. (39 min.), son., color. Disponível em: https://youtu.be/EDaI5_z-hBo?t=2200. Acesso em: 25 ago. 2021.

10 ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42. p. 29.

11 LIU, H. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. **Journal of World Trade**, v. 51, n. 2, p. 309 - 334, 2017.

12 O padrão proposto originalmente permitiria chaves criptográficas de 100 bits, mas a NSA exigiu que esse

Além disso, críticos suspeitavam que pudesse haver um backdoor – uma vulnerabilidade propositalmente inserida no sistema – no algoritmo.

Ainda, a década de 1970 foi marcada por outro evento chave: a publicação do artigo *New directions in cryptography* pelos pesquisadores Whitfield Diffie e Martin Hellman na revista *IEEE Transactions on Information Theory* em 1976[13]. Hoje conhecido como criptografia de chave pública ou criptografia assimétrica, o método de distribuição de chaves desenvolvido pela dupla permitia o desenvolvimento de sistemas que dispensavam qualquer terceiro de confiança. Conjugados, a resistência civil ao LUCIFER/DES e o advento da criptografia assimétrica sinalizavam uma ameaça ao controle da NSA sobre a criptografia. Preocupações dessa natureza já eram expressas pelas lideranças da agência no fim da década. Em 1979, por exemplo, Bobby Inman, então diretor da agência, escrevia acerca da matéria[14]:

> Da perspectiva da NSA, o cerne do problema é que preocupações maiores sobre a proteção das telecomunicações no setor não-governamental implica maior conhecimento e discussão pública sobre técnicas de proteção das comunicações. A principal dessas técnicas é, é claro, a criptografia. Há um perigo bastante real e crítico de que discussão pública irrestrita sobre questões criptológicas prejudicará seriamente a habilidade desse governo em conduzir inteligência de sinais e a capacidade desse governo para desempenhar sua missão de proteger informações de segurança nacional de exploração hostil (ênfase dos autores deste estudo, tradução livre)

O segundo ponto de inflexão ocorreu anos mais tarde, na década de 1990 – embora durante esse intervalo a pressão dos EUA contra a disseminação da criptografia tenha permanecido constante. O marco inicial dessa nova fase das guerras criptográficas se deu em 1993, quando foi proposto o *Escrowed Encryption Standard* (padrão de criptografia sob custódia, em tradução livre). Como o nome sugere, tratou-se de uma proposta por meio da qual o governo estadunidense pretendia padronizar a venda de criptografia para terceiros, condicionando-a à custódia das chaves criptográficas de suas comunicações por agentes de investigação pública[15].

---

número fosse reduzido para 56. Uma vez que chaves menores são mais facilmente quebráveis por meio de ataques de busca exaustiva de chave, nos quais se percorre rapidamente todas as chaves possíveis, críticos passaram a enxergar o LUCIFER/DES como desenvolvido para que a chave fosse "longa o bastante para frustrar bisbilhoteiros de corporações, mas pequena o bastante para ser quebrada pela NSA". Ver FROOMKIN, M. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995, p. 735, tradução livre.

13 DIFFIE, Whitfiead. HELLMAN, Marin. New directions in cryptography. **IEEE Transactions on Information Theory**, 22, 644-654.

14 INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. **Cryptologia**, v. 3, n. 3, 129 - 135, 1979.

15 FROOMKIN, Michael. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

Esse objetivo seria alcançado através da implementação dos chamados "Clipper Chip" e "Capstone Chip" respectivamente em telefones e computadores – coprocessadores que encriptariam as comunicações realizadas pelos usuários, mas guardariam uma cópia das chaves criptográficas em custódia de uma entidade terceira considerada confiável pelos proponentes do padrão. Dessa forma, através de um *backdoor*, as entidades investigativas estadunidenses poderiam ter acesso a todo conteúdo daa todo conteúdo das comunicações encriptadas dos usuários.[16]

O padrão proposto foi alvo de severas críticas por parte do setor empresarial, ciente de que a comercialização de dispositivos contendo o Clipper e o Capstone estava fadada a sofrer perante a concorrência internacional de empresas estrangeiras não submetidas a essa exigência legal. Ao mesmo tempo, houve grande mobilização contrária ao *Escrowed Encryption Standard* por parte da comunidade técnico-científica e da sociedade civil, que respectivamente apontavam os riscos de segurança do modelo e as afrontas às liberdades civis que ele representava.[17]

Em paralelo à pressão contrária à utilização do Clipper e do Capstone, o lançamento do PGP (*Pretty Good Privacy*) em 1991 foi fundamental para a queda do *Escrowed Encryption Standard*. Trata-se de um software gratuito de criptografia de chave pública, que serviu como exposição inicial da população civil aos algoritmos criptográficos realmente seguros. Seu criador, Phil Zimmermann, foi submetido a anos de investigação por parte das autoridades estadunidenses, mas eventualmente considerado inocente, mediante o reconhecimento de que os métodos utilizados para a disseminação do software eram protegidos pela legislação para a liberdade de expressão nos EUA.[18]

Durante a década de 1990, diversas audiências públicas foram realizadas acerca do assunto, que contribuiu enormemente para a disseminação pública do debate sobre criptografia, segurança e privacidade. Os debates culminaram na derrocada pública de propostas como o Clipper e Capstone.

A derrota pública do *Escrowed Encryption Standard*, as pressões populares pela liberação do uso de criptografia forte e segura nos EUA e a concorrência internacional por parte de países que também estavam desenvolvendo suas técnicas criptográficas culminaram, ao final do milênio, no afrouxamento das barreiras criadas desde os anos 70 para a comercialização dessa tecnologia. Nesse período, observou-se um crescimento considerável no uso de serviços criptografados, que passaram a ser empregados em grande escala pela população civil.

16 SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 234-235.

17 ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42.

18 SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 226-237.

Isso não significa que as guerras criptográficas tenham simplesmente se encerrado ao fim do século XX. Como argumenta a socióloga Karina Rider[19], a primeira década do século XXI foi marcada pela consolidação dos programas de vigilância massiva conduzidos pelo setor de inteligência dos EUA com a cooperação de diversas empresas de tecnologia. O Bullrun, um dos principais programas em questão, visava especificamente assegurar que a NSA continuaria apta a acessar comunicações criptografadas, fosse pelo enfraquecimento intencional dos algoritmos ou pela manipulação do mercado criptográfico. Se nos holofotes debate público as guerras criptográficas a década de 2010 pode ser compreendida como um período de ocultamento das guerras criptográficas, que passam a ocorrer longe dos holofotes do debate público.

2.2. Guerras criptográficas atuais (2013 - presente)

A chamada Segunda Guerra Criptográfica teve início aproximadamente no ano de 2013, a partir das denúncias de Edward Snowden. O ex-integrante tanto da Agência Central de Inteligência (CIA) quanto da Agência Nacional de Segurança dos EUA (NSA) denunciou as práticas de cibervigilância adotadas pelo governo estadunidense, o que iniciou um movimento global de busca por mecanismos de segurança verdadeiramente efetivos.

Um segundo evento notório ocorreu em 2015: trata-se do caso *Apple vs. FBI*. O processo ocorreu em virtude da criptografia total de disco utilizada nos celulares da fabricante. O FBI buscava por meios judiciais uma forma de obrigar a empresa auxiliar no desbloqueio de um iPhone 5C, cujos conteúdos estavam protegidos com criptografia forte, e que havia sido utilizado por um indivíduo investigado em virtude do ataque terrorista de San Bernardino, na Califórnia. A empresa recusou-se a auxiliar o órgão de investigação, alegando que a implementação de um *backdoor* em seu sistema operacional resultaria em prejuízos para a segurança de toda a base de usuários da plataforma iOS. Apesar de o FBI ter desistido do processo judicial, por ter contornado a criptografia do dispositivo por meios diversos e acessado as informações pretendidas, o caso *Apple vs. FBI* foi utilizado como exemplo para motivar um aumento na pressão exercida por autoridades investigativas contra técnicas de criptografia forte[20].Essa pressão é muito bem ilustrada pelo discurso[21] proferido em 2014 pelo então diretor do FBI, James Comey, que contribuiu significativamente para a difusão pública do conceito de "*Going Dark*". Trata-se da ideia de que os mecanismos modernos de segurança e privacidade representam um "obscurecimento" das ferramentas investigativas estatais e representam, portanto, um empecilho ao combate ao crime cibernético, ao terrorismo e à efetivação da justiça.

19 RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

20 MITCHELL, Bonnie et al. **Going Dark**: Impact to Intelligence and Law Enforcement and Threat Mitigation. US Department of Homeland Security. Office of Intelligence and Analysis. 2017. p. 14

21 COMEY; James B. **Going Dark:** Are Technology, Privacy, and Public Safety on a Collision Course? Out. 2014, discurso realizado na Brookings Institution. [Online]. Disponível em https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acesso em: 02 ago. 2021.

O *Going Dark* foi posteriormente mencionado em um relatório[22] publicado em 2017 pelo Gabinete do Diretor de Inteligência Nacional dos EUA (ODNI). No documento, são apresentadas possíveis soluções para a questão do obscurecimento, com recomendações que incluem o fortalecimento das chamadas atividades de *hacking* governamental, bem como de parcerias técnicas com representantes do setor privado, a fim de possibilitar às autoridades investigativas o acesso aos meios de prova considerados necessários para a persecução penal de possíveis infratores.

A narrativa do obscurecimento eventualmente ganhou repercussão internacional e motivou a criação de legislações que buscam o enfraquecimento de técnicas de criptografia forte em diversos países. Notadamente, pode-se citar a aprovação do *Telecommunications and Other Legislation Amendment* na Austrália em 2018, que determina, entre outros, que provedores de serviços de comunicação facilitem o acesso das autoridades estatais a dados, inclusive cifrados, por meio de mandados de assistência técnica ou acesso a informações.[23]

A Índia recentemente também tornou-se um exemplo de país cuja legislação apresenta possíveis obstáculos para o uso de técnicas criptográficas. Isto porque em 2021 foi aprovada a emenda às regras aplicáveis às mídias digitais no país, com obrigações de rastreabilidade dos perpetuadores originais dos conteúdos publicados. Nesse sentido, há receio de que aplicativos de mensageria instantânea com criptografia de ponta-a-ponta para proteger as comunicações de seus usuários possam ter a segurança de seus sistemas prejudicada para atender às exigências legais.[24] [25]

2.3. As guerras criptográficas no Brasil

2.3.1. Os bloqueios do WhatsApp no país

De forma similar ao que ocorreu nos EUA e outros países ao redor do globo, o debate quanto ao obscurecimento da justiça também ganhou força no Brasil. As quatro tentativas de bloqueio do aplicativo WhatsApp entre os anos de 2015 e 2016 foram algumas das primeiras instâncias desse debate no país.

Em fevereiro de 2015, na Comarca de Teresina, Piauí, o juiz Luiz de Moura Correia concedeu o pedido, realizado pelo Núcleo de Inteligência da Polícia Civil do Estado do Piauí, de suspensão das atividades da empresa no Brasil. Em nota, o magistrado afirmou que a medida se deu "em razão de reiterados descumprimentos de ordens judiciais emanadas

22 MITCHELL, **Bonnie et al. Going Dark:** Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017.

23 Stilgherrian. **The Encryption Debate in Australia:** 2021 Update. 2021.

24 GROVER, Gurshabad; RAJWADE, Tanaya; KATIRA, Divyank. The Ministry And The Trace: Subverting End-To-End Encryption, 14 NUJS Law Review. 1(2021). p. 2-6. Disponível em http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/. Acesso em: 02 ago. 2021.

25 RAY, Trisha. The Encryption Debate in India: 2021 Update. 2021.

deste Juízo, em diversos procedimentos que apuram crimes da mais elevada gravidade"[26]. A ordem foi suspensa no mesmo dia pelo Tribunal de Justiça do Piauí[27], que a considerou desproporcional e danosa aos usuários, além de entender que existiam meios menos gravosos de investigação. O bloqueio não chegou a se concretizar.

O segundo bloqueio aconteceu em dezembro daquele mesmo ano, sendo determinado pela 1ª Vara Criminal de São Bernardo do Campo, São Paulo e suspenso cerca de 12 horas após seu início[28]. Conforme relata a liminar de suspensão do bloqueio[29], a empresa descumpriu comando judicial de interceptação de comunicações telemáticas de três pessoas investigadas no contexto de apuração da prática de tráfico de drogas, o que suscitou a aplicação de multa diária e, subsequentemente, o bloqueio da aplicação por 48 horas. O Tribunal de Justiça do Estado de São Paulo suspendeu o bloqueio por entender que a medida violava o princípio da proporcionalidade e que existiriam meios menos gravosos de coerção da empresa, como a elevação do valor da multa.

Após os dois primeiros bloqueios, o WhatsApp anunciou no dia 05 de abril de 2016 a implementação da criptografia de ponta-a-ponta[30], afirmando que "todas as mensagens, fotos, vídeos, arquivos e mensagens de voz" trocadas entre usuários que utilizassem as últimas versões da aplicação estariam protegidas pela criptografia, a partir do protocolo criptográfico Signal.

Posteriormente naquele mês ocorreu o terceiro caso, quando a vara criminal da Comarca de Lagarto, Sergipe, determinou, em 26 de abril, a suspensão do aplicativo por 72 horas em razão de novo descumprimento de ordem judicial de entrega de dados pessoais de usuários do aplicativo[31]. A ordem citou os artigos 3, 10, 11, 12, 13 e 15 do Marco Civil da Internet como seus fundamentos. O bloqueio foi suspenso pelo Tribunal de Justiça do Sergipe[32], que entendeu que a suspensão dos serviços gerou "caos geral em todo o território", bem como não ser possível afirmar "que as informações poderiam ser

26 BRASIL. Central de Inquéritos da Comarca de Teresina. **Nota**. Juiz Luiz de Moura Correia. Teresina, 26 fev. 2015. Disponível em: http://s2.glbimg.com/MdNVliNDOaF45o27HM8_tsG3wlI=/s.glbimg.com/jo/g1/f/original/2015/02/26/nota_juiz_whatsapp_ok.jpg. Acesso em: 29/07/2021.

27 BRASIL. Tribunal de Justiça do Estado do Piauí. **Mandado de Segurança nº 2015.0001.001592-4**. Rel. Des. Raimundo Nonato da Costa Alencar. Teresina, 26 fev. 2015. Disponível em: <http://www.migalhas.com.br/arquivos/2015/2/art20150227-03.pdf> Acesso em: 29/07/2021.

28 BARIFOUSE, R.; DUARTE, F.; BARRUCHO, L. G. Liberação do WhatsApp não encerra polêmica disputa com Justiça brasileira. **G1**. Tecnologia e Games. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/12/liberacao-do-whatsapp-nao-encerra-polemica-disputa-com-justica-brasileira.html. Acesso em: 29/07/2021.

29 BRASIL. Tribunal de Justiça do Estado de São Paulo. **Mandado de Segurança nº 2271462-77.2015.8.26.0000**. Decisão liminar. Rel. Des. Xavier de Souza. São Paulo, 17 dez. 2015. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_22714627720158260000_17122015.pdf. Acesso em: 29/07/2021.

30 WHATSAPP INC. **Blog do WhatsApp**. Criptografia de Ponta-a-Ponta. 05 abr. 2016. Disponível em: https://blog.whatsapp.com/end-to-end-encryption. Acesso em: 30/07/2021

31 BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. **Processo nº 201655090143**. Decisão. Juiz Marcel Maia Montalvão. Lagarto, Sergipe, 26 abr. 2016.

32 BRASIL. Tribunal de Justiça do Estado de Sergipe. **Mandado de Segurança nº 201600110899**. Decisão liminar. Rel. Des. Ricardo Múcio Santana de Abreu Lima. Aracaju, 3 mai. 2016. Disponível em: <http://www.omci.org.br/m/jurisprudencias/ arquivos/2016/tjse_201600110899_03052016.pdf> Acesso em: 2 nov. 2016.

fornecidas pelo WhatsApp ou que estas podem ser desencriptadas para servir à Justiça".

Por fim, o quarto bloqueio foi determinado pela 2ª vara criminal da Comarca de Duque de Caxias, Rio de Janeiro, também por descumprimento de ordem judicial de quebra de sigilo e interceptação telemática de mensagens. Conforme relata a decisão[33], a ordem foi respondida com um e-mail redigido em inglês, o que foi interpretado pela magistrada como uma sinalização de desconsideração da autoridade nacional. O documento faz referência aos artigos 7, 10 e 11 do MCI, ao art. 139, IV, do Código de Processo Civil e ao art. 3º do Código de Processo Penal. O bloqueio foi suspenso pelo Supremo Tribunal Federal, que entendeu[34] que o bloqueio violava o preceito fundamental da liberdade de expressão, bem como configurava medida desproporcional. Assim, com base no poder geral de cautela, reverteu a decisão.

2.3.2. A criptografia no Supremo Tribunal Federal: a ADI 5527 e a ADPF 403

Os diversos episódios de bloqueio do WhatsApp no Brasil geraram grande repercussão entre os diferentes setores da sociedade: desde os usuários em geral, que se viram impactados pela inacessibilidade do serviço durante a vigência dessas ordens judiciais, até a comunidade jurídica e técnico-científica, que comentaram extensamente sobre a legitimidade ou não dos comandos de bloqueio.

Concomitantemente à discussão acerca dos casos, foram ajuizadas perante o Supremo Tribunal Federal a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403[35] e, pouco depois, a Ação Direta de Inconstitucionalidade (ADI) nº 5527[36]. O objetivo dessas ações foi, em resumo, questionar a validade jurídica das ordens de bloqueio do WhatsApp perante a instância máxima do Poder Judiciário brasileiro, para que a decisão crie um mecanismo jurisprudencial que impeça novas ordens de bloqueio da plataforma.

Ajuizada logo após a segunda determinação de bloqueio da plataforma, a ADPF 403 sustenta que ordens judiciais dessa natureza violam o preceito fundamental da liberdade de comunicação – enunciada no art. 5º, IX, da Constituição Federal. Além disso, alega-se que houve também um descumprimento do princípio da proporcionalidade, haja vista que as ordens de bloqueio – relativas a casos esparsos e individualizados que tramitam no Judiciário – resultam na inacessibilidade da plataforma por toda a sociedade brasileira.

33 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Inquérito Policial nº 062-00164/2016**. Juíza Daniela Barbosa Assumpção de Souza. Duque de Caxias, RJ, jul. 2016. Disponível em: <https://drive.google.com/file/d/0Bw3seZUv__5ubnFudjUwMm9OZGc/view>. Acesso em: 30/07/2021

34 BRASIL. Supremo Tribunal Federal. **Medida cautelar de arguição de descumprimento de preceito fundamental**. Decisão liminar. Rel. Min. Ricardo Lewandowski. Brasília, 19 jul. 2016. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Acesso em: 30/07/2021.

35 BRASIL. Supremo Tribunal Federal. **ADPF 403**. Relator: Edson Fachin. Brasília, DF. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acesso em: 06 ago. 2021.

36 BRASIL. Supremo Tribunal Federal. **ADI 5527**. Relatora: Rosa Weber. Brasília, DF. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Acesso em: 06 ago. 2021.

A ADI 5527, por sua vez, busca declarar a inconstitucionalidade dos artigos do Marco Civil da Internet (Lei nº 12.965/2014) utilizados para fundamentar as ordens judiciais de bloqueio do WhatsApp. Mais especificamente, argumenta-se em favor da declaração de inconstitucionalidade dos incisos III e IV do art. 12 do Marco Civil, que dizem respeito às sanções de suspensão temporária e de proibição das atividades de provedores de aplicação por falha em disponibilizar conteúdos de comunicações privadas requeridas em juízo (conforme previsto no art. 10, §2º, da mesma lei). Além disso, a ADI busca limitar os efeitos do art. 10, §2º, para que esse dispositivo legal seja aplicável apenas a casos de persecução penal – e não para descumprimento de ordens judiciais na seara cível, como ocorreu com os bloqueios do WhatsApp.

Em decorrência da similaridade de temas tratados em ambas as ações, foi realizada uma audiência pública conjunta em 2017, para que fossem colhidas informações sobre questões técnicas e práticas envolvidas nas controvérsias dos bloqueios da plataforma. Durante dois dias, diversas entidades, representando os interesses dos setores técnico-científico, governamental, terceiro setor e setor empresarial, foram ouvidas pelos Ministros relatores de ambas as ações de controle concentrado de constitucionalidade[37] As decisões proferidas pelo STF em cada um desses processos serão paradigmáticas para o futuro das comunicações protegidas por criptografia forte no Brasil. Em decorrência da complexidade e sensibilidade do tema, contudo, tanto a ADPF 403 quanto a ADI 5527 ainda estão aguardando julgamento definitivo, em razão de vista solicitada pelo Ministro Alexandre de Moraes em maio de 2020, mas pronunciamentos e votos importantes já foram proferidos por seus relatores.[38]

A Ministra Rosa Weber, relatora da ADI 5527, por exemplo, já se pronunciou em sentido de que as previsões dos incisos III e IV do art. 12 do Marco Civil são destinadas ao descumprimento de obrigações de proteção de registros, dados pessoais e comunicações – e não para o descumprimento de ordens judiciais.

Além disso, defendeu não existir uma dicotomia entre a busca pela segurança pública e o direito à privacidade – como costuma ser alegado pelos órgãos investigativos e os defensores da ideia do obscurecimento. A Ministra, nesse sentido, pontuou que medidas de acesso excepcional a comunicações cifradas representam violações aos direitos à liberdade de expressão e à proteção ao sigilo das comunicações. Além disso, que o enfraquecimento da criptografia representaria um retrocesso para o país e seria um "presente para regimes autoritários e criminosos".

O Ministro Edson Fachin – relator da ADPF 403 –, por sua vez, defendeu a ideia de que direitos digitais devem ser tão abrangentes quanto os direitos que a população detém no meio offline e representam direitos fundamentais dos brasileiros. Nesse sentido, o

37 ABREU, Jaqueline. **Audiência Pública sobre Criptografia e Bloqueios do WhatsApp:** argumentos diante do STF. 26/06/2017. Bloqueios.info . Disponível em <http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/ >, acesso em 02 ago 2021.

38 CANTO, Mariana. RAMIRO, André. REAL, Paula C. **Criptografia no STF:** O que dizem os votos de Rosa Weber e Edson Fachin e o que podemos aprender com eles. Disponível em https://ip.rec.br/2020/06/22/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/. Acesso em 02 ago 2021.

Ministro argumentou que a criptografia é um meio de se assegurar a proteção de direitos que são essenciais para a vida pública em uma sociedade democrática. Por isso, seria contraditório reduzir a segurança na internet em nome da segurança pública. Fachin também argumentou que a implementação de *backdoors* ou demais vulnerabilidades sistêmicas em algoritmos criptográficos – mesmo que apenas destinados a autoridades investigativas –, representaria um enfraquecimento da segurança desses sistemas de forma universal. Isso porque atores terceiros mal intencionados também teriam acesso a essas ferramentas, colocando em risco a totalidade dos usuários dos serviços afetados.

2.3.3. A criptografia perante a lei brasileira e outros conflitos recentes

A legislação brasileira vigente, em sua maioria, não faz menção específica a técnicas criptográficas. Isso não significa, contudo, que não exista um incentivo perceptível para a implementação dessa tecnologia em sistemas digitais.

O Marco Civil da Internet, por exemplo, promove o uso de medidas técnicas compatíveis com os padrões internacionais para a preservação da estabilidade, segurança e funcionalidade da rede (art. 3º, V). O decreto regulamentar dessa lei (Decreto nº 8.771/2016), por sua vez, enuncia a criptografia como uma das soluções tecnológicas possíveis e recomendadas para gerir registros digitais de maneira segura (art. 13, IV).

Já mais recentemente, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) versou sobre a adoção de padrões técnicos adequados para garantir a segurança e salvaguarda de dados pessoais que estiverem sob a tutela de agentes de tratamento. Enunciados nesse sentido podem ser encontrados, por exemplo, entre os princípios norteadores da proteção de dados no Brasil (art. 6º, VI e VII), nos requisitos legais para segurança e sigilo de dados (arts. 46, 47), nos dispositivos que prevêem um abrandamento das penalidades aplicadas em incidentes de proteção de dados quando restar comprovado que os agentes de tratamento envolvidos adotaram padrões técnicos, administrativos e operacionais adequados para evitar o incidente (arts. 48, § 3º, e 52, §1º, VIII), entre outros.

No que diz respeito especificamente ao uso de criptografia em aplicativos de mensageria privada, o Superior Tribunal de Justiça já decidiu mais de uma vez em defesa da encriptação de dados utilizada nesses serviços. Nesse sentido se pronunciaram a Terceira Seção[39] e a Quinta Turma[40] do STJ, que não consideraram cabível a imposição de multa a provedores de mensageria privada por descumprimento de ordem judicial em decorrência

39 BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Disponível em < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, acesso em 03 ago 2021.

40 BRASIL.Superior Tribunal de Justiça. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma.** 24/06/2021. Disponível em <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx>, acesso em 03 ago 2021.

de impossibilidades técnicas inerentes à tecnologia empregada.

Apesar desses enunciados legais e dos entendimentos jurisprudenciais recentes, observa-se no Legislativo nacional a tramitação de uma série de projetos de lei que, de uma forma ou outra, buscam relativizar o direito ao uso de criptografia forte no Brasil. Podem-se citar, a título de exemplo, o PL nº 5.285/2009, o PL nº 9.808/2018, o PL nº 11.007/2018 e o PL nº 2.418/2019. Apesar de disporem sobre medidas legislativas distintas, todos esses projetos têm em comum o objetivo de restringir ou enfraquecer o direito ao uso de técnicas criptográficas no Brasil – seja por meio da criminalização expressa do ato ou mesmo por meio da institucionalização de mecanismos de acesso excepcional do Estado a comunicações cifradas.[41]

Não obstante, a importação da narrativa do *Going Dark* para o Brasil teve ainda outras repercussões para o cenário nacional. Em 2019, foi organizado pelo então Ministro da Justiça e Segurança Pública, Sérgio Moro, o I Simpósio Going Dark Brasil.[42] O evento destinou-se à exposição das dificuldades vivenciadas por órgãos investigativos estatais em virtude de técnicas criptográficas e terminou com a assinatura de uma declaração[43] por representantes de 13 países. No documento, os avanços tecnológicos recentes – como criptografia e técnicas semelhantes – são apresentados como técnicas utilizadas por terroristas e criminosos para barrar o poder investigativo estatal, que motivariam, portanto, a ação conjunta da comunidade internacional para prevenir abusos nesse sentido.

Menciona-se, ainda, o apelidado "Pacote Anticrime", também idealizado pelo ex-Ministro Sérgio Moro e promulgado na forma da Lei nº 13.964/2019. Em seu texto original, a regulação previa a ampliação dos poderes de interceptação de órgãos investigativos estatais e pressupunha o dever das plataformas de colaborar para com a persecução penal. Dessa forma, o mecanismo deixava subentendida a extensão dessas obrigações para provedores de serviços protegidos por criptografia forte.

Mais recentemente, o texto preliminar do novo Código de Processo Penal[44] gerou controvérsias em decorrência da possível alteração dos mecanismos vigentes de autoridades investigativas a informações sigilosas. O projeto inclui uma expansão dos poderes estatais para interceptação de comunicações telemáticas. Dentre os enunciados previstos, destaca-se a obrigação de assistência estabelecida para provedores de serviços

41 Confira: RAMIRO, André. CANTO, Mariana. REAL, P. C. et al. **O Mosaico Legislativo da Criptografia no Brasil: Uma Análise de Projetos de Lei**. IP.Rec. Disponível em <https://ip.rec.br/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-no-Brasil-uma-an%C3%A1lise-de-Projetos-de-Lei-1.pdf >, acesso em 04 ago 2021.

42 BRASIL. Ministério da Justiça e Segurança pública. **Simpósio sobre Going Dark termina com declaração de 13 países.** Disponível em <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2>, acesso em 03 ago 2021.

43 BRASIL. **Declaração do 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 04 ago 2021.

44 AGÊNCIA CÂMARA DE NOTÍCIAS. Relatório preliminar do novo CPP incorpora provas digitais e novas tecnologias ao processo criminal. Relator: Deputado João Campos. 13/04/2021. Disponível em <https://www.camara.leg.br/noticias/745824-relatorio-preliminar-do-novo-cpp-incorpora-provas-digitais-e-novas-tecnologias-ao-processo-criminal/ >, acesso em 26 ago. 2021.

de telecomunicações, segundo a qual seus provedores passariam a ter a obrigação legal de disponibilizar os recursos e meios tecnológicos necessários para sua interceptação

Esses enunciados provocaram receio em integrantes da sociedade civil organizada e da comunidade técnico-científica nacional[45] e internacional[46], pela possibilidade de que se estabeleça um mecanismo legal para inserção de vulnerabilidades em sistemas criptográficos, como pressuposto para a conformidade regulatória de serviços de comunicação que empregam medidas de segurança dessa natureza. Isso, por sua vez, pode representar uma redução sistêmica na confiabilidade e segurança proporcionada por esses serviços, em prol de alegados benefícios à segurança nacional.

Percebe-se, portanto, que a importação da narrativa do obscurecimento para o contexto brasileiro, bem como a existência de uma guerra institucional contra a criptografia – uma Guerra Criptográfica –, representam tensões e ameaças atuais para o futuro dessa tecnologia no Brasil.

3. Metodologia

Esta seção descreve a metodologia utilizada na pesquisa. O item 3.1. detalha a seleção e o perfil dos entrevistados. O item 3.2 discute a dinâmica das entrevistas. O item 3.3 detalha o procedimento de codificação e análise dos dados. O item 3.4. ressalta as limitações da metodologia adotada.

3.1. Seleção dos entrevistados

A seleção de entrevistados foi realizada pelo método de amostragem em bola de neve, em que os participantes do estudo indicam novos participantes, criando uma rede social que se expande a partir das conexões dos entrevistados[47]. Esse método apresenta a vantagem de possibilitar o acesso a grupos de difícil acesso, como especialistas. Todavia, por se tratar de uma amostragem não-probabilística, não garante a representatividade da população estudada e é mais sensível a vieses de seleção, o que constitui uma limitação metodológica desta pesquisa. Os participantes iniciais foram definidos a partir das redes sociais da equipe do projeto e de indicações da ISOC Brasil, sendo favorecidas pessoas com expertise ou participação prévia na discussão pública sobre os temas de criptografia,

45 COALIZÃO PELOS DIREITOS NA REDE. Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. 20 de maio de 2021. Disponível em < https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>, acesso em 25 ago. 2021.

46 Global Encryption Coalition. Brazilian Code of Criminal Procedure reform must not undermine encryption. June 28, 2021. Disponível em < https://www.globalencryption.org/2021/06/brazilian-code-of-criminal-procedure-reform-must-not-undermine-encryption/>, acesso em 25 ago. 2021.

47 VINUTO, J. A amostragem em Bola de Neve na pesquisa qualitativa: um debate em aberto. **Temáticas** (UNICAMP), v. 44, p. 201-218, 2014.

privacidade e segurança da informação. No total, foram enviados 76 convites a possíveis entrevistados.

Foram realizadas 45 entrevistas: uma delas foi excluída da análise porque as respostas foram insuficientes e outra porque se constatou posteriormente que o entrevistado não possuía vínculo com o setor presumido. Das 43 entrevistas consideradas válidas, 13 foram conduzidas com representantes do setor privado e 10 com cada um dos demais setores (comunidade acadêmica, sociedade civil organizada e setor público). Houve paridade de gênero em todos os setores, exceto o privado, com 8 entrevistados do gênero masculino e 5 do feminino.

Quanto à área de formação, houve uma predominância da àrea jurídica (27 entrevistas), seguido pelo campo computacional (8, incluíndo Ciência da Computação, Redes e Engenharia da Computação), Ciências Sociais (5), Comunicação (4), Administração Pública e Políticas Públicas (3), Ciência Política e Relações Internacionais (2), Economia (1), História (1), Administração (1), Artes Visuais (1) e área interdisciplinar (3). Ainda, 14 dos entrevistados possuíam múltiplas formações, seja por terem feito múltiplas graduações ou por terem feito graduação e pós-graduação em áreas distintas.

Quanto à atuação profissional, as trajetórias são bastante heterogêneas. Entrevistamos gestores de relações governamentais de grandes plataformas digitais, pesquisadores de ONGs de tecnologia e direitos humanos, professores universitários dedicados a pesquisar temas conexos, servidores de agências reguladoras relevantes para o campo tecnológico, pesquisadores de mestrado e/ou doutorado voltados aos temas de internet e sociedade, advogados especializados em direito digital, operadores da justiça criminal nos níveis federal e estadual, assessores parlamentares federais, ativistas de direitos digitais e software livre, analistas de cibersegurança de entes públicos e privados, consultores privados de segurança da informação, entre outros vínculos dos entrevistados.

3.2. Realização das entrevistas

O roteiro das entrevistas continha perguntas referentes aos seguintes temas: trajetória profissional e acadêmica; importância atribuída à privacidade e à criptografia; percepção sobre a relação entre privacidade e segurança; satisfação com o ambiente regulatório nacional; opinião sobre acesso excepcional e riscos percebidos; opinião sobre o debate público relativo à privacidade no Brasil; opinião sobre meios alternativos de acesso a conteúdo cifrado que não envolvessem interferir na criptografia; e opinião sobre a legitimidade dos bloqueios do WhatsApp no Brasil. Para entrevistados com formação jurídica, também foi perguntado seu entendimento sobre a licitude de bloqueios judiciais de aplicação com base no Marco Civil da Internet. Para entrevistados do setor público, foi questionada sua avaliação sobre a importância atribuída à segurança na informação no contexto da digitalização governamental. Sua íntegra pode ser consultada no Apêndice 1.

As entrevistas tiveram caráter semiestruturado, isto é, o roteiro funcionou como um conjunto de diretrizes previamente fixadas, não como um protocolo a ser seguido à risca em cada interlocução concreta, e conduzidas de modo similar a conversas informais[48]. Essa opção metodológica intentou favorecer o estabelecimento de uma relação de confiança e segurança com os entrevistados, de modo a deixá-los mais à vontade para falar de forma mais livre e sincera - requisito necessário à realização de entrevistas que produzam maior riqueza de dados[49] -, sobretudo em razão do caráter controverso e sensível de alguns dos temas tratados. Adicionalmente, essa opção possibilitou uma exploração mais aprofundada das perspectivas e saberes específicos dos entrevistados.

Essa opção, no entanto, contribuiu para que nem todos os entrevistados respondessem à totalidade do roteiro uniformemente. Isso se deu em parte porque a exploração aprofundada de suas respostas a questões específicas ocupou parte do tempo de entrevista que seria preenchido por outras questões, o que exigiu que temas específicos fossem priorizados conforme o caso concreto. Paralelamente, a supracitada heterogeneidade de trajetórias e saberes também favoreceu essa variação, pois questões relativas a áreas do conhecimento ou setores específicos não necessariamente faziam sentido para todos. Por exemplo, uma questão sobre a interpretação de dispositivos específicos do Marco Civil da Internet pressupunha algum grau de conhecimento jurídico pelo entrevistado, de modo que não faria sentido colocá-la em todas as entrevistas.

3.3. Codificação e análise dos dados

Após a realização das entrevistas, seu conteúdo foi transcrito e uma estratégia de manuseio dos dados foi elaborada para que os dados gerados permanecessem em sigilo e em segurança. Primeiramente, os nomes reais dos entrevistados foram substituídos por nomes fictícios gerados por um software gerador de nomes e uma tabela de conversão foi criada. Os arquivos foram cifrados e inseridos num aplicativo de nuvem criptografado. Os pesquisadores envolvidos nessa etapa de análise baixaram e alocaram os arquivos (entrevistas, transcrições, a tabela de conversão de nomes) em um compartimento cifrado de seus dispositivos locais. A chave para decriptação foi compartilhada através de um aplicativo de mensageria - igualmente encriptado e com a funcionalidade de auto destruição da mensagem após alguns minutos. A fim de excluir permanentemente os arquivos originais dos computadores pessoais, foi utilizada a ferramenta BleachBit - que destrói os rastros digitais dos arquivos. Uma vez decodificados, a análise pôde ser feita com o manuseio dos materiais anteriormente alocados no compartimento criptografado. As transferências de unidades de análise entre os pesquisadores também foram realizadas através de canais criptografados.

48 BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. **Em Tese - Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC**, Florianópolis, v. 2, n. 1 (3), p. 68-80, jan./jul. 2005, p.75.

49 GASKELL, G. Entrevistas individuais e grupais. In: BAUER, M. W.; GASKELL, G. (Org.). **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis, RJ: Vozes, 2000, pp. 64-89, p 74.

O conteúdo das entrevistas foi submetido, então, à análise qualitativa, que consiste em um "um conjunto de técnicas de pesquisa para tornar válidas e replicáveis inferências de textos (ou outro material significativo) aos contextos de seu uso"[50]. A codificação e o tratamento estatístico dos dados qualitativos foram auxiliados pelo software Atlas.ti 7.0, que oferece uma miríade de ferramentas destinadas a amparar pesquisadores na análise qualitativa[51]. Apesar de seus benefícios, é importante destacar que o programa não conduz a análise sozinho e é necessário que os pesquisadores produzam as conclusões a partir de seus aportes conceituais e epistemológicos.

A análise qualitativa sistemática teve caráter indutivo, isto é, a construção dos códigos e categorias de análise foi realizada com base no que se apreendeu dos próprios dados a partir de uma exploração inicial, e não em um conjunto pré-definido de critérios. Assumindo uma abordagem interpretativa, buscamos reconstruir os sentidos dados pelos entrevistados aos temas discutidos, o que possibilita tanto uma apreensão geral de suas crenças, visões de mundo e argumentos quanto a geração de novas hipóteses sobre o conjunto de fenômenos discutido na entrevista a partir das teorias nativas desses profissionais[52].

A fim de restringir o escopo da análise, foram selecionados quatro temas gerais explorados em diferentes segmentos das entrevistas: i) implementação de acesso excepcional em sistemas criptográficos para acesso a dados cifrados para fins de persecução penal; ii) conhecimentos e riscos sobre potenciais alternativas para acesso das autoridades ao conteúdo decifrado sem interferência direta na criptografia; iii) o ambiente regulatório nacional referente à criptografia; iv) os bloqueios do WhatsApp no Brasil e sua relação com o Marco Civil da Internet.

Para codificação e análise de cada um desses temas, foi seguido o seguinte procedimento: distribuição das entrevistas entre os pesquisadores responsáveis pela parte empírica da pesquisa para exploração inicial e codificação aberta do segmento, seguida por uma revisão conjunta da totalidade do universo codificado e consolidação dos códigos. Com base nisso, buscou-se estabelecer relações de significado entre os códigos e, a partir delas, reconstruir narrativamente os principais argumentos e enquadramentos dados pelos entrevistados aos temas tratados. Em razão da replicação quádrupla desse procedimento, foram produzidos quatro esquemas de codificação distintos e independentes, os quais podem ser consultados no Apêndice 2.

50 KRIPPENDORFF, K. **Content Analysis**: an introduction to its methodology. Thousand Oaks, Calif.: Sage Publications, 2004, p.18.

51 SILVA JUNIOR, L. A.; LEAO, M. B. C. O software Atlas.ti como recurso para a análise de conteúdo: analisando a robótica no Ensino de Ciências em teses brasileiras. **Ciênc. educ.** (Bauru), Bauru , v. 24, n. 3, p. 715-728, set. 2018.

52 ROSENTHAL, G. **Pesquisa social interpretativa**: uma introdução. Porto Alegre: Edipucrs, 2014.

3.4. Limitações da metodologia adotada

Em razão do caráter não-probabilístico da metodologia de seleção adotada, bem como do caráter semiestruturado das entrevistas e das variações na aplicação do roteiro, os resultados abaixo apresentados não devem ser interpretados como representativos das opiniões ou atitudes de qualquer segmento populacional.

O que eles constituem é um panorama empiricamente fundamentado de crenças, argumentos e racionalidades que atravessam o debate público sobre *Going Dark* e *Crypto Wars* no Brasil, conforme se pôde extrair à luz de 43 entrevistas com profissionais que participaram da construção desse debate.

4. Resultados

Esta seção apresenta os resultados da análise de conteúdo. Os resultados são apresentados na forma de reconstruções narrativas sobre as categorias de enunciados mais frequentes, a fim de evidenciar as conexões lógicas que permeiam suas racionalidades.

Todos os nomes utilizados são fictícios e foram determinados aleatoriamente a partir de um software gerador de nomes. As ênfases nas citações são obra dos pesquisadores do estudo.

4.1. Sobre a inserção de mecanismos de acesso excepcional na criptografia

As questões sobre mecanismos de acesso excepcional foram respondidas por todos os entrevistados.

4.1.1. O discurso favorável ao acesso excepcional

O apoio ao acesso excepcional se fundamenta no entendimento de que o acesso às comunicações privadas é **necessário para a segurança pública (argumento usado 4x)**, valor que deveria ser priorizado quando em conflito com outros direitos, como privacidade e liberdade de expressão. Segundo esse raciocínio, os danos causados por certos crimes - por exemplo, sequestros, tráfico de drogas, abuso infantil, terrorismo - são tão graves que justificam a relativização desses direitos em nome do interesse coletivo.

Além disso, **cidadãos e empresas têm a obrigação de obedecer à justiça (7x)**, o que implica no dever de cumprir ordens judiciais de entrega de dados para investigações criminais,

ainda que isso exija vulnerabilizar a criptografia. Isso porque o acesso excepcional já seria legalmente previsto por ser **equivalente a uma interceptação telefônica (3x).** Nesse caso, compreende-se que a prerrogativa de acesso estatal a comunicações privadas nos casos previstos pela Lei das Interceptações Telefônicas se estende às plataformas digitais. Nas palavras do entrevistado Afonso:

> Já tive do outro lado. Já tive do lado de quem tem que prender o bandido. E dá um trabalho quando você está com os dados todos criptografados. [...] Mecanismo excepcional é uma palavra também que combina bem. É um acesso excepcional, é o acesso do grampo telefônico. **A polícia não fica grampeando todo mundo à revelia, tem uma regra. Pra mim, essa regra pode ser a mesma regra para grampear o Whatsapp**.
>
> Afonso tem formação na área computacional, com foco em segurança da informação, e tem ampla experiência na docência, consultoria privada em redes e gestão de projetos.

Nesse ponto, há quem considere, inclusive, que **o acesso excepcional seria um meio investigativo tão ou menos gravoso que os empregados atualmente (2x)**. O raciocínio é o seguinte: uma vez que é necessário acessar tais comunicações para investigações de alguma forma, o acesso excepcional permitiria acessar o canal objetivado de forma precisa. Isso causaria danos menores que os de uma busca e apreensão, por exemplo, que além de suprimir a inviolabilidade do domicílio, possibilita a busca em todo o dispositivo e todas as informações nele contidas. Essa é a visão da entrevistada Thais, por exemplo:

> Gente, seria muito melhor se a gente trabalhasse com determinado aplicativo que a gente dissesse “eu quero saber só as mensagens do WhatsApp”. É só o WhatsApp, eu não to querendo suas fotos, sua lista telefônica, o que você conversa com sua mulher, entendeu? [...] Seria muito mais prático. Então acaba que **por falta de determinados aplicativos para fazer e ter acesso a essas mensagens, a gente se utiliza às vezes de mecanismos mais invasivos do que nós precisávamos muitas vezes**.”
>
> Thais tem formação jurídica e atua no sistema de justiça criminal, com foco em crimes cibernéticos

Quanto ao potencial de abuso pela autoridade, esses riscos seriam mitigados pela existência de **controles institucionais robustos (11x)**. Tais controles incluem a existência de ordem judicial específica e fundamentada, com determinação da finalidade e dos indivíduos específicos a serem afetados. Com frequência ressalta-se que deveria ser um recurso acionado **somente em casos de crimes graves (7x)**, como os supracitados, e **quando já se esgotaram outras possibilidades de investigação (3x)**. Junto a isso,

por vezes aparece a percepção de que **é necessário confiar nas instituições (2x)**. O entrevistado Julian resume bem:

> Agora, eu tenho que confiar na justiça. Eu, como advogado... Existindo uma lei que diga quando, como, em que condições e que somente nessas condições isso pode acontecer e há uma autoridade judicial investida pelo Estado para tomar essa decisão, **se eu não confiar nisso, eu não posso confiar em nada na justiça**. Seria uma confiança seletiva: "Não, eu confio na justiça, mas isso não". Por quê? Tem tribunal, tem corregedoria, tem CNJ, nós temos que confiar. [...] Não havendo outro recurso e diante de uma eventual gravidade do crime, com lei própria dizendo como isso vai acontecer, com decisão judicial específica e fundamentada, aí eu acho que sim, eu acho que nós teremos que enfrentar circunstâncias [em] que a paz social é mais importante que a paz criminosa.
>
> Julian tem formação jurídica, ampla experiência no setor público com regulação de tecnologia e trabalha no setor de relações institucionais de uma grande empresa

Defender que o Estado tenha acesso a conteúdos criptografados para fins de investigação aparece, ainda, como **uma forma de reafirmar a autoridade pública (1x).** Nessa linha, a defesa do acesso excepcional reiteraria simbolicamente que a competência investigativa e a autoridade geral do Estado estão acima de interesses e decisões de empresas privadas, as quais podem se achar na posição de desafiá-las em virtude de seu poder global. Para Natália, a defesa do acesso excepcional se conecta a essa disputa simbólica.

> As empresas precisam dar um jeito de colaborar com a gente, com a sociedade mesmo. Porque a empresa faz o modelo de negócios dela e eles querem ganhar dinheiro, então **se não existe uma pressão do poder público para que haja essa colaboração, por que eles vão gastar dinheiro montando um setor inteiro de uma empresa para dar suporte para as autoridades públicas?** Então você pensa, nossa, hoje o Google, o Facebook, eles têm escritórios e setores totalmente montados para dar suporte para o *law enforcement*, para a investigação de autoridades públicas. Por que eles fariam isso se não houver uma pressão do setor público nesse sentido? Então precisa ter essa pressão.
>
> Natalia tem formação jurídica e atua no sistema de justiça criminal, com foco em crimes cibernéticos

4.1.2. O discurso contrário ao acesso excepcional

A rejeição ao acesso excepcional tem como base a percepção de que a medida **contraria princípios básicos e boas práticas de segurança da informação (20x)**. Isso porque o aumento na complexidade de um sistema necessariamente reduz sua segurança, sobretudo mediante a introdução intencional de uma vulnerabilidade a ser utilizada regularmente. Assim, o acesso excepcional foi descrito como uma medida que "enfraquece a tecnologia como um todo" e "estaria quebrando a confiabilidade da criptografia por essência".

Conectados a tal preocupação estiveram os dois principais riscos apontados. O primeiro foi de que **o mecanismo fosse explorado por terceiros maliciosos (18x)**, a exemplo de criminosos cibernéticos e governos estrangeiros, que poderiam fazer uso da vulnerabilidade para fins ilícitos. Desse modo, a própria **segurança do Estado seria enfraquecida (4x)**, uma vez que a confidencialidade das comunicações das próprias autoridades depende de plataformas criptografadas. É essa a perspectiva do entrevistado Alvin:

> Vamos supor por um momento, esse é um pressuposto muito duro, no qual eu não creio - em termos pessoais eu não creio -, mas vamos supor que há bons atores e maus atores. Vamos supor que eu vivo num país de bons atores e que há uma boa política, um bom MP, boas autoridades, todos são moralmente bons, vamos supor isso, ok? A pergunta é: essas pessoas boas devem poder acessar com acesso excepcional para poder investigar situações ilegais? Bom, eu poderia pensar: sim, porque são bons! Eu sou bom, eles são bons, queremos proteger os bons. O problema é que essa lógica não existe. Eu não creio nessa lógica. Não são só bons, há de tudo. Mas seguindo nessa lógica, o problema é que no mundo nem todos são bons, há outros países, há outras organizações, há hackers, há máfias, há outros estados, não? **Então quando se cria esse acesso excepcional para os "bons", para essa gente pura que quer me proteger e cuidar de mim, quando se cria esse acesso excepcional para eles, também se abre uma vulnerabilidade para outros**. Então, na realidade, está criando uma vulnerabilidade que pode ser explorada por outros governos, outras organizações, por outras empresas, outros hackers, enfim.
>
> Alvin é economista, tem ampla experiência nos setores público e privado e atua no setor de relações institucionais de uma grande plataforma

O segundo principal risco foi de que o acesso excepcional fosse alvo de **abuso pelas próprias autoridades (18x)**, que poderiam instrumentalizá-lo para vigilância e perseguição política de opositores ou recorrer ao mecanismo de forma ampla e generalizada. A esse respeito, foi destacada uma preocupação com uma **possível banalização das quebras de sigilo (3x).** A entrevistada Vitória resume a preocupação:

> Como eu estava dizendo antes, as quebras têm conteúdo exploratório. E mais do que isso, antes até delas terem conteúdo exploratório, elas são em regra usadas como primeiro recurso de investigação. [...] As interceptações telefônicas, telemáticas... Está escrito na Lei 9296 que elas deveriam ser usadas como último recurso de investigação, quando todo o resto falha e se mostra insuficiente. Mas a gente percebe uma banalização, mesmo, e uma tendência dos juízes... Das autoridades policiais para requisitarem, do MP também, e dos juízes para deferirem sem critérios e sem uma demonstração efetiva de que algo precisaria ter sido feito antes, para que se demonstre uma necessidade intransponível de se quebrar esse tipo de dado. **Então eu entendo que se a gente encampar esse discurso também em relação à criptografia, ela será quebrada como regra e de forma extremamente ampla**.
>
> Vitória tem formação jurídica e ampla experiência advogando na intersecção entre processo penal e novas tecnologias

Outro argumento frequente foi de que **há ou deve haver meios alternativos de investigação (19x)**, entre os quais foram citados: análise de metadados, busca e apreensão de dispositivos, recuperação dos dados armazenados em *backups* na nuvem e infiltração policial. Alia-se a esse raciocínio o argumento de que **necessidade e eficácia da medida não foram suficientemente demonstradas (6x)**, haja vista a ausência de dados conclusivos referentes ao número de investigações que de fato não alcançam êxito devido à criptografia. Além disso, há **possibilidade de criminosos abandonarem plataformas em que a criptografia foi enfraquecida (8x)**, o que tornaria a eficácia do acesso excepcional nula. Os entrevistados Gilson e Maiara sintetizam esses dois últimos argumentos:

> Eu tenho muita curiosidade de saber também os números de situações que a polícia não conseguiu resolver por conta da criptografia, qual é a porcentagem. E acho que esse é um dado muito oculto, que para mim sempre é um buraco. Sempre que eu vou dar uma aula eu fico assim: **cara, a gente não sabe se a criptografia, hoje, é um problema**. Porque, assim, talvez tudo que eu falo mudasse se a gente percebesse que, sei lá, 95% dos crimes do Brasil não são solucionados por conta da criptografia, pois ela está atrapalhando.

> Beleza, talvez a gente mudasse de ideia. Mas a gente não sabe se não é 0,000009% dos crimes, então fica difícil saber desses dois extremos, onde que a gente está."
>
> Gilson é jurista, experiente no setor público e na docência, sua produção acadêmica se volta a questões envolvendo internet e direitos fundamentais

> Eu tenho essa percepção que é muito complicado porque na medida em que algumas empresas passam a dar esse acesso, **a gente sabe que a criminalidade migra**. Igual a gente vai mudar para o Signal, eles migram. Grandes organizações criminosas hoje contratam técnicos e eles têm condição de fazer o seu próprio aplicativo de mensagem que não vai dar acesso para o *law enforcement*, que não vai dar acesso, e aí você vai estar fazendo todo esse movimento, diminuindo – e eu tenho essa percepção, que vai estar diminuindo, sim – a segurança das informações das pessoas, as nossas mesmo.
>
> Maiara é jornalista, experiente em produção audiovisual e trabalha com educação de grupos ativistas, com foco em segurança digital

Sob esse ponto de vista, o acesso excepcional seria desproporcional na medida em que **afeta os direitos de todos os usuários (26x)** e impacta sua segurança, privacidade e liberdade de expressão em nome da resolução de alguns crimes. Isso atingiria sobretudo jornalistas, ativistas, minorias sociais e opositores governamentais, os quais estariam mais sujeitos a danos se suas comunicações privadas fossem violadas. Nesse sentido, foi notado que a própria possibilidade do governo se valer indevidamente do acesso excepcional já atingiria direitos em virtude do efeito inibitório que a consciência de estar sendo vigiado provoca sobre os indivíduos, o que poderia levá-los, por exemplo, a se refrear de expressar divergências políticas por temer o monitoramento estatal.

Ainda nesse prisma, foi observado que o acesso excepcional **impacta negativamente a confiança no ecossistema digital (13x)**, o que é necessário para que os cidadãos se sintam aptos a fazer uso dos bens e serviços num contexto de digitalização. Nessa linha, os **custos operacionais e reputacionais impostos aos provedores (11x)** foram citados como causadores de repercussões econômicas negativas, pois a complexidade de se desenvolver e manter um mecanismo dessa natureza seria elevada e plataformas que se valem do uso da criptografia como um diferencial competitivo associado à maior segurança, como o WhatsApp, sofreriam um enorme dano à marca e poderiam ter seus modelos de negócios inviabilizados.

4.2. Sobre alternativas ao acesso excepcional

Quanto ao conhecimento de métodos e técnicas alternativos capazes de fornecer às autoridades acesso ao conteúdo de dados protegidos por criptografia para fins de investigações criminais, 33 dos 43 entrevistados responderam a essa questão. Dos 33 respondentes, **7 afirmaram não lembrar ou desconhecer alguma alternativa**. Desse modo, foram 26 respondentes que falaram sobre alternativas e métodos ou técnicas.

Uma das principais alternativas citadas para o acesso aos dados foi a **apreensão dos dispositivos específicos relevantes para o caso (6x)**. Uma vez realizada a apreensão, as autoridades poderiam acessar seu conteúdo. Se o conteúdo estiver protegido por algum recurso de segurança, como criptografia de disco, as autoridades poderiam prosseguir de duas formas: I) compelir, mediante ordem judicial, algum usuário que conheça a senha ou chave de acesso a fornecê-la; ou ii) lançar mão de ferramentas que exploram vulnerabilidades na tecnologia para burlar os mecanismos convencionais de autenticação.

Essa segunda hipótese está conceitualmente próxima de todo um leque de alternativas objeto de frequente citação e agrupadas sob as rubricas de ***government hacking*** **ou** ***lawful hacking*** **(19x)**: o uso de técnicas e ferramentas destinadas a comprometer a segurança de dispositivos ou softwares utilizados pelas pessoas sob investigação, a fim de possibilitar a obtenção dos dados necessários à produção das provas. Nesse universo, métodos específicos citados incluíram:

- **Busca exaustiva de chave (3x):** A utilização de métodos computacionais para quebrar a segurança de um sistema criptográfico, a fim de decifrar texto sem que se tenha acesso autorizado à chave de decifragem. Exemplos incluem ataques de força-bruta, em que um elevado número de chaves ou senhas possíveis é percorrido em alta velocidade, ou de dicionário, em que se percorre uma lista pré-definida de possíveis chaves ou senhas. Essa solução seria adequada para casos em que a criptografia utilizada não é computacionalmente segura ou quando o sistema não possui proteções contra a execução de um número muito elevado de tentativas.

- **Engenharia social (3x)**: a autoridade policial encobriria sua identidade em uma interação com a pessoa investigada, a fim de induzi-la a cometer um ato que comprometeria a confidencialidade de suas informações, como o envio de credenciais de acesso a contas ou a inoculação de software malicioso em seu dispositivo.

- **Spyware (7x):** a introdução oculta de código malicioso no sistema alvejado para a exploração de vulnerabilidades não-solucionadas por seus desenvolvedores, o que favoreceria a coleta remota dos dados necessários à investigação. A depender da ferramenta utilizada, seria possível ativar o microfone, a câmera e/ou a geolocalização do dispositivo, bem como registrar mensagens digitadas e/ou enviados, sites e aplicativos utilizados.

Um segundo conjunto de soluções citadas envolveria algum grau de cooperação com as provedoras dos canais de comunicação. Nesse âmbito, foi mencionada a técnica de **escaneamento do cliente (2x)** (*client-side scanning)*, um mecanismo em que o software do dispositivo ou canal comunicativo testaria o conteúdo de cada mensagem enviada contra uma base de dados pré-definidas de conteúdos danosos, os quais estariam sinalizados com identificadores únicos. Se uma ocorrência daquele conteúdo fosse encontrada na base, alguma ação seria desencadeada: o envio seria impedido ou as autoridades seriam alertadas.

Soluções de chave ou usuário fantasma (2x) seguem o mesmo espírito: demanda-se que a plataforma implemente um mecanismo para introduzir uma terceira ponta na conversa sem que as partes se comunicando tenham ciência. Um aplicativo poderia transformar a conversa entre dois usuários num grupo do qual a autoridade faria parte sem que a interface da conversa fosse modificada ou que os dois usuários recebessem qualquer notificação. Paula exemplifica o funcionamento da prática e junto apresenta um ponto de discussão.

> Outro método que a gente viu foi o *ghost key*, que é muito defendido no Reino Unido, que é basicamente você mudar a interface para que o usuário não perceba que tem um agente com ele em uma conversa, seguindo a conversa dele, então ao invés de aparecer três pessoas na conversa, aparecem duas. **Mas há uma grande discussão se isso não é mais uma forma de acesso excepcional, você implementar uma vulnerabilidade que pode ser considerada acesso excepcional de toda forma.**
>
> Paula, formação jurídica e uma área interdisciplinar. Pesquisadora na área de privacidade e vigilância. Experiência na sociedade civil e academia.

Outra alternativa foi a **análise de metadados (5x)** num contexto em que estes não estão protegidos com criptografia. Desse modo, seria possível apreender informações sobre o horário de comunicações, localização, frequência de comunicações, etc. O entrevistado Eduardo defende que a prática seja, também, acompanhada de uma preocupação com a privacidade.

> [...] eu não defendo que haja uma colaboração extensiva sobre metadados porque isso feriria também a privacidade, mas acho que de outra maneira, seguindo o princípio de minimização de coleta de dados, de colaboração pontual, acho que é possível pensar em formas. Acho que esse é um debate em construção em que você preserve o que está sendo conversado, o que está sendo o mérito, o conteúdo da conversa, mas sem fornecer às autoridades judiciais algum tipo mínimo de informação de contexto ou usando metadados para expressão técnica. Mas aqui, de novo, acho que é um debate

> em construção, difícil. Há outros aplicativos de mensageria, o Signal por exemplo, que tem criptografado, é isso, metadados podem ser criptografados. Então o objeto da criptografia pode ser o conteúdo que está sendo conversado, mas a criptografia pode também abranger alguns metadados. E aí se você quer acesso aos metadados que estão criptografados, também é vulneração da criptografia.
>
> Eduardo. Formação jurídica, ampla experiência no setor público, trabalha com relações governamentais em uma grande empresa de tecnologia

Também foi citado o **acesso a dados em backups mantidos por terceiros (3x)**. A esse respeito, foi destacada existência de backups de conteúdos de conversas que gozam de níveis inferiores de proteção ou são armazenados de forma inteiramente descriptografada, os quais já seriam utilizados pelas autoridades para contornar a criptografia. Em sua entrevista, Thais descreveu como a prática vem sendo utilizada.

> E, na verdade, hoje em dia, com a nuvem, a gente já faz isso, entendeu? [...] Quando a gente faz o afastamento [do sigilo] da nuvem, ela acaba sendo assim, vamos dizer, como um *backdoor*, é quase não, é um *backdoor*. Porque quando a gente pede o afastamento [do sigilo] da nuvem porque você, justamente, você não tem acesso mediante a criptografia. Só que assim, não é todo mundo que tem a nuvem, tem aquela coisa toda de você fazer o backup. Tem nuvens de determinados apps que são mais acessíveis, sempre foram. Então não é todo mundo que utiliza ela, e tal, mas acaba que quando a gente tem uma quebra dessa, vem tudo da pessoa, entendeu?
>
> Thais. Formação jurídica, atua no sistema de justiça criminal, com foco em crimes cibernéticos.

Na mesma linha, **o monitoramento das redes sociais (1x)** foi citado como medida que permitiria apreender informações relevantes à investigação, como viagens realizadas, relações pessoais, bens, etc.

4.2.1. Os riscos das alternativas

Junto à pergunta sobre os métodos alternativos de obtenção de dados para investigação que não impliquem na quebra de criptografia, os entrevistados foram questionados, também, sobre os riscos atribuídos às práticas citadas.

Uma percepção recorrentemente manifestada foi de que a maioria das alternativas supracitadas implica em **riscos de abuso pela autoridade pública (9x)**, por vezes conectados às possibilidade de **violação excessiva da privacidade (6x)**. Essa preocupação esteve associada sobretudo às práticas de *lawful hacking* e apreensão do dispositivo.

Nesse caso, o acesso investigativo à totalidade do dispositivo da pessoa investigada poderia resultar na coleta e análise de dados sobre uma série de atividades e interações referentes à sua intimidade e irrelevantes para a apuração dos fatos investigados.

Outra preocupação dessa natureza foi a possível **violação do devido processo legal (2x)**, pela possibilidade de busca de provas no meio de digital - abundante em informação - como um atalho investigativo, mesmo que os demais meios de produção de prova não estivessem exauridos. Na mesma ótica, foi expressa preocupação com a **vulneração de terceiros não envolvidos na investigação (x1)** e que possam ter informações e comunicações pessoais alocadas no dispositivo.

No âmbito das práticas que se baseiam em algum grau de cooperação direta com a plataforma, como escaneamento do cliente e soluções de chave fantasma ou usuário fantasma, uma percepção manifestada foi a de que tais iniciativas apresentariam **riscos similares aos do acesso excepcional via backdoor (4x)**, nas palavras de Jéssica:

> Para o direito das pessoas, sim, em uma visão mais ética, eu acho que é antiético você ter um usuário fantasma sem a pessoa ter consentido. Eu acho que é eticamente equivocado isso. Então eu vejo que isso pode ser utilizado também para, mais uma vez, violar outros direitos. Então como que eu sei se esses usuários fantasma vão ser colocados em grupos. Ele vai ser utilizado somente para fazer investigações criminais, ou para de repente começar a tentar verificar que tipos de debates estão sendo feitos para tolher a liberdade de expressão? Não sabe. Eu acho que cai no mesmo problema do acesso excepcional, essas outras questões aí.
>
> Jéssica, formação em engenharia, experiência ampla em organizações de governança da internet.

A esse respeito, dois pontos merecem destaque. Em primeiro lugar, constatou-se incerteza sobre tais soluções efetivamente não interferirem na criptografia, especialmente no contexto das soluções de chave-fantasma, que implicam em interferência no mecanismo de gerenciamento de chave, ainda que possam não alterar o processo de cifragem. Em segundo lugar, há a percepção de que mesmo que tais mecanismos preservem a criptografia no sentido estrito, eles nulificam seu propósito: desse modo, os riscos de abuso, o efeito inibitório e os danos à confiança no ecossistema digital estariam presentes da mesma forma. Alvin aborda esse problema em sua fala:

> Obviamente *ghosting* é o mesmo [que acesso excepcional] [...]. **Um princípio fundamental da criptografia é que somente as pessoas que estão participando dessa conversação acessam o conteúdo.**

> Quando tem uma terceira pessoa sem que você saiba que esta pessoa está, obviamente há uma violação da privacidade e coloca em questão o que conversávamos antes.
>
> Alvin, economista, ampla experiência nos setores público e privado. Atua no setor de políticas públicas de uma grande empresa.

Por fim, houve uma preocupação geral com a possibilidade de **vazamento de dados em poder das autoridades públicas (2x)** - dada a falta de confiança nos sistemas de segurança da informação empenhados pelo governo com os sucessivos casos de enormes vazamentos de dados dos cidadãos brasileiros. Há uma preocupação, portanto, com os parâmetros de segurança nos protocolos de arquivamento de material digital pelas autoridades.

4.3. Sobre o ambiente regulatório nacional sobre criptografia

As perguntas sobre ambiente regulatório foram respondidas por 42 entrevistados. **5 respondentes afirmaram desconhecer o ambiente regulatório nacional relativo ao tema.**

Entrevistados manifestaram o entendimento de que **a criptografia tem sua importância reconhecida e seu uso encorajado (9x),** numa visão recorrentemente positiva do ambiente regulatório brasileiro. Esse incentivo seria resultado de normas com o Marco Civil da Internet, cujo decreto regulamentador incentiva expressamente o uso de encriptação para garantia da segurança dos dados (art. 13º, inciso IV) e a LGPD, que compele os agentes de tratamento à adoção de medidas técnicas de segurança para a proteção dos dados contra incidentes (arts. 6º, incisos VII e VIII, 13º, 44º, 46º e 49º). Como argumentado por Carla:

> O que a gente tem de direitos fundamentais e de direitos em geral já serve para a gente basear e proteger o uso da criptografia. [...] eu acho que, como uma pessoa que pesquisa esse assunto e está vendo a jurisprudência e a doutrina caminhar para esse reconhecimento, **eu acredito que o que a gente tem já possibilita uma legalidade, um ambiente que favorece e entende a importância das aplicações criptográficas.**
>
> Carla, formação jurídica, atua como pesquisadora das relações entre direito e novas tecnologias.

Essa percepção se aliava à de que os **últimos anos foram marcados por avanços significativos no debate público sobre o tema (7x)**, o que foi, por vezes, exemplificado pela referência aos votos dos ministros do Supremo Tribunal Federal que relataram as ações relacionadas aos bloqueios do WhatsApp no Brasil. Também foi citada como

exemplo a decisão da Terceira Seção do Superior Tribunal de Justiça que considerou ilegal a aplicação de multa por descumprimento de ordem judicial de entrega de dados em razão de impossibilidade técnica de interceptar decorrente de criptografia. Essas decisões sinalizariam uma evolução no entendimento dos judiciário sobre o assunto.

Na trilha desse raciocínio, alguns entrevistados avaliaram que **o cenário brasileiro é mais favorável em relação à criptografia que os de diversos outros países (4x)**, haja vista que não há proibição ou restrição a seu uso e que a interação entre as normas e os desenvolvimentos jurisprudenciais supracitados resultaria num ambiente bastante favorável a essa tecnologia. Carolina traz esse argumento em perspectiva com o contexto internacional.

> Por outro lado, o fato da gente não ter a proibição, que é algo que muitos países estão sofrendo, inclusive países democráticos, **são revezes que países democráticos inclusive estão sofrendo por conta dessa agenda da segurança nacional,** países que têm histórico de terrorismo e por aí vai, nesse sentido eu acho que a gente está bem, ainda.
>
> Carolina, formação interdisciplinar, ampla experiência com advocacy em questões de tecnologia, atua com segurança digital para defensores de direitos humanos.

Por outro lado, um apontamento comum foi de que **o debate ainda precisa evoluir em conteúdo e alcance (6x)**. Esse avanço teria duas dimensões: em primeiro lugar, seria preciso amadurecer o entendimento das autoridades sobre o tema, a fim de garantir que compreendam a importância da criptografia e as consequências de seu enfraquecimento, bem como a relação entre sua proteção e a concretização dos direitos conexos positivados em nosso arcabouço. Em segundo lugar, seria importante ampliar o alcance da discussão, a fim de que a sociedade como um todo, e não apenas alguns especialistas e ativistas, compreenda, valorize e defenda a criptografia.

Nesse sentido, diversos entrevistados expressaram preocupação com o cenário presente, argumentando que **a criptografia está ameaçada (10x)**. As ameaças citadas incluem propostas de alterações legislativas que enfraqueceriam a segurança dos sistemas, como obrigações de implementar sistemas de custódia de chaves ou mecanismos de rastreabilidade de mensagens privadas encaminhadas - a exemplo do PL 2630. Também foi destacado que o STF ainda não concluiu o julgamento das ações relevantes ao tema, o que não elimina a possibilidade de consolidar um entendimento futuro que comprometa o uso da criptografia no país a despeito dos votos iniciais dos relatores das ações. Em sua fala, Paula apresenta essas preocupações:

> Mas o legislativo ainda é preocupante **porque diversos PLs buscam estabelecer mecanismos de enfraquecimento de criptografia, seja por acesso excepcional, seja por outros meios.** Então eu acho que essa pauta poderia estar melhor posicionada no Brasil.

> Em relação a nível global eu acho que a narrativa é bem parecida em muitos países, então... Países que se consideram democráticos, veem a criptografia com maus olhos. Essa semana, se não me engano foi essa semana, um comissário do RU [Reino Unido] falou que a criptografia é um dos maiores empecilhos para o combate a pedofilia. **Então, essas narrativas e esses posicionamentos vem enfraquecendo a força da criptografia como, digamos, asseguradora de direitos ao redor do mundo também. Então, é bastante preocupante** [...].
>
> Paula, formação jurídica e em área interdisciplinar, pesquisadora na área de privacidade e vigilância. Experiência na sociedade civil e academia.

Esse raciocínio também se alia à leitura de que **há pouca ou nenhuma regulação referente à criptografia no Brasil (12x)**. Essa perspectiva entende que nosso arcabouço legislativo não trata da criptografia, mas de conceitos com um grau mais elevado de abstração, como privacidade e segurança. Além disso, o país não dispõe de um ente público atuante no estabelecimento de padrões tecnológicos, como o Instituto Nacional de Padrões de Tecnologia (NIST) dos Estados Unidos.

> Bom, eu diria que em relação à criptografia, **eu diria que a gente tem quase nada de regulação.** A gente tem algumas diretrizes que dizem da importância de usar, mas acho que a gente tem muito pouco de regulação sobre a criptografia. Eu diria que eu estou bastante insatisfeita. O que numa escala de 0 a 10.. Totalmente insatisfeita seria 0, então eu diria que eu estou aí perto de 1”
>
> Nicole, formação jurídica e em ciências sociais, ampla experiência no setor privado em empresas de tecnologia, atualmente trabalha em um escritório de advocacia.

Do entendimento de que há pouca ou nenhuma regulação, dois discursos distintos emergiram.

Um deles demanda mais regulação, asseverando que **deve haver uma garantia jurídica explícita do direito ao uso de criptografia (9x)**, e sugere essa inovação normativa como um remédio contra as ameaças a esse recurso. Essa garantia poderia vir na forma de um dispositivo legal ou de uma jurisprudência oriunda de um tribunal superior que tornasse ilícita a penalização pelo emprego da tecnologia. Por esse motivo, quando perguntado sobre a satisfação com o ambiente regulatório sobre criptografia, Marco se diz pouco satisfeito.

> [...] Ao mesmo tempo que não temos nenhuma lei que proíba criptografia forte para as pessoas, a gente não tem nenhuma lei que aprove a criptografia forte para as pessoas e fale “isso daí é um direito seu”. Então acho que isso me deixa insatisfeito, que a

> criptografia forte deve ser um direito de você querer se comunicar. Um direito seu, um direito civil seu.
>
> Marco, cientista social e ativista, ampla experiência no trabalho com difusão de software livre.

Mas, além dessa demanda por uma garantia de uso, foi argumentado diversas vezes que **deveria haver uma parametrização legal da criptografia, a fim de fornecer maior segurança aos usuários (14x)**. Tal padronização poderia consistir numa obrigação de criptografar as informações imposta a certas categorias de entes públicos e privados, como autoridades de segurança pública, instituições financeiras e provedores de serviços de mensageria. Alternativamente, poderia ser instituída uma autoridade para o estabelecimento de padrões, a exemplo do NIST nos Estados Unidos.

> [...] Eu deixaria mais clara a questão da inviolabilidade dela [da criptografia]. Então, em quais casos a criptografia é essencial e não pode ser alvo de ordens judiciais para [inaudível] essa criptografia e em quais casos ela é boa, mas não essencial. **Eu diria inclusive que a criptografia fosse obrigatória para certas aplicações de internet.** Então, eu sinceramente acho que uma essencialidade dela, ou seja, quando ela é obrigatória; e um outro ponto é, quando ela pode ser relativizada.
>
> Nicole, formação jurídica e em Ciências Sociais, ampla experiência no setor privado em empresas de tecnologia, atualmente trabalha em um escritório de advocacia.

O segundo discurso, por outro lado, considera que **não é evidente que regular criptografia seja positivo (6x)** e questiona tanto a necessidade disso quanto potenciais efeitos negativos de propostas dessa natureza. Argumenta-se que o desenvolvimento e o uso da criptografia já são permitidos na medida em que não são objeto de restrição ou vedação legal. Ainda, nota que a criptografia é tanto uma técnica quanto uma ciência, de modo que regulações que incidam sobre o desenvolvimento do campo em questão podem afetar indevidamente a autonomia intelectual e o progresso científico de pesquisadores de segurança da informação. Essa preocupação aparece na fala de Cristiano, por exemplo:

> A gente não tem, então... Eu não sei se eu quero um ambiente regulatório. Eu não sei agora. Assim, depende do que quer dizer essa pergunta, porque eu não quero ninguém regulando como eu posso ou não posso deixar de usar criptografia, alguém que me diga, como tinha anos atrás. [...] **se a gente tá falando nesse tipo de coisa, que vai dizer o tamanho da chave que eu posso usar, os algoritmos que eu posso ou não utilizar em termos de limitar a força dos algoritmos**

> **que eu posso utilizar ou me obrigar a utilizar algum tipo de backdoor ou chave mestra... Esquece. Eu estou bem feliz em não ter nada.**
>
> Cristiano, cientista da computação com ampla experiência no campo da segurança da informação na academia e no setor privado.

O principal fundamento do discurso contrário a propostas regulatórias que tratam expressamente da criptografia é a percepção de que a **neutralidade tecnológica é positiva e deve ser preservada (4x)**. Assim, o fato de os instrumentos presentes não abordarem expressamente a criptografia seria uma virtude, não um defeito. Uma vez que não é possível prever os desenvolvimentos tecnológicos das próximas décadas, qualquer norma que incida sobre tecnologias específicas tem o potencial de obsolescência acelerada, mesmo aquelas que presentemente poderiam parecer positivas, como o estabelecimento de um dever de uso da criptografia.

> **O problema de você regular muito é que, na computação como um todo, né, ela muda muito, muda diariamente.** Se você atende a um padrão mínimo você pode ficar confortável né, mas passou um ano, dois, às vezes aquele padrão está desatualizado e você vai apresentar um certificado de que está em conformidade, e pode até não ser punido mas o sistema vai ser invadido do mesmo jeito, né.
>
> Sérgio, formação em Ciência da Computação. Servidor público federal e pesquisador.

4.4. Sobre os bloqueios do WhatsApp e sua relação com o Marco Civil da Internet

A pergunta sobre a avaliação dos bloqueios do WhatsApp foi respondida por 41 dos 43 entrevistados. A pergunta sobre o Marco Civil da Internet autorizar ou não tais medidas foi respondida por 23 deles.

Uma percepção frequente entre os entrevistados foi de que **os bloqueios judiciais do WhatsApp no Brasil foram ilegítimos (17x)**.

Uma das razões para tal avaliação foi de que os bloqueios se fundamentaram em **interpretações inadequadas do Marco Civil da Internet (11x)**, especialmente de seu capítulo III, seção II, que versa sobre a proteção de registros, dados pessoais e comunicações privadas. Sob esse ponto de vista, essa seção conteria **sanções aplicáveis somente a provedores que violassem as garantias da privacidade e da proteção dos dados dos usuários (11x)**. Na ocasião dos bloqueios, esse requisito não estaria presente, pois o descumprimento de comando judicial de compartilhamento de dados com as autoridades para fins de persecução penal não corresponderia a uma violação a tais direitos.

> Totalmente ilegítimos, porque primeiro que foi um caso de interpretação totalmente equivocada do MCI. Existia um dispositivo nos artigos 11 e 12 que trazia **sanções que deveriam ser aplicadas no contexto em que o controlador de dados - embora o MCI não use o termo controlador de dados, o contexto é esse - [...] esteja operando e ele não garanta os princípios da privacidade**. E aí, pelo uso incorreto, ele poderia vir a ser sancionado.
>
> Ian, formação jurídica e na área computacional, ampla experiência no setor público.

Pelo contrário, quando esse descumprimento resultasse da incapacidade operacional de produzir a informação solicitada em razão da criptografia, a incapacidade de observar a ordem judicial resultaria precisamente do cumprimento do dever de garantir a segurança dos dados. Adicionalmente, nesse caso, a sanção ao provedor seria ilegítima porque **tal entrave técnico tornaria o cumprimento da ordem original impossível (6x)**. Desse modo, a obrigação de cumprí-la seria similar à obrigação de produzir uma prova diabólica, além de representar uma penalização da própria ferramenta.

A eficácia material dos bloqueios também foi avaliada negativamente pelos entrevistados, que os consideraram **ineficazes devido à possibilidade de contorná-los por meio de redes privadas virtuais (*Virtual Private Networks* - VPNs)**[53] **(4x)**.

Nessa ótica, foram tecidas críticas a um **desconhecimento das autoridades judiciais sobre o funcionamento da tecnologia (8x)**. Desse desconhecimento sobre a criptografia adviria uma expectativa, por parte dos decisores, de acesso facilitado aos conteúdos das comunicações privadas como um **atalho nas investigações criminais (2x)**, bem como uma frustração quando da não concretização dessa expectativa.

Independentemente da interpretação do Marco Civil da Internet, contudo, a principal razão para a avaliação negativa dos bloqueios foi o entendimento de que **os danos decorrentes da medida foram desproporcionais (22x)**. Os direitos de dezenas de milhões de usuários do aplicativo foram atingidos, ocasionando, inclusive, **danos econômicos a esses usuários (6x)**. Essa desproporcionalidade tornaria os bloqueios ilegítimos independentemente do conteúdo do Marco Civil da Internet, uma vez que afrontaria diretamente preceitos constitucionais como liberdade de expressão e livre-iniciativa.

Na mesma seara, **a competência do Poder Judiciário brasileiro para determinar unilateralmente os bloqueios foi questionada (2x)** em razão da medida ter atingido usuários em outros países da América Latina, representando uma extrapolação indevida da jurisdição brasileira.

53 Recurso tecnológico que estabelece uma conexão de rede privada criada sobre uma infraestrutura de rede pública. O uso de VPNs permite que o usuário cifre seu tráfego e oculte sua identidade e sua localização online.

> [...] E também do ponto de vista social, é uma decisão muito drástica, porque o Whatsapp é um dos meios de comunicação mais utilizado pelos brasileiros. **Isso tem consequências negativas tanto para as pessoas que estão utilizando esses aplicativos, para o trabalho, para falar com seus familiares, como também até mesmo econômicas, porque tem gente que depende disso para conseguir vender marmita, vender...** não sei, coisas que ela tem ali, os contatos e que dependem disso para fazer atividades diárias. Então esse nível de bloqueio é tão drástico que tem efeitos bastante negativos para as pessoas como um todo. Acho que é uma decisão bastante equivocada.
>
> Laura tem formação jurídica. Experiência com pesquisa e ativismo envolvendo tecnologia e sociedade no terceiro setor.

Além do debate sobre o mérito dos episódios, os entrevistados também refletiram sobre suas causas concretas, em geral atribuindo-os a uma **disputa política entre o Facebook e as instituições do sistema de justiça criminal brasileiro (10x)**. Foi recordado que a primeira ordem de compartilhamento de dados cujo descumprimento resultou no bloqueio precedeu a implementação da criptografia de ponta-a-ponta, sendo seu descumprimento atribuído à negligência da empresa para com as autoridades nacionais. Tal negligência teria ocasionado uma reação de reafirmação da soberania nacional por meio da determinação dos bloqueios, de modo a compelir as empresas à observância do cenário nacional.

> Então esses bloqueios acabaram acontecendo por um desrespeito de uma empresa que vem trabalhar no Brasil, que tem escritório no Brasil, que é o escritório de marketing do Facebook e que ganha dinheiro no território nacional a partir dos dados colhidos das pessoas em território nacional e que **não se preocupou em ter um departamento jurídico à altura para dar o atendimento para a justiça no Brasil.**
>
> Natália, formação jurídica, atua no sistema de justiça criminal, com foco em crimes cibernéticos.

> Se a criptografia é legal no país, e seu uso não é proibido, é preciso que se aceite de fato a incapacidade técnica de entregar esse tipo de conteúdo. [O] que a justiça brasileira encenou naquela ocasião foi uma queda de braço com as empresas que não teve bons resultados. Não teve bons resultados nem pro caso específico, nem pra questão regulatória mais ampla. **Sendo a criptografia legal, não acho que as**

> **empresas estejam nesse caso equivocadas ou resistindo a uma ordem judicial. Elas estão preservando a integridade de um sistema que se apoia no uso de criptografia.**
>
> Tatiana, formação jurídica, ampla atuação na sociedade civil com defesa dos direitos humanos, pesquisadora em privacidade e segurança.

Com menor frequência, houve entrevistados que consideraram que **os bloqueios foram legítimos (6x)**.

A primeira tese a esse respeito afirmou que o **art. 11 fundamenta os bloqueios ao condicionar o tratamento de dados à observância da legislação brasileira (3x).** Segundo esse raciocínio, o descumprimento de uma ordem judicial legítima de compartilhamento dos dados implica em descumprimento da legislação brasileira, uma vez que a ordem em questão se alicerça em normas que compõem o arcabouço legal nacional.

Para esses entrevistados, o primeiro bloqueio é especialmente relevante, uma vez que a empresa não podia alegar que o uso de criptografia representasse um impedimento técnico ao cumprimento da ordem. Assim sendo, a opção pela inobservância da ordem não representaria somente um desafio político à autoridade do Poder Judiciário nacional, mas uma efetiva violação da ordem legal brasileira. Assim sendo, constituiria infração ao art. 11 do Marco Civil, o que atrairia a aplicação das sanções previstas em seu artigo 12, entre elas, a suspensão e a proibição das atividades que envolvem os atos previstos no art. 11.

> Eu entendo que sim, que ele autoriza sim, porque quando ele fala... [...] 'em qualquer operação de coleta, armazenamento, guarda e tratamento ou de comunicações 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'. Então a gente entende que **no art. 11, se todos esses atos - está bem claro aqui -, eles devem obedecer à legislação brasileira, qualquer ordem judicial que determine o afastamento do direito à privacidade ou a proteção... para se afastar esse direito da privacidade ou para se afastar o sigilo de comunicações, tem que ser obedecida a legislação brasileira.** Quando fala isso, já significa que as sanções pelo não cumprimento da ordem judicial [são aplicáveis]. Isso [o não cumprimento da ordem] já é o descumprimento da legislação brasileira. É isso que a gente entende.
>
> Natália tem formação jurídica e atua no sistema de justiça criminal, com foco em crimes cibernéticos.

Alternativamente, outra tese entendeu que **os bloqueios poderiam ser determinados independentemente do Marco Civil da Internet em virtude do poder geral de cautela do juiz (3x)**. Enquanto garantia da efetividade processual, tal figura implica que o magistrado tem o dever-poder de conceder medidas cautelares atípicas - não previstas na norma legal - na ocasião em que as medidas previstas não sejam adequadas ou suficientes ao caso concreto. Sob esse ponto de vista, o caso em discussão acionaria tal prerrogativa, sobretudo em razão de medidas anteriores já terem sido determinadas e a empresa ter se recusado a aquiescê-las, além de se tratar de crimes graves - tráfico de drogas.

> Eu entendo que o Marco Civil tem lá as sanções, que ele não informa quem vai aplicar e o poder judiciário tem se utilizado desse artigo para justificar os bloqueios. **Mas meu entendimento também é que o poder judiciário poderia determinar bloqueios sem [o] Marco Civil, porque existe um poder geral de cautela do juiz para determinar as medidas necessárias para a obtenção de material probatório ou eficácia de suas decisões que poderia ser invocado sem qualquer necessidade do marco civil.** Tanto é assim, que quando houve a discussão no STF, [...] não havia necessidade de declaração de inconstitucionalidade daqueles dispositivos porque com eles ou sem eles o Poder Judiciário poderia ter tomado aquelas medidas. E a gente vai discutir se isso é legítimo ou não à luz da constituição, é uma outra discussão. Mas em termos de marco normativo mesmo, eu acho que tanto faz o marco civil dizer ou não dizer. Eu acho que a discussão é realmente de parâmetros constitucionais, de controle das decisões judiciais e não particularmente da redação do marco civil.
>
> Silvana tem formação interdisciplinar na área jurídica e no campo da comunicação e ampla experiência no setor público.

5. Análise e discussão

Esta seção discute o conteúdo de alguns dos enunciados extraídos das entrevistas. Cada uma das suas subseções se debruça sobre um dos temas relatados na seção anterior. Somente os enunciados relativos à percepção sobre o ambiente regulatório não são discutidos, haja vista que tal ambiente já foi caracterizado objetivamente nas seções 2.4.2 e 2.4.3 deste estudo.

5.1. Sobre o acesso excepcional

O apoio à inserção de mecanismos de acesso excepcional entre nossos entrevistados foi justificado a partir de um raciocínio jurídico-político cuja premissa é a prioridade da

segurança pública sobre outros direitos ameaçados pela medida. Considera-se que, se garantir a segurança pública exige acessar comunicações privadas e há casos previstos em lei para que esse acesso ocorra, é inaceitável que a lei não seja cumprida. Nessa lógica, os riscos resultantes do acesso são vistos como um ônus indesejado, porém necessário, uma espécie de "mal menor" se a alternativa é o descumprimento da lei e o impedimento das investigações. De todo modo, os riscos de abuso poderiam ser prevenidos por garantias institucionais, como controle judicial e a reserva desse acesso a casos realmente excepcionais: investigações de crimes graves em que outros meios investigativos foram exauridos. Por fim, seria necessário confiar nas instituições por princípio.

A controvérsia jurídica evocada por esse ponto de vista não se limita à questão do dever de interceptar, mas implica num debate sobre a existência ou não de um dever de produzir uma arquitetura tecnológica que viabilize a interceptação. Como observa Jacqueline Abreu[54], raciocínios como esse "parecem querer extrair da própria previsão legal no direito brasileiro de *procedimentos de quebra de sigilo* o dever de que a *habilidade de quebra de sigilo* sempre exista". Para a autora, embora a existência desse dever seja patente no setor de telecomunicações em razão de diversas resoluções da Agência Nacional de Telecomunicações que o prevêem expressamente[55], não se pode concluir que se estenda às empresas de tecnologia e provedoras de aplicações de internet, uma vez que tais empresas não são concessionárias de serviço público e, portanto, restam fora do escopo de entidades sujeitas às resoluções supracitadas.

O Marco Civil da Internet, por sua vez, se restringe a compelir as empresas à guarda dos metadados relativos a IP, data e hora de acesso. Assim sendo, o dever jurídico de ter a habilidade de quebrar o sigilo das comunicações "não é evidente; carece de fundamentação — e pode muito bem ser que a conclusão seja de que não exista"[56]. A questão colocada, portanto, é se tal dever deveria passar a existir, o que evoca considerações sobre seus benefícios e danos. Na racionalidade valorativa que alicerça a defesa do acesso excepcional no material empírico examinado, o cálculo é nítido: os custos de obstaculização da persecução penal superam significativamente os riscos e danos decorrentes do enfraquecimento criptográfico, em especial porque tal ponto de vista se alicerça numa confiança principiológica na capacidade efetiva das instituições para coibir abusos de poder.

Cumpre notar, contudo, que tal confiança se apoia fundamentalmente em considerações referentes a controles institucionais sobre abusos intencionais pela autoridade pública. No entanto, não é discutido o risco de usurpação da falha de segurança por terceiros

54 ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42. p. 32

55 As normas mais relevantes nesse sentido seriam as Resoluções nº 73/1998 (Regulamento dos Serviços de Telecomunicações), nº 426/2005 (Regulamento do Serviço Telefônico Fixo Comutado), nº 477/2007 (Regulamento do Serviço Móvel Pessoal) e nº 614/2013 (Regulamento do Serviço de Comunicação Multimídia)

56 ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42. p. 34

maliciosos, como criminosos cibernéticos ou governos estrangeiros.

Perspectiva divergente é oferecida pelo discurso contrário ao acesso excepcional, que apresenta dois eixos: a ênfase nos danos decorrentes da medida nos âmbitos técnico, jurídico-político e econômico e o questionamento de sua necessidade e de sua eficácia. O primeiro eixo assevera que uma vez introduzida a vulnerabilidade, ela será passível de uso indevido por criminosos e governantes maliciosos. Isso causaria uma série de repercussões indesejáveis, entre as quais se destacam a redução da segurança e da confiança no ambiente digital, a violação aos direitos dos usuários e a imposição de ônus econômicos substanciais aos provedores.

As preocupações relativas à segurança da informação são amparadas pelo consenso científico atual no campo da segurança da informação, que atesta a impossibilidade de assegurar somente a exploração lícita e legítima da referida vulnerabilidade. Ainda, os requisitos de escalabilidade associados a sistemas de custódia de chave impõem a necessidade de reversão de melhores práticas de segurança - a exemplo do *forward secrecy*, arranjo em que as chaves de decifragem são substituídas imediatamente após cada uso, a fim de reduzir os danos de seu eventual comprometimento[57]. Nesse sentido, a redução de segurança resultante da vulnerabilidade seria agravada porque a reversão correlata dessas boas práticas implicaria num aumento dos ganhos de um eventual atacante, o que ampliaria os incentivos para que a exploração da falha se concretizasse.

As preocupações jurídicas e políticas, por sua vez, se alinham aos entendimentos dos relatores das ações relativas aos bloqueios do WhatsApp no Supremo Tribunal Federal, bem como ao crescente reconhecimento internacional de que a criptografia é necessária para a proteção dos direitos à privacidade e à liberdade de expressão[58]. Mas para além da reflexão abstrata, os apontamentos dos entrevistados a esse respeito devem ser entendidos no contexto do cenário jurídico-político brasileiro, entre elas, um ceticismo referente à capacidade das instituições de coibir abusos e uma percepção de que haveria banalização das quebras de sigilo na justiça criminal brasileira.

Quanto ao ceticismo institucional, o exame do ambiente político brasileiro oferece elementos para a apreciação de sua pertinência. Em relatório conjunto[59] sobre o ambiente político e tecnológico brasileiro no ano de 2020, o Centro de Análise da Liberdade e do Autoritarismo (LAUT) e a Associação Data Privacy Brasil de Pesquisa (DPBR) identificam treze iniciativas estatais que favorecem o uso de tecnologias de informação e comunicação para ampliar indevidamente a vigilância e o controle estatal sobre a população, colocando em risco liberdades democráticas. Entre as medidas

57 ABELSON, Hal *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. **Journal of Cybersecurity**, v. 1, n. 1, p. 69-79, 2015. p.69.

58 HOBOKEN, J. V.; SCHULZ, W. **Human rights and encryption**. Paris: UNESCO, 2016.

59 ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO (LAUT). Retrospectiva - Tecnoautoritarismo 2020. **LAUT,** 2021. Disponível em: https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf. Acesso em: 04/08/2021.

examinadas estiveram autorizações de quebras de sigilos de dados cadastrais sem ordem judicial, a construção de dossiês sobre indivíduos denominados "antifascistas" e o monitoramento e classificação de jornalistas, parlamentares e formadores de opinião de acordo com sua posição ideológica. Tais ponderações também são amparadas por outros levantamentos[6061], que evidenciam uma tendência progressiva à criminalização e restrição do direito ao protesto no país desde 2013.

Quanto à questão específica sobre a existência de uma tendência judicial à banalização das quebras de sigilo, sua aferição encontra obstáculos metodológicos. A Resolução CNJ nº 59/2008 determina que todas as varas criminais do país forneçam informes regulares sobre os pedidos de interceptação de comunicações e as decisões de quebra de sigilo. Parte desses dados é exibida em formato agregado por meio do Sistema Nacional de Controle de Interceptações Telefônicas[62]. No entanto, o sistema só exibe o número de decisões por tribunal, segmento judicial e tipo de decisão, de modo que não é possível aferir sequer o percentual de pedidos deferidos e rejeitados. Ainda que o fosse, isso não resolveria a questão, que possui uma dupla dimensão. Do ponto de vista descritivo, seria necessário mapear que condições empíricas têm sido interpretadas como suficientes para a contemplação dos requisitos previstos na Lei 9296. Do ponto de vista normativo, seria preciso avaliar se tais interpretações são razoáveis no que tange às garantias processuais. Análises de conteúdo jurisprudencial poderão explorar essa lacuna no debate.

É importante notar, contudo, que houve um aumento percentual extremo no número de decisões de quebra de sigilo telemático nos últimos cinco anos: em todo o ano de 2015, foram produzidas 1943 decisões dessa natureza, contra 6.898 somente nos seis primeiros meses de 2020, representando um aumento percentual de 255%. Esse crescimento já seria notório em si mesmo, mas a ausência de dados sobre a segunda metade de 2020 sugere que ele seja significativamente maior. Ainda a esse respeito, pesquisadores do InternetLab[63] observam que os números apresentados no sistema podem não revelar a grandeza real do volume de interceptações, haja vista que já houve discrepância histórica entre as informações presentes no sistema e dados oriundos do setor privado: em 2016, o relatório de transparência da empresa Telefónica (que operava como Vivo no Brasil) informava ter recebido 326.811 requerimentos de interceptações no Brasil em 2015, um número que ultrapassa tanto o número de ofícios expedidos a empresas (95.481) quanto a soma de telefones e telefones-VOIP interceptados naquele ano (294.217) segundo os dados do SNCI.

60 ALMEIDA, Frederico de. MONTEIRO, Filipe Jordão; SMIDERLE, Afonso.a criminalização dos protestos do movimento passe livre em são paulo (2013-2015). **Revista Brasileira de Ciências Sociais** [online]. v. 35, n. 102, 2020.

61 ARTIGO 19. **As restrições ao direito de protesto no Brasil**. 5 anos de junho de 2013: Como os três poderes intensificaram sua articulação e sofisticaram os mecanismos de restrição ao direito de protesto progressivamente. Artigo 19, 2018. Disponível em: https://artigo19.org/5anosde2013/. Acesso em: 04/08/2021.

62 BRASIL. Conselho Nacional de Justiça (CNJ). Sistema Nacional de Controle de Interceptações Telefônicas. **CNJ**, Brasília, 2021. Disponível em: https://www.cnj.jus.br/sistemas/sistema-nacional-de-controle-de-interceptacoes-telefonicas/. Acesso em: 04/08/2021.

63 ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. p. 44-45

Para os pesquisadores:

> Tudo isso aponta que os números relativos a interceptações no Brasil merecem um estudo próprio. Se se revelarem altos, podem sugerir, de um lado, que a proteção teórica pretendida pela necessidade de ordem judicial e pela previsão de requisitos mais rigorosos para realização desse procedimento na Lei de Interceptações não se reflete na prática. De outro, pode também apontar para deficiências estruturais nas capacidades investigativas da polícia judiciária, fazendo com que esta seja fortemente dependente desse meio agressivo de instrução probatória. Não são poucas as manifestações no sentido de que autoridades de segurança pública recorrem a medidas de interceptação e de quebra de sigilo como *prima ratio*.

Ainda sobre a cultura de interceptações no Brasil, o relatório do InternetLab recorda que o Brasil já foi condenado pela Corte Interamericana de Direitos Humanos por conduzir interceptações telefônicas irregularmente sobre as comunicações de trabalhadores rurais do Movimento Sem-Terra. A irregularidade decorreu das interceptações terem sido autorizadas pela Polícia Militar - que não era competente para fazê-lo -, sem notificação ao Ministério Público e fora do âmbito de uma investigação criminal[64] em andamento. Cumpre notar que as autoridades responsáveis pelo ilícito não foram responsabilizadas.

As preocupações quanto aos impactos negativos sobre a confiança e a economia digital, por fim, também demandam testes empíricos. A esse respeito, convém citar a pesquisa conduzida pelos pesquisadores do Law & Economics Consulting Associates e comissionada pela Internet Society sobre o tema[65]. O trabalho investigou os custos e benefícios potenciais da Lei de Alteração das Telecomunicações e de Outras Legislações (de Assistência e Acesso) (LATO) aprovada na Austrália em 2018. Essa norma compele provedores de tecnologia da informação a auxiliar as autoridades no acesso ao conteúdo de dados cifrados, inclusive mediante alterações na arquitetura de seus sistemas. A pesquisa articulou entrevistas em profundidade conduzidas com os 9 principais provedores multinacionais atuantes no país à aplicação anônima de um questionário a outros 79 provedores.

O estudo concluiu que a LATO teria uma série de impactos negativos potenciais sobre os provedores e seus clientes. Destacam-se, a esse respeito, a ampliação da incerteza no ambiente de negócios, danos à imagem da marca dos provedores vulneráveis ao enfraquecimento de seus serviços e redução da confiança no ambiente digital. Esse

64 Conferir MASI, Carlos Velho. O caso Escher e outros v. Brasil e o sigilo das comunicações telefônicas. **Revista dos Tribunais**, v. 932, Junho de 2013, pp. 309-352

65 BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. O impacto econômico das leis que enfraquecem a criptografia. **Law & Economics Consulting Associates** (LECA). Tradução de Paulo Renã da Silva Santarém. 2021. Disponível em: https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia .Acesso em: 04/08/2021.

último aspecto pode implicar na diminuição da demanda agregada, o que incentivaria as empresas a assumirem custos mais elevados a fim de minimizar os danos. Mais estudos são necessários para precisar a extensão desses danos e verificar se outras legislações com disposições análogas produzem efeitos similares em outras jurisdições.

O segundo eixo do discurso contrário ao excesso excepcional, por sua vez, consiste no questionamento dos benefícios alegados dessa medida: sua necessidade e sua eficácia não teriam sido demonstradas empiricamente de forma conclusiva e seria provável que dela resultasse a migração dos criminosos para outras plataformas. Conjugado ao eixo anterior, esse discurso entende o acesso excepcional como uma medida desproporcionalmente danosa e potencialmente ineficaz. A primeira alegação é amparada pela ausência de dados ou estudos que avaliem o efeito da implementação de criptografia forte em plataformas e dispositivos sobre os índices de sucesso na resolução de investigações criminais. A segunda, por sua vez, exige novos estudos, que deverão investigar os efeitos da implementação de mecanismos de acesso excepcional sobre a atividade criminosa em plataformas.

5.2. Sobre as alternativas ao acesso excepcional

Quanto a possíveis métodos ou técnicas alternativas para facultar às autoridades o acesso às informações demandadas sem comprometimento da criptografia, percebeu-se que dois conjuntos principais de soluções potenciais foram levantados: um baseado na quebra da segurança das informações em uma das pontas pela autoridade estatal e outro baseado na cooperação com as empresas provedoras de tecnologia em que as informações estão armazenadas ou são comunicadas.

No primeiro conjunto, foi levantada inicialmente a possibilidade de apreensão e desbloqueio dos dispositivos relevantes. Se, por um lado, tal solução oferece o benefício de não interferir na criptografia empregada no sistema, é preciso reconhecer que carrega em si mesma repercussões significativas sobre os direitos dos cidadãos, sobretudo no que tange à proteção de dados pessoais armazenados em dispositivos e às condições de afastamento legítimo do sigilo de dados estáticos. Tais impactos foram notados pelos entrevistados, que expressaram a preocupação com a possibilidade de violação excessiva da intimidade na medida em que os dispositivos móveis de um indivíduo presumivelmente contêm informações que extrapolam em muito o que é relevante para as investigações.

Coloca-se, então, a questão da legitimidade do compelimento judicial à entrega de senha. A esse respeito, a sexta turma do STJ firmou entendimento de que o chamamento judicial ao desbloqueio do dispositivo é legítimo. Porém, inexiste obrigação de informação da senha por parte do investigado em virtude do postulado constitucional de vedação

à autoincriminação[66]. Em reconsideração de voto, o relator, ministro Nefi Cordeiro, considerou que "é válida a ordem judicial de entrega das senhas dos dispositivos eletrônicos apreendidos, mas o réu não é obrigado a fornecer essas senhas, e nem deve sofrer sanções".

Em conformidade a esse precedente, portanto, o acesso ao conteúdo do dispositivo apreendido demandaria o recurso a métodos e ferramentas voltadas à segurança ofensiva. Isso levanta o debate sobre o uso de *lawful hacking* ou *hacking governamental* para comprometimento de uma das pontas do canal criptografado. Como evidenciado pela análise das entrevistas, embora esses termos sejam usados genericamente para designar o uso de recursos e métodos voltados à exploração de vulnerabilidades, o universo de recursos e métodos pode variar enormemente, uma vez que o conceito abarca abordagens tão distintas quanto engenharia social e o uso de *spyware* para obtenção do acesso alvejado.

Uma vez que não gozam de previsão expressa no direito processual penal brasileiro, as práticas de *hacking* governamental vêm sendo discutidas primariamente no Poder Legislativo, onde foi estabelecido um grupo de trabalho destinado à elaboração de um anteprojeto de reforma do Código de Processo Penal. No texto substitutivo que vem fundamentando os trabalhos do referido GT até a data de finalização deste paper[67], a matéria é contemplada em duas hipóteses de obtenção de prova: a "coleta remota, oculta ou não, de dados em repouso acessados à distância" e a "coleta por acesso forçado de sistema informático ou de redes de dados".

O teor genérico dessa proposições faz ecoar preocupações descritas na relatoria de acompanhamento sobre criptografia e anonimato publicada pelo Relator Especial das Nações Unidas (ONU) para a Liberdade de Opinião e Expressão em 2018. O documento alerta para uma tendência dos Estados a normatizar as práticas de *hacking* através de autorizações legais redigidas em "linguagem vaga e ambígua, fornecendo às autoridades amplos poderes com supervisão externa mínima"[68]. A fim de abordar tais riscos, a relatoria recomenda que o recurso ao *hacking* governamental seja autorizado somente em circunstâncias excepcionais, observados os requisitos de legalidade, necessidade, proporcionalidade e finalidade legítima, cuja existência deve ser atestada casuisticamente

66 BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 580.664 - RJ**. Rel. Ministro Nefi Cordeiro. Brasília, 20 out. 2020. Disponível em:https://stj.jusbrasil.com.br/jurisprudencia/1206242995/habeas-corpus-hc-580664-rj-2020-0111177-4/inteiro-teor-1206243005 . Acesso em: 05 ago. 2021

67 BRASIL. Câmara dos Deputados. **Parecer do Relator, Dep. João Campos (REPUBLIC-GO) da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 8045, de 2010, do Senado Federal, que trata do "Código de Processo Penal" (revoga o Decreto-Lei nº 3.689, de 1941. Altera os Decretos-Lei nº 2.848, de 1940; 1.002, de 1969; as Leis nº 4.898, de 1965, 7.210, de 1984; 8.038, de 1990; 9.099, de 1995; 9.279, de 1996; 9.609, de 1998; 11.340, de 2006; 11.343, de 2006), e apensados ao Projeto de Lei nº 8.045, de 2010**. Portal da Câmara dos Deputados. Brasília, 26 abr. 2021. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/gt-anteprojeto-do-novo-codigo-de-processo-penal/documentos/outros-documentos/substitutivo-relator-joao-campos. Acesso em: 05 ago. 2021. p. 481.

68 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponível em:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acesso em: 05 ago. 2021. p. 8.

por um órgão judicial independente e imparcial[69].

Similarmente, um relatório produzido pelo centro de referência em direitos digitais *Access Now* sobre a matéria, em 2016[70], recomenda uma proibição preventiva do *hacking* governamental em razão de seus riscos para os direitos humanos. O documento recomenda que eventuais autorizações aquiesçam a parâmetros de notificação do usuário, transparência, supervisão pública, integridade de sistemas, cooperação internacional, remédio efetivo e salvaguardas contra o acesso ilegítimo, em adição aos propostos pela relatoria da ONU.

O segundo conjunto principal de alternativas à criptografia difere do primeiro na medida em que se apoia em práticas de cooperação com a plataforma. Nesse âmbito, as principais possibilidades levantadas foram o uso de métodos de usuário ou chave fantasma e de sistemas de escaneamento do cliente (*client-side scanning*).

O debate sobre propostas de usuário ou chave fantasma ganhou tração recente em decorrência de um artigo publicado por dois diretores técnicos do *Government Communications Headquarters*, principal autoridade do Reino Unido[71]. Os autores defendem que a adição velada de um terceiro às conversas dos investigados como mecanismo para o acesso a informações necessárias às investigações não interferiria na criptografia, o que faria dela uma saída viável para o debate sobre *Going Dark*.

A proposta repercutiu negativamente na comunidade da segurança da informação, resultando em uma carta aberta[72] de resposta assinada por 23 organizações da sociedade civil do campo dos direitos digitais, 7 empresas de tecnologia e comércio e 17 especialistas em segurança digital e sua governança globalmente reconhecidos no campo acadêmico. Na carta, os signatários afirmam que a proposta de chave fantasma "criaria riscos de segurança digital ao minar sistemas de autenticação criptográfica, introduzir vulnerabilidades potenciais e criar novos riscos de abuso e uso indevido desses sistemas" (tradução livre). Tal posicionamento foi reiterado em uma planilha de fatos sobre a proposta produzida pela *Internet Society*[73]. Similarmente, um artigo de opinião escrito pelo cientista da computação e jurista Ross Schulman questionou a premissa fundamental de que tal método não representaria uma interferência na criptografia. Em suas palavras:

---

69 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponível em:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acesso em: 05 ago. 2021. p. 18.

70 STEPANOVICH, Amie et al. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em:https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Acesso em: 05 ago. 2021.

71 LEVY, Ian. ROBINSON, Crispin. Principles for a More Informed Exceptional Access Debate. **Lawfare - Hard National Security Choices**, 29 nov. 2018. Disponível em: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate . Acesso em 05 ago. 2021.

72 BRADFORD, Sharon. THOMPSON, Andi Wilson. Open Letter to GCHQ on the Threats Posed by the Ghost Proposal. **Lawfare - Hard National Security Choices**, 30 mai. 2019. Disponível em: https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal. Acesso em: 05 ago. 2021.

73 INTERNET SOCIETY. Fact Sheet: Ghost Proposals. **Internet Society**, 24 mar. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/. Acesso em: 06 ago. 2021.

> Em sua proposta, Levy e Crispin afirmam que a proposta de chaves fantasmas não "tocaria" na criptografia. Essa afirmação simplesmente não é verdadeira segundo nenhuma definição normal de "criptografia". Enquanto o método proposto pode nem sempre envolver modificações nos algoritmos criptográficos fundamentais [...], ele iria requerer "tocar" e modificar as chaves criptográficas. Os processos de distribuição e autenticação das chaves são em si mesmos partes integrais da totalidade do sistema criptográfico. Enfraquecê-los tem um impacto similar a enfraquecer o próprio algoritmo no tocante à segurança[74] (tradução livre).

O autor observa que a implementação desses serviços exigiria alterações nos sistemas em escala massiva para produzir um mecanismo de adição de chave a ser ativado em dispositivos específicos sob demanda. Os impactos resultantes seriam similares aos de um sistema de custódia de chaves: aumento da complexidade do sistema e redução correlata de sua segurança, possibilidade de exploração por terceiros maliciosos e redução da confiança na plataforma. Por essas razões, conclui-se que as propostas de implementação de usuário ou chave fantasma constituem outro mecanismo de acesso excepcional e comportam riscos e problemas técnicos, sociais, jurídicos, políticos e econômicos análogos.

Outra alternativa baseada na cooperação com as provedoras de dispositivos e canais são os sistemas de escaneamento do cliente, por vezes também designados como filtragem na ponta (*endpoint filtering*). A proposta também foi objeto de críticas na comunidade de segurança da informação nos últimos anos. Em uma planilha de fatos divulgada sobre o assunto, a *Internet Society*[75] observou que a proposta elevaria a complexidade do sistema, ampliando a superfície de ataque explorável por atacantes maliciosos. Eles poderiam monitorar e interferir nas comunicações dos usuários a partir da manipulação da base de dados de conteúdo danoso. Ainda, alertava para a possibilidade de eventuais usos abusivos dessa capacidade, como a censura política da comunicação de conteúdos legítimos.

Em um posicionamento público sobre o tema, a *Electronic Frontier Foundation* alertou para outros problema relacionados à proposta[76]: a base de dados provavelmente seria armazenada no servidor, que tenderia a ser informado dos identificadores de cada imagem enviada pelo usuário. Uma vez que tal sistema fosse implementado, funcionalidades análogas poderiam ser-lhe incorporadas para facultar acesso a conteúdos textuais à guisa

74 SCHULMAN, Ross. Why the Ghost Keys 'Solution' to Encryption is No Solution. **Just Security**, 18 jul. 2019. Disponível em: https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/. Acesso em: 05 ago. 2021.

75 INTERNET SOCIETY. Fact Sheet: Client-Side Scanning. **Internet Society**, 24 mar. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/. Acesso em: 06 ago. 2021.

76 PORTNOY, Erica. Why Adding Client-Side Scanning Breaks End-To-End Encryption. **Electronic Frontier Foundation**, 1 nov. 2019. Disponível em: https://www.eff.org/pt-br/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption. Acesso em: 06 ago. 2021.

do combate à desinformação. O potencial de utilização desse tipo de mecanismo para acesso a conteúdos de comunicações implicaria num incentivo contínuo à ampliação indevida da base de dados. No limite, a totalidade do dicionário poderia ser incorporada a essa base, efetivamente possibilitando a decifragem total das mensagens e nulificando o propósito da criptografia.

Com relação aos metadados, o debate sobre seu acesso tem sido um ponto de menor controvérsia jurídica. O regime de guarda de dados estabelecido pelo Marco Civil da Internet parametriza as informações que devem ser armazenadas pelos provedores de serviços de internet, os quais podem ser acessados pelas autoridades competentes mediante determinação judicial. Em conformidade à lógica de minimização do tratamento de dados associada ao princípio da necessidade da LGPD, a coleta e o armazenamento dos dados pessoais, inclusive metadados sobre contas e comunicações, deve se limitar ao mínimo necessário para a realização dos objetivos do tratamento.

Ademais, especialistas têm alertado para riscos associados à construção de grafos sociais projetados a partir de metadados, como sua monetização indevida por plataformas e o uso para mapeamento de redes sociais de dissidentes políticos, jornalistas e ativistas[77]. No contexto tecnoautoritário descrito previamente, tais preocupações adquirem maior gravidade, o que reforça a necessidade de minimização na coleta e armazenamento dos metadados e a coerência dos parâmetros determinados pelo Marco Civil da Internet com tal perspectiva precaucionária.

Por outro lado, ante a pressão pela moderação de conteúdos em ambientes criptografados, alguns estudiosos têm considerado a análise de metadados como uma alternativa menos invasiva que as demais. Em um relatório recente sobre o tema[78], o *Center for Democracy and Technology* considerou tal método como apto a preservar a privacidade do usuário e a criptografia, desde que a análise ocorra exclusivamente no dispositivo do usuário e não implique em acesso a conteúdos decifrados.

Para além desses apontamentos relativos a propostas específicas, o exame dos enunciados dos entrevistados acerca das alegadas alternativas ao acesso excepcional evidencia uma racionalidade sociotécnica que reconhece as estruturas técnicas dos sistemas criptográficos como indissociáveis das conotações políticas que adquiriram ao longo dos anos no que tange à defesa dos direitos humanos, como privacidade e liberdade de expressão. Por esse motivo, as alegadas alternativas - a exemplo do escaneamento do cliente e da análise de metadados - enfrentam variados graus de resistência mesmo quando sua implementação não implica necessariamente numa interferência direta no algoritmo criptográfico ou gerenciamento de chaves.

77 INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. **Internet Society**, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/. Acesso em: 06 ago. 2021.

78 KAMARA et al. **Outside Looking In**: Approaches to Content Moderation in End-to-End Encrypted Systems. Center for Democracy and Technology Research, Washington, ago. 2021. Disponível em: https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/. Acesso em: 26 ago. 2021.

5.3. Sobre os bloqueios do WhatsApp no Brasil e sua relação com o Marco Civil da Internet

Os entendimentos dos entrevistados acerca dos bloqueios do WhatsApp e de sua relação com o Marco Civil da Internet evidenciaram diferentes interpretações do conteúdo da lei. A controvérsia jurídica diz respeito especificamente ao capítulo III, seção II, do referido diploma legal. Tais dispositivos, em resumo, dispõem sobre o regime aplicável às operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações realizadas em território nacional. Envolvem também quando tais atividades são realizadas por pessoa jurídica sediada no exterior, desde que ofereça serviços para o público brasileiro e possua ao menos uma integrante de seu grupo econômico sediado em território nacional.

A esse respeito, cumpre destacar que o art. 10 preconiza que a guarda e a disponibilização dessas informações devem preservar a imagem, a vida privada, a honra e a intimidade das partes envolvidas. O art. 11, por sua vez, condiciona tais atividades ao respeito da "legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros"[79]. O art. 12, por fim, estabelece sanções para o descumprimento dos arts. 10 e 11. Os incisos III e IV desse dispositivo, ademais, prevêem as determinações de suspensão temporária das atividades referentes ao art. 11 ou a proibição de exercício dessas atividades.

No tocante à interpretação desses dispositivos, duas teses principais foram levantadas. A primeira delas considera as sanções do artigo 12 inaplicáveis a casos de descumprimento de ordens judiciais de entrega de dados em razão desse descumprimento não implicar em violação à privacidade e à proteção de dados - pelo contrário, quando decorrente de implementação criptográfica, tal inobservância decorreria do sucesso em proteger tais direitos. Tal interpretação se alicerça nas referências expressas nos artigos em questão à defesa desses direitos, bem como ao compromisso mais geral do MCI como a defesa da privacidade. Trata-se de leitura afim a uma racionalidade comprometida primariamente com a defesa da privacidade e refratária ao acesso excepcional e a medidas vistas como invasivas da privacidade em geral.

A segunda tese, por outro lado, enxerga tais sanções como aplicáveis aos casos em questão por entender que tais descumprimentos implicam numa violação do artigo 11. Isso porque a redação do artigo 11 estabeleceria o respeito à legislação brasileira como um dever autônomo em relação ao dever de observância da privacidade e da proteção de dados. Assim, ao descumprir uma ordem judicial adequadamente fundamentada e emitida por uma autoridade competente, as empresas estariam infringindo o ordenamento

79 BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DF: Presidência da República, 2014. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 ago. 2021.

nacional e ficariam consequentemente sujeitas à suspensão de seus serviços nos termos do art. 12. Essa posição se conecta a uma racionalidade que vê as guerras criptográficas primariamente com um conflito político entre Estados e empresas globais de tecnologia e se compromete com a reafirmação da autoridade estatal diante da ameaça posta por tais empresas à referida autoridade. Tal tese foi, inclusive, um dos fundamentos da terceira tentativa de bloqueio (segundo bloqueio concretizado) do WhatsApp no Brasil.

Na apreciação do mérito dessas interpretações, convém reiterar inicialmente que, conforme previamente argumentado, a existência de um dever de aptidão à quebra de sigilo aplicável às empresas de tecnologia e aos provedores de aplicações de internet no direito brasileiro não é evidente. Assim, põe-se a questão da licitude da fixação de sanções ao agente econômico que descumpre uma ordem judicial de entrega de dados em razão de, agindo de forma lícita, ter produzido uma arquitetura informacional que lhe torna inapto à quebra de sigilo. A esse respeito, a quinta turma do STJ confirmou a decisão do Ministro Ribeiro Dantas no Recurso Especial Nº 1871695 – RO (2020/0095443-3), que afastou tal possibilidade por entender que ninguém deve ser obrigado a fazer o impossível e que os benefícios da criptografia superam em muito seus eventuais ônus para a sociedade[80].

Nesse sentido, também importa destacar o entendimento da Ministra Rosa Weber em seu voto proferido nos autos da Ação Declaratória de Inconstitucionalidade (ADI) nº 5527. Segundo a Relatora, as referidas sanções enunciadas do Marco Civil prestam-se especificamente a regular sobre o descumprimento do dever de observância da legislação brasileira em atividades de tratamento de registros, dados pessoais e comunicações. Os dispositivos em questão – e, em especial, as referidas sanções legais –, ainda segundo a Ministra, não se aplicam no contexto do descumprimento de ordens judiciais.

Conclui-se, então, que a inaplicabilidade das sanções em questão se encontra respaldada tanto pelo entendimento da relatora nesse caso, em que pese restar pendente a conclusão do julgamento do STF, quanto pela jurisprudência do STJ.

Outro segmento dos entrevistados apontou que, independentemente de haver ou não permissão legal no Marco Civil da Internet que possibilite as ordens de bloqueio, essas determinações judiciais seriam possíveis em decorrência do chamado poder geral de cautela do juiz. Trata-se de um mecanismo inicialmente previsto no art. 798 do Código de Processo Civil de 1973, por meio do qual o juiz teria discricionariedade para aplicar medidas cautelares diversas das previamente estipuladas em lei, a fim de garantir o resultado útil do processo.

Esse instrumento foi, de certa forma, ampliado no Código de Processo Civil de 2015, no qual deixou-se de enunciar os métodos legalmente previstos de medidas cautelares. Alternativamente, o art. 301 enuncia a permissão geral segundo a qual “a tutela de

80 BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Disponível em < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, acesso em 03 ago 2021.

urgência de natureza cautelar pode ser efetivada mediante arresto, sequestro, arrolamento de bens, registro de protesto contra alienação de bem e qualquer outra medida idônea para asseguração do direito". A regra do processo civil no código vigente, nesse sentido, é integralmente centrada no poder geral de cautela do juiz para determinar medidas cautelares e tutelas antecipadas durante o rito do processo.

No âmbito do Direito Processual Penal, o poder geral de cautela do juiz firma-se por entendimento jurisprudencial que traz a aplicabilidade subsidiária do Código de Processo Civil – e, por consequência, o enunciado do art. 301 desse diploma legal – para o processo penal. Trata-se de interpretação decorrente do art. 3º do Código de Processo Penal, que autoriza a "interpretação extensiva e a interpretação analógica, bem como o suplemento dos princípios gerais de direito". Com isso, o CPP permite o uso de institutos jurídicos externos ao processo penal para suprir eventuais lacunas legais.

Há divergência na doutrina jurídica quanto à aplicabilidade do poder geral de cautela do juiz em sede de processos criminais. Contudo, o entendimento jurisprudencial majoritário no país posiciona-se no sentido de que se trata de prerrogativa necessária à atividade do aplicador da lei – sobretudo no que diz respeito às medidas cautelares não pessoais, ou seja, diversas daquelas aplicadas ao réu no curso do processo penal. O poder de cautela, nesse sentido, decorre da teoria dos poderes implícitos do juiz, em prol da efetivação da justiça. Trata-se de uma prerrogativa recorrentemente empregada, por exemplo, para determinar astreintes a integrantes da relação processual que não sejam o réu (ao qual são aplicáveis apenas as medidas cautelares expressamente previstas em lei) e que descumpriram ordens judiciais consideradas necessárias para a instrução do processo.

Na imposição de medidas atípicas através do poder de cautela do juiz, contudo, é essencial que sejam observados preceitos de proporcionalidade e necessidade da medida elencada frente ao objetivo almejado com a decisão. O exame desses preceitos no caso dos bloqueios do WhatsApp retoma um tema bastante discutido pelos entrevistados: o entendimento de que os bloqueios foram injustificados em razão de sua desproporcionalidade, mais do que pelo Marco Civil da Internet.

Nesse sentido, o impacto das ordens de bloqueio se coloca como central. Para diversos entrevistados, foi o dano resultante dos bloqueios do WhatsApp, mais do que a redação do Marco Civil da Internet, que ocasionava sua ilegitimidade. Como se pôde constatar na seção deste trabalho que descreveu os bloqueios, todas as ordens de suspensão da eficácia dos bloqueios tiveram por fundamento o princípio da proporcionalidade. Ainda, duas delas entenderam que haveria meios menos gravosos de garantia da efetivação da lei. Nesse sentido, embora esteja pendente a posição do STF no contexto das ações que discutem os casos, o exame das quatro decisões de suspensão dos bloqueios sugere que os requisitos de necessidade (haveria meios menos gravosos disponíveis) e proporcionalidade (o dano resultante foi difuso e excessivo) não estariam presentes.

Assim, a análise dos bloqueios do WhatsApp e de sua relação com o Marco Civil da

Internet nos leva a três conclusões: i) tese restritiva das sanções previstas no art. 12 do Marco Civil da Internet a violações à privacidade e à proteção de dados é respaldada pelo entendimento da ministra Rosa Weber, pendente a conclusão do julgamento, de modo que o artigo 11 não poderia fundamentar os bloqueios; ii) o poder geral de cautela do juiz também não poderia fundamentar adequadamente os bloqueios, haja vista ausentes os requisitos de proporcionalidade e necessidade, conforme evidenciado pelas ordens de suspensão dos bloqueios; iii) sanções econômicas também não poderiam ser aplicadas, conforme entendimento firmado pelo STJ, em razão da impossibilidade fática de entrega dos dados aliada ao sopesamento dos custos e benefícios da criptografia, que legitima a manutenção da criptografia no sistema.

6. Conclusão

A interlocução com os mais de 40 profissionais entrevistados para a realização do presente estudo evidenciou a multiplicidade de dimensões e perspectivas que atravessam o debate sobre as políticas de criptografia no século XXI, em especial no tocante às guerras criptográficas. Embora essa complexidade impossibilite uma investigação exaustiva de todos os aspectos da controvérsia em questão, a análise sistemática do conteúdo das entrevistas resultou numa cartografia de seus principais elementos contenciosos, bem como dos pressupostos valorativos e fáticos que fundamentam os posicionamentos dos atores. A partir desse mapeamento, foram examinadas as relações entre as percepções dos atores e os contextos socioeconômicos, jurídicos, políticos e técnicos com que se relacionam objetivamente.

Durante as fases I e II das guerras criptográficas, o cerne da controvérsia tem sido por vezes identificado com a questão do acesso excepcional a conteúdos protegidos por criptografia forte. Nos enunciados analisados, observou-se que a defesa de medidas dessa sorte se articula a uma racionalidade de cunho essencialmente político-jurídico. Seus pressupostos fundamentais são a primazia da segurança - entendida como o sucesso na persecução penal, sobretudo se tratando de crimes graves - sobre a privacidade e a existência de um dever de aptidão à quebra de sigilo aplicável às empresas de tecnologia e provedoras de aplicação. Ainda, entende a crença na confiabilidade dos controles institucionais como um princípio normativo cuja aceitação é necessária ao funcionamento do Estado, sob risco de desqualificação de toda a institucionalidade, e dela infere mitigáveis os riscos de abuso da ferramenta pela autoridade pública.

O discurso contrário ao acesso excepcional, por sua vez, adota uma ênfase distinta. Por um lado, argumenta que os danos da medida são excessivos nos planos técnico (redução da segurança do sistema), jurídico-político (desproporcionalidade, riscos aos direitos dos usuários e danos à confiança no ambiente digital) e econômico (ônus demasiados aos provedores e prejuízo à toda economia digital). Por outro, questiona a eficácia e a necessidade da medida, argumentando que não é possível saber até que ponto a criptografia efetivamente contribui para o insucesso investigativo e que é provável que os criminosos alvejados evadiriam a plataforma enfraquecida.

O mapeamento dos argumentos que permeiam esses discursos visibiliza a existência de premissas jurídicas e fáticas passíveis de exame hermenêutico ou empírico, o que pode contribuir significativamente para o amadurecimento do debate. A análise apresentada evidenciou, por exemplo, que a existência de um dever de aptidão à quebra de sigilo aplicável aos setores de tecnologia e de aplicações digitais no Brasil é, no mínimo, juridicamente contestável. Similarmente, demonstrou que as preocupações com os danos do acesso excepcional encontram respaldo teórico na ciência criptográfica e empírico em estudos sobre o ambiente político brasileiro e sobre os impactos econômicos de normas restritivas da criptografia.

Por outro lado, verificou que há obstáculos metodológicos a uma aferição qualificada da alegada banalização das quebras de sigilo no país - ainda que o crescimento explosivo no volume de quebras seja um fenômeno digno de nota em si mesmo. Ainda, chama atenção para a necessidade de estudos que investiguem a dimensão efetiva do alegado obstáculo representado pela criptografia no êxito da investigação criminal e averiguem o lastro empírico da tese da migração da criminalidade em decorrência da implementação de acesso excepcional.

Embora essa qualificação possa surtir efeitos positivos sobre o debate, a contraposição entre as ênfases e as premissas ético-políticas das duas racionalidades expostas também sugere que a simples testagem factual das alegações dos dois lados tem um potencial limitado de resolução da controvérsia estabelecida. Isso porque os pontos de vista dos atores se inserem em narrativas, atitudes e disposições afetivas mais gerais sobre as relações entre Estado e indivíduo, entre privacidade e segurança. A defesa do acesso excepcional trata a confiabilidade dos controles institucionais como um princípio normativo, ao passo que a oposição a tal medida tem como princípio o ceticismo sobre a eficácia desses controles. Um lado associa a segurança a imagens de persecução penal eficaz, o outro a plataformas tecnológicas desenhadas visando a máxima proteção das informações trafegadas. Um lado vê a atuação repressiva do Estado como fundamentalmente garantidora do interesse público, o outro a vê como altamente passível de instrumentalização política contra as liberdades democráticas.

Tomemos como exemplo a tese de que há um dever de aptidão à quebra de sigilo aplicável aos setores de tecnologia e de aplicações digitais no Brasil. Sua contestação dificilmente resolveria a controvérsia: os defensores do acesso excepcional poderiam simplesmente replicá-la, mobilizando outros argumentos jurídicos para fundamentar a existência de tal dever, ou, alternativamente, deslocar o debate do plano descritivo ao plano normativo, defendendo que se tal dever inexiste, ele *deveria* passar a existir por força de lei ou jurisprudência superior. Isso porque sua posição supõe, para além da questão específica sobre a existência dessa previsão no ordenamento brasileiro, ser fundamentalmente inaceitável que existam espaços comunicativos inacessíveis aos olhos da autoridade estatal.

Isso é similarmente corroborado pelo exame das controvérsias envolvendo as alegadas alternativas ao acesso excepcional. Propostas como escaneamento do cliente, *hacking* governamental e uso extensivo de metadados tendem a encontrar enorme resistência entre ativistas e acadêmicos dos direitos digitais. Ainda que não interfiram necessariamente no algoritmo utilizado e nem nos processos de geração e gerenciamento de chaves -, tais soluções são vistas como minando a criptografia porque atingem os valores que o emprego criptografia convencionalmente busca proteger. Assim sendo, observa-se que a defesa da criptografia se conecta a preocupações mais amplas como a proteção da privacidade, da liberdade de expressão, dos direitos políticos e valores democráticos, num contexto em que estes são ameaçados pela criminalidade cibernética e pelo vigilantismo estatal. Nesse prisma, a ampliação do vigilantismo é vista como um ataque à criptografia mesmo que não envolva uma interferência no sistema criptográfico em sentido estrito.

Do mesmo modo, a controvérsia em torno da interpretação dos arts. 10, 11 e 12 do Marco Civil da Internet evoca esse dissenso mais profundo sobre os valores que devem orientar a interpretação da lei. A interpretação contrária aos bloqueios enfatiza os trechos protetivos da privacidade e da proteção de dados pessoais dos dispositivos precisamente por serem esses os valores fundamentais que tal racionalidade encampa. Por outro lado, a interpretação favorável aos bloqueios enfatiza a obrigação de respeito à legislação brasileira porque suas preocupações primárias são com a ameaça posta pelas empresas globais de tecnologia à autoridade estatal, que se acham na posição de desafiar em razão de seu poder econômico transnacional. Das perspectivas de ambos os atores, o que está em questão é mais profundo que a redação desses dispositivos específicos.

Ao longo deste estudo, objetivou-se apresentar as dimensões argumentativas que permeiam o debate atual entre a segurança pública e a defesa estatal versus os direitos à privacidade e à liberdade de expressão no meio digital – sob o cerne da utilização de técnicas de criptografia forte. Trata-se de um debate longevo, datado ao menos da segunda metade do século XX, e que permanece essencialmente perene desde então. Percebe-se, contudo, que se trata de uma questão mais profunda do que se observa em primeira análise: os argumentos em favor de ambos os posicionamentos adquirem dimensões múltiplas, que extravasam a própria legitimidade da criptografia. As múltiplas faces dessa discussão – sociais, políticas, jurídicas, entre outras – não podem, portanto, ser consideradas individualmente em prol da resolução completa da controvérsia.

Buscou-se, finalmente, oferecer uma contribuição sobre as perspectivas que integram o debate sobre o uso da criptografia. Espera-se que o mapeamento dos dados dos entrevistados, bem como a análise desses pronunciamentos à luz dos mecanismos jurídicos vigentes no Brasil, possam ser utilizados para uma qualificação mais profunda do debate em pauta a partir de estudos futuros.

7. Referências bibliográficas

ABELSON, Hal *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. **Journal of Cybersecurity**, v. 1, n. 1, p. 69-79, 2015. p.69.

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42. p. 29.

ABREU, Jaqueline. Audiência Pública sobre Criptografia e Bloqueios do WhatsApp: argumentos diante do STF. 26/06/2017. Bloqueios.info . Disponível em <http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/ >, acesso em 02 ago 2021.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. p. 44-45

AGÊNCIA CÂMARA DE NOTÍCIAS. **Relatório preliminar do novo CPP incorpora provas digitais e novas tecnologias ao processo criminal.** Relator: Deputado João Campos. 13/04/2021. Disponível em <https://www.camara.leg.br/noticias/745824-relatorio-preliminar-do-novo-cpp-incorpora-provas-digitais-e-novas-tecnologias-ao-processo-criminal/>, acesso em 26 ago. 2021.

ALMEIDA, Frederico de. MONTEIRO, Filipe Jordão; SMIDERLE, Afonso.a criminalização dos protestos do movimento passe livre em são paulo (2013-2015). **Revista Brasileira de Ciências Sociais** [online]. v. 35, n. 102, 2020.

ANTONIALLI, Dennys. M.;ABREU, Jacqueline; MASSARO, Heloisa. M. M. ; LUCIANO, Maria. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. **Revista Brasileira de Ciências Criminais**, v. 154, p. 177-214, 2019.

ARTIGO 19. **As restrições ao direito de protesto no Brasil**. 5 anos de junho de 2013: Como os três poderes intensificaram sua articulação e sofisticaram os mecanismos de restrição ao direito de protesto progressivamente. Artigo 19, 2018. Disponível em: https://artigo19.org/5anosde2013/. Acesso em: 04/08/2021.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO (LAUT). **Retrospectiva - Tecnoautoritarismo 2020. LAUT,** 2021. Disponível em: https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf. Acesso em: 04/08/2021.

BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. O impacto econômico das leis que enfraquecem a criptografia. **Law & Economics Consulting Associates** (LECA). Tradução de Paulo Renà da Silva Santarém. 2021. Disponível em: https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia . Acesso em: 04/08/2021.

BARIFOUSE, R.; DUARTE, F.; BARRUCHO, L. G. Liberação do WhatsApp não encerra polêmica disputa com Justiça brasileira. **G1**. Tecnologia e Games. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/12/liberacao-do-whatsapp-nao-encerra-polemica-disputa-com-justica-brasileira.html. Acesso em: 29/07/2021.

BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (BERKMAN). **Não Entre em Pânico**: Avançando no debate sobre "obscurecimento" (Going Dark). 2018. Tradução pelo Instituto de Tecnologia e Sociedade do Rio. Disponível em: https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf Acesso em 02/08/2021.

BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. **Em Tese - Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC**, Florianópolis, v. 2, n. 1 (3), p. 68-80, jan./jul. 2005.

BRADFORD, Sharon. THOMPSON, Andi Wilson. Open Letter to GCHQ on the Threats Posed by the Ghost Proposal. **Lawfare - Hard National Security Choices**, 30 mai. 2019. Disponível em: https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal. Acesso em: 05 ago. 2021.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DF: Presidência da República, 2014. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 ago. 2021.

BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. **Processo nº 201655090143**. Decisão. Juiz Marcel Maia Montalvão. Lagarto, Sergipe, 26 abr. 2016.

BRASIL. Tribunal de Justiça do Estado de Sergipe. **Mandado de Segurança nº 201600110899**. Decisão liminar. Rel. Des. Ricardo Múcio Santana de Abreu Lima. Aracaju, 3 mai. 2016. Disponível em: <http://www.omci.org.br/m/jurisprudencias/ arquivos/2016/tjse_201600110899_03052016.pdf> Acesso em: 2 nov. 2016.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Inquérito Policial nº 062-00164/2016**. Juíza Daniela Barbosa Assumpção de Souza. Duque de Caxias, RJ, jul. 2016. Disponível em: <https://drive.google.com/file/d/0Bw3seZUv__5ubnFudjUwMm9OZGc/view>. Acesso em: 30/07/2021

BRASIL. Conselho Nacional de Justiça (CNJ). Sistema Nacional de Controle de Interceptações Telefônicas. **CNJ**, Brasília, 2021. Disponível em: https://www.cnj.jus.br/sistemas/sistema-nacional-de-controle-de-interceptacoes-telefonicas/. Acesso em: 04/08/2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Mandado de Segurança nº 2271462-77.2015.8.26.0000**. Decisão liminar. Rel. Des. Xavier de Souza. São Paulo, 17 dez. 2015. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_22714627720158260000_17122015.pdf. Acesso em: 29/07/2021.

BRASIL. Central de Inquéritos da Comarca de Teresina. **Nota**. Juiz Luiz de Moura Correia. Teresina, 26 fev. 2015. Disponível em: http://s2.glbimg.com/MdNVliNDOaF45o27HM8_tsG3wll=/s.glbimg.com/jo/g1/f/original/2015/02/26/nota_juiz_whatsapp_ok.jpg. Acesso em: 29/07/2021.

BRASIL. Tribunal de Justiça do Estado do Piauí. **Mandado de Segurança nº 2015.0001.001592-4**. Rel. Des. Raimundo Nonato da Costa Alencar. Teresina, 26 fev. 2015. Disponível em: <http://www.migalhas.com.br/arquivos/2015/2/art20150227-03.pdf> Acesso em: 29/07/2021.

BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Disponível em < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, acesso em 03 ago 2021.

BRASIL.Superior Tribunal de Justiça. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma.** 24/06/2021. Disponível em <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx>, acesso em 03 ago 2021.

BRASIL. Ministério da Justiça e Segurança pública. **Simpósio sobre Going Dark termina com declaração de 13 países.** Disponível em <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2>, acesso em 03 ago 2021.

BRASIL. Supremo Tribunal Federal. **Medida cautelar de arguição de descumprimento de preceito fundamental**. Decisão liminar. Rel. Min. Ricardo Lewandowski. Brasília, 19 jul. 2016. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Acesso em: 30/07/2021.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental Nº 403.** Relator: Edson Fachin. Brasília, DF. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acesso em: 06 ago. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade Nº 5527**. Relatora: Rosa Weber. Brasília, DF. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Acesso em: 06 ago. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus Nº 51.531 - RO**. Rel. Ministro Nefi Cordeiro. Brasília, 09 mai. 2016. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/inteiro-teor-340165652. Acesso em: 05 ago. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 580.664 - RJ**. Rel. Ministro Nefi Cordeiro. Brasília, 20 out. 2020. Disponível em:https://stj.jusbrasil.com.br/jurisprudencia/1206242995/habeas-corpus-hc-580664-rj-2020-0111177-4/inteiro-teor-1206243005 . Acesso em: 05 ago. 2021

BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. Processo nº 201655090143. **Decisão. Juiz Marcel Maia Montalvão**. Lagarto, Sergipe, 26 abr. 2016.

BRASIL. **Declaração do 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 04 ago 2021.

BRASIL. Câmara dos Deputados. **Parecer do Relator, Dep. João Campos (REPUBLIC-GO) da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 8045, de 2010, do Senado Federal, que trata do "Código de Processo Penal" (revoga o Decreto-Lei nº 3.689, de 1941. Altera os Decretos-Lei nº 2.848, de 1940; 1.002, de 1969; as Leis nº 4.898, de 1965, 7.210, de 1984; 8.038, de 1990; 9.099, de 1995; 9.279, de 1996; 9.609, de 1998; 11.340, de 2006; 11.343, de 2006), e apensados ao Projeto de Lei nº 8.045, de 2010**. Portal da Câmara dos Deputados. Brasília, 26 abr. 2021. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/gt-anteprojeto-do-novo-codigo-de-processo-penal/documentos/outros-documentos/substitutivo-relator-joao-campos. Acesso em: 05 ago. 2021. p. 481.

CANABARRO, Diego. AULA 4 - Criptografia: experiências regulatórias e debates internacionais com Diego Canabarro. Belo Horizonte: **Instituto Iris,** 2021. (39 min.), son., color. Disponível em: https://youtu.be/EDaI5_z-hBo?t=2200. Acesso em: 25 ago. 2021.

CANTO, Mariana. RAMIRO, André. REAL, Paula C. Criptografia no STF: O que dizem os votos de Rosa Weber e Edson Fachin e o que podemos aprender com eles. **IP.Rec – Instituto de Pesquisa em Direito e Tecnologia do Recife.** Disponível em <https://ip.rec.br/2020/06/22/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/ >, acesso em 02 ago 2021.

CARVALHO, Thaís Bernardes. **O bloqueio judicial do WhatsApp no território brasileiro no contexto do Estado Democrático de Direito.** 2017. 69 f. Monografia de graduação

no curso de Direito - Universidade Federal de Lavras, Lavras, 2017; Disponível em http://repositorio.ufla.br/handle/1/30751. Acesso em 16 de agosto de 2021.

CRABTREE, B. & MILLER, W. **Doing qualitative research**. Thousand Oaks, Calif.: Sage Publications, 1999.

COALIZÃO PELOS DIREITOS NA REDE. **Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia.** 20 de maio de 2021. Disponível em <https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>, acesso em 25 ago. 2021.

COMEY; James B. **Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?** Out. 2014, discurso realizado na Brookings Institution. [Online]. Disponível em https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acesso em: 02 ago. 2021.

BRANDÃO, et al. (Org). **Tecnologias e conectividade**: direito e políticas na governança das redes. 1ed. Belo Horizonte: 2018, v. 1, p. 15-30.

DIFFIE, Whitfiead. HELLMAN, Marin. **New directions in cryptography.** IEEE Transactions on Information Theory, 22, 644-654.

DONEDA, Danilo. MACHADO, Diego. (coords.) **A criptografia no direito brasileiro**. São Paulo: Thompson Reuters - Revista do Tribunais, 2019.

FROOMKIN, Michael. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

GASKELL, G. Entrevistas individuais e grupais. In: BAUER, M. W.; GASKELL, G. (Org.). **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis, RJ: Vozes, 2000, pp. 64-89.

Global Encryption Coalition. Brazilian Code of Criminal Procedure reform must not undermine encryption. June 28, 2021. Disponível em <https://www.globalencryption.org/2021/06/brazilian-code-of-criminal-procedure-reform-must-not-undermine-encryption/>, acesso em 25 ago. 2021.

GROVER, Gurshabad; RAJWADE, Tanaya; KATIRA, Divyank. The Ministry And The Trace: Subverting End-To-End Encryption, 14 NUJS Law Review. 1(2021). p. 2-6. Disponível em <http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/ >. Acesso em: 02 ago. 2021.

HOBOKEN, J. V.; SCHULZ, W. **Human rights and encryption**. Paris: UNESCO, 2016.

INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. Cryptologia, v. 3, n. 3, 129 - 135, 1979.

INTERNET SOCIETY. Fact Sheet: Ghost Proposals. **Internet Society**, 24 mar. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/. Acesso em: 06 ago. 2021.

INTERNET SOCIETY. Fact Sheet: Client-Side Scanning. **Internet Society**, 24 mar. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/. Acesso em: 06 ago. 2021.

INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. **Internet Society**, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/. Acesso em: 06 ago. 2021.

JARVIS, Craig. **A New Crypto Wars Chronology (I)**. 21 fev. 2020. LinkedIn: Craig Jarvis. Disponível em: https://www.linkedin.com/pulse/new-crypto-wars-chronology-craig-jarvis/. Acesso em: 29 jul. 2021.

JARVIS, Craig. **A New Crypto Wars Chronology (II)**. 20 jul. 2020. LinkedIn: Craig Jarvis. Disponível em: https://www.linkedin.com/pulse/new-crypto-wars-chronology-ii-craig-jarvis/?articleId=6690894456150859776. Acesso em: 29 jul. 2021

JARVIS, Craig. Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. CRC Press, 2020.

KAMARA et al. Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems. **Center for Democracy and Technology Research,** Washington, ago. 2021. Disponível em: https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/. Acesso em: 26 ago. 2021.

KRIPPENDORFF, K. **Content Analysis**: an introduction to its methodology. Thousand Oaks, Calif.: Sage Publications, 2004.

KURTZ, Lahis P.; MENEZES, Victor. A.. **Entre o direito e a força na sociedade da informação: bloqueio judicial do WhatsApp e ADI nº 5.527.** In: Fabrício Bertini Pasquot Polido; Lucas Costa dos Anjos; Luiza

LEVY, Ian. ROBINSON, Crispin. Principles for a More Informed Exceptional Access Debate. **Lawfare - Hard National Security Choices**, 29 nov. 2018. Disponível em: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate . Acesso em 05 ago. 2021.

LIU, H. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. Journal of World Trade, v. 51, n. 2, p. 309 - 334, 2017.

MASI, Carlos Velho. O caso Escher e outros v. Brasil e o sigilo das comunicações telefônicas. **Revista dos Tribunais**, v. 932, Junho de 2013, pp. 309-352

MITCHELL, Bonnie et al. Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponível em:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acesso em: 05 ago. 2021. p. 8.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponível em:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acesso em: 05 ago. 2021. p. 18.

PORTNOY, Erica. Why Adding Client-Side Scanning Breaks End-To-End Encryption. **Electronic Frontier Foundation**, 1 nov. 2019. Disponível em: https://www.eff.org/pt-br/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption. Acesso em: 06 ago. 2021.

QUEIROZ, Rafael Mafei Rabelo. PONCE, Paula Perdigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, v.1,n.1, fev/2020, p.64-90.

RAMIRO, André. CANTO, Mariana. REAL, P. C. et al. **O Mosaico Legislativo da Criptografia no Brasil: Uma Análise de Projetos de Lei**. IP.Rec. Disponível em <https://ip.rec.br/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-no-Brasil-uma-an%C3%A1lise-de-Projetos-de-Lei-1.pdf >, acesso em 04 ago 2021.

RAY, Trisha. The Encryption Debate in India: 2021 Update. 2021.

RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

RODRIGUES, G. R. A controvérsia cifrada: o Clipper e o mito da derrota estatal nas guerras criptográficas dos anos 1990. Em: ALVES, Marco Antônio Sousa. NOBRE, Marcio Rimet. (orgs.). **A sociedade da informação em questão**: o direito, o poder e o sujeito na contemporaneidade. Belo Horizonte: D'Plácido, 2019.

ROSENTHAL, G. **Pesquisa social interpretativa**: uma introdução. Porto Alegre:

Edipucrs, 2014.

SCHNEIER, Bruce. **Applied Cryptography**: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. New Jersey: John Willey & Sons, 1996, p. 30.

SCHULMAN, Ross. Why the Ghost Keys 'Solution' to Encryption is No Solution. **Just Security**, 18 jul. 2019. Disponível em: https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/. Acesso em: 05 ago. 2021.

SILVA JUNIOR, L. A.; LEAO, M. B. C. O software Atlas.ti como recurso para a análise de conteúdo: analisando a robótica no Ensino de Ciências em teses brasileiras. **Ciênc. educ.** (Bauru), Bauru , v. 24, n. 3, p. 715-728, set. 2018.

SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 234-235.

STEPANOVICH, Amie et al. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em:https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Acesso em: 05 ago. 2021.

STILGHERRIAN. The Encryption Debate in Australia: 2021 Update. 2021.

VINUTO, J. A amostragem em Bola de Neve na pesquisa qualitativa: um debate em aberto. **Temáticas** (UNICAMP), v. 44, p. 201-218, 2014.

WHATSAPP INC. **Blog do WhatsApp**. Criptografia de Ponta-a-Ponta. 05 abr. 2016. Disponível em: https://blog.whatsapp.com/end-to-end-encryption. Acesso em: 30/07/2021

Apêndice 1 - Roteiro da entrevista

Bloco I - Apresentação e temas gerais

Qual sua idade?

Cidade onde reside?

Qual sua área de formação?

Onde você trabalha atualmente? (Cargo atual e atribuições)

Conte um pouco da sua trajetória profissional? (EXPLORAR: Onde trabalhou? Quais funções exerceu? Como foi o contato com as questões de internet e sociedade?)

Como as transformações que a internet trouxe à sociedade impactaram na sua trajetória profissional?

Pensando nas transformações que a internet trouxe para a sociedade, tem algo que você entende como especialmente positivo ou especialmente negativo?

Bloco II - Criptografia, privacidade e segurança

Numa escala de 0 a 10, que importância você atribui à privacidade **na sociedade atual**? Por que?

Numa escala de 0 a 10, que importância você atribui **à sua** privacidade? Por que?

Como você avalia o debate público sobre privacidade hoje? (EXPLORAR: Brasil, outros países, etc)

Como você enxerga a relação entre privacidade e segurança hoje? (EXPLORAR: há contextos em que esses valores conflitam?)

Na sua percepção, quais são as relações entre segurança pública e segurança da informação?

Numa escala de 0 a 10, que importância você atribui à criptografia **na sociedade atual**? Por quê?

Numa escala de 0 a 10, que importância você atribui à criptografia **nas aplicações que você usa?** Por quê?

Numa escala de 0 a 10, qual seu nível de satisfação com o atual ambiente regulatório sobre criptografia? Por que?

Se você pudesse, você mudaria algo nesse ambiente? O que?

No seu entendimento, há situações em que o uso de criptografia conflita com o interesse público? (Explorar diferentes entendimentos sobre o público)

Você apoiaria a introdução de um mecanismo de acesso excepcional na criptografia para fins de investigação criminal? (Explorar: Por que? Se sim, quais situações legítimas e ilegítimas para o uso desse mecanismo? Há riscos relacionados a isso? Se há riscos, quais? Há custos econômicos, reputacionais ou sociais associados? Existe algum meio termo?)

No seu entendimento, é possível conciliar a segurança dos usuários com a introdução de um mecanismo de acesso excepcional na criptografia?

Como você avalia a legitimidade dos bloqueios do WhatsApp ocorridos em 2015 e 2016 no Brasil? (Explorar as dimensões da legitimidade)

Para profissionais do Direito: No seu entendimento, o Marco Civil da Internet autoriza bloqueios de aplicação por descumprimento de ordens de entrega de dados para fins de investigações criminais?

Você conhece alguma alternativa para o acesso a esses dados que não envolva acesso excepcional? (Explorar: se sim, quais? quais os riscos associados a cada uma?)

Você já atuou profissionalmente em alguma situação que envolvesse de alguma forma a questão do acesso a dados criptografados?

No seu trabalho, você lida com questões relacionadas à regulação de criptografia de alguma maneira?

Para servidores/gestores públicos: Na sua opinião, os esforços de modernização do serviço público e digitalização do governo vêm acompanhados de uma preocupação com segurança da informação?

Bloco III - Capacitação e educação

Considerando aspectos técnicos e regulatórios, de zero à 10, qual nota você atribui ao seu grau de conhecimento sobre criptografia? Por que? (Explorar: há lacunas? Se sim, quais?)

Você já realizou algum curso ou capacitação voltada para este campo? (Explorar: Se sim, qual foi a instituição responsável? Qual a duração? Qual foi a modalidade - online ao vivo, online gravado, presencial?)

O que um curso voltado para avançar essa discussão deveria abordar?

Há algo que eu não perguntei que você acha que faria sentido eu ter perguntado?

Apêndice 2 - Famílias de códigos

I - Códigos sobre acesso excepcional (AE::) para fins de investigação criminal

AE:: Apoiaria

AE:: Banalização das quebras de sigilo

AE:: Causará evasão do serviço

AE:: Com controles institucionais rigorosos

AE:: Compromete a legalidade da prova

AE:: Custo operacional para o provedor

AE:: Custo reputacional para o provedor

AE:: Desnecessário, pois há outros meios de investigação

AE:: É preciso confiar na justiça

AE:: Fere os princípios de Segurança da Informação e criptografia

AE:: Fere a segurança do Estado

AE:: Impacta a confiança no ecossistema digital

AE:: Importante em nome da segurança

AE:: Indeterminado se apoiaria

AE:: Manifestação de desconhecimento, dúvida ou incerteza

AE:: Não apoiaria

AE:: Não há evidência de ganho

AE:: Necessário defender para valorizar a autoridade pública

AE:: Obrigação de colaborar com a justiça

AE:: Obrigação de obedecer comando judicial

AE:: Tão ou menos grave que os meios atualmente empregados

AE:: Para crimes específicos

AE:: Risco de abuso pela autoridade

AE:: Risco de usurpação por terceiros maliciosos

AE:: Risco para direitos

AE:: Semelhante à interceptação telefônica

AE:: Último remédio

AE:: Vulnera terceiros

II - Códigos sobre satisfação com o ambiente regulatório (AR::) sobre criptografia

AR:: Brasil está melhor que o exterior

AR:: Criar uma instituição para determinar padrões

AR:: Cripto está ameaçada

AR:: Decisões do STF são boas

AR:: Desconhece

AR:: Deve haver padronização para um nível maior de segurança

AR:: Deve haver proteção contra backdoor/bloqueio de apps

AR:: Enforcement é frágil

AR:: Importância da criptografia é reconhecida

AR:: Inexistente

AR:: Neutralidade tecnológica é positiva/importante

AR:: Positivo, debate sobre going dark tem avançado

AR:: Pouco regulado, não abrange maior parte dos usos

III - Códigos sobre a legitimidade dos bloqueios do Whatsapp em 2015/16 (BW::) e sobre se o Marco Civil da Internet autoriza tal medida (MCI::)

BW:: Atalho investigativo

BW:: Autoriza, se for proporcional

BW:: Bloqueios foram desproporcionais

BW:: Bloqueios foram ilegítimos

BW:: Havia desconhecimento sobre a tecnologia

BW:: Motivado por disputa de forças

BW:: Gerou danos econômicos

BW:: Ignorância das empresas

BW:: Inconstitucional

BW:: Ineficazes, pois pessoas baixaram VPN

BW:: Interpretação equivocada do Marco Civil da Internet

BW:: Justiça brasileira não-competente

BW:: Legítimos, lei tem que ser cumprida

BW:: Penaliza a ferramenta

BW:: Pode autorizar

BW:: Primeiro bloqueio não envolveu criptografia

MCI:: Autoriza, pois art. 11 fala de “legislação brasileira”

MCI:: Fora do poder geral de cautela

MCI:: Independente do MCI, devido ao poder geral de cautela

MCI:: Independente do MCI, pois fundamento foi o CPP

MCI:: Não autoriza

MCI:: Não autoriza, pois medida é gravosa demais

MCI:: Não autoriza, pois é prova diabólica

MCI:: Sanções são somente para proteger a privacidade

MCI:: Sanções tem que existir como recurso final

MCI:: Se recusou a responder

IV - Códigos sobre os conhecidos métodos alternativos (MA::) de acesso à informações criptografadas e seus riscos

MA Riscos:: Incidente de segurança

MA Riscos:: Outros

MA Riscos:: Risco de abuso pela autoridade

MA Riscos:: Violação indiscriminada da intimidade

MA Riscos:: Vulnera terceiros

MA:: Back up

MA:: Busca, apreensão e desbloqueio

MA:: Client-side scanning

MA:: Busca exaustiva de chave

MA:: Desconhece ou não lembra

MA:: Engenharia social

MA:: Espelhamento do número

MA:: Ghosting

MA:: Infiltração tradicional

MA:: Lawful hacking

MA:: Metadados

MA:: Outros

MA:: Phishing

MA:: Spyware