UFPE

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

ANDRÉ BARBOSA RAMIRO COSTA

POLÍTICAS DE ENCRIPTAÇÃO:

Entre a Codificação de Direitos, Regulação Pública e o Cipher-Ativismo

Recife

2021

ANDRÉ BARBOSA RAMIRO COSTA

POLÍTICAS DE ENCRIPTAÇÃO:

Entre a Codificação de Direitos, Regulação Pública e o Cipher-Ativismo

Este trabalho foi apresentado ao Programa de Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Ciência da Computação. Área de concentração: Teoria da Computação.

Orientador: **Ruy José Guerra Barretto de Queiroz**

Recife

2021

Catalogação na fonte
Bibliotecária Nataly Soares Leite Moro, CRB4-1722

C837p Costa, André Barbosa Ramiro
Políticas de encriptação: entre a codificação de direitos, regulação pública e o cipher-ativismo / André Barbosa Ramiro Costa. – 2021.
165 f.

Orientador: Ruy José Guerra Barretto de Queiroz.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2021.
Inclui referências.

1. Criptografia. 2. Cypherpunks. 3. Privacidade. 4. Vigilância. I. Queiroz, Ruy José Guerra Barretto de (orientador). II. Título

004 CDD (23. ed.) UFPE - CCEN 2021 – 194

André Barbosa Ramiro Costa

“Políticas de Encriptação: Entre a Codificação de Direitos, Regulação Pública e o Cipher-ativismo”

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Aprovado em: 23/04/2021.

_____

Orientador: Prof. Dr. Ruy José Guerra Barretto de Queiroz

BANCA EXAMINADORA

_____

Prof. Dr. Carlos André Guimarães Ferraz (Examinador interno)
Universidade Federal de Pernambuco

_____

Prof. Dr. Danilo César Maganhoto Doneda (Examinador externo)
Instituto de Direito Público

_____

Profa. Dra. Maria Amália Arruda Câmara (Examinadora externa)
Universidade de Pernambuco

AGRADECIMENTOS

É necessário observar a trajetória acadêmica, também, pelo que não é, tradicionalmente, ciência e academia. Relações sociais, que lançam contextos às vivências do sujeito e estremecem objetividades; políticas, que são práxis da tradição e das micro-revoluções sociais, sejam geradoras de desigualdades ou emancipações; famílias, que projetam sentimentos em estado bruto; amigos e amores, um sentido sensível que preenche espaços que as instituições, grande parte das vezes, parecem negar. Esses elementos invadem o espaço acadêmico, admita-o ou não, moldando valores que vão gerar significado à produção científica. Agradeço a essa conjunção de fatores que não deixam.

Agradeço à Faculdade de Direito do Recife (FDR) que, mais pela composição política e humana, me permitiu um anti-percurso jurídico rumo à semiótica e à cibernética, erodindo e edificando um retorno possível às ciências jurídicas; aos companheiros co-fundadores e pesquisadores do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), uma conjunção de inquietudes e vionarismos, criadores de um ambiente inédito, atualizado, qualificado e qualificante de debate, pesquisa e incidência política sobre tecnologia e sociedade no Nordeste; ao Centro de Informática (CIn), que parecia falar, no campo da Ciência da Computação, do que ninguém falava no Direito: tecnologia, política e direitos humanos; a Vitor, aos três Pedros, Débora, Beto, Cássio, Orlando, André, Eduarda e todos aqueles e aquelas que, simplesmente, escolhi; ao bairro da Boa Vista, Sagres à céu aberto, fauna e flora noturna de uma episteme tropical; à Sônia, Adriana e Gustavos, pai e irmão, elos infinitos, origem meio e fim, que não desacreditaram das minhas trilhas sempre por linhas tênues; e à Clara, manhã, tarde e noite, que jamais pude sonhar e, mesmo assim, *somos*.

Innovation is a garden of forking paths.

The Social Shaping of Technology (Robin Williams e David Edge, 1996)

RESUMO

Restrições e liberdades sobre o uso de criptografia - e de encriptar, especificamente, conferindo sigilo às comunicações - acompanha (ou mesmo antecede) a popularização do uso da Internet e, de forma ampla, tem relação estreita com o desenvolvimento tecnológico. Se até a segunda metade do século vinte o emprego de técnicas de encriptação era, em grande medida, restrito ao Estado, a partir de meados da década de setenta uma revolução criptográfica entra em cena, com a criptografia de chave pública, para implicar uma redistribuição de poder e, consequentemente, provocar em conflitos políticos e regulatórios envolvendo indústria, Estado, academia e sociedade civil. Por um lado, o emprego de criptografia forte significa o estabelecimento de sistemas de segurança da informação confiáveis e resilientes, além de simbolizar a retomada da autonomia, privacidade e autodeterminação informacional do indivíduo, associando-se com a garantia aos direitos fundamentais em tempos de programas de vigilância governamental em expansão e de abusivos mercados de dados pessoais. Por outro, a democratização das técnicas de sigilo têm provocado ações reativas das forças de investigação criminal, uma vez que é desafiada a capacidade de interceptação de comunicações e acesso a dispositivos e comunicações pessoais, repercutindo sobre a cultura investigativa de produção de provas sobre tradicionais formas de monitoramento social. Três bloqueios do WhatsApp em território nacional (com repercussão em países vizinhos), entre 2015 e 2016, duas ações em trâmite no Supremo Tribunal Federal e uma série de Projetos de Lei que, em maior ou menor medida, objetivam flexibilizar a robustez da criptografia são alguns dos fatos sociopolíticos que ilustram o debate no Brasil. No plano internacional, entre as agendas políticas mais recorrentes do *Federal Bureau of Investigation* (FBI) e, em ampla medida, do *Department of Justice* dos Estados Unidos nos últimos anos, estão as tentativas de criar meios legais para obrigar plataformas a inserirem meios de "acesso excepcional" a comunicações encriptadas em seus sistemas. Como resultado, uma histórica e persistente disputa de narrativas é entrelaçada ao longo das últimas três décadas, gerando movimentos ativistas pautados no uso livre da criptografia, articulações científicas pela ética e responsabilidade no trabalho criptográfico e coalizões geopolíticas internacionais representadas, por um lado, por agências investigação governamentais, e por outro, por entidades da sociedade civil organizada. Este trabalho, portanto, buscou realizar, criticamente, um revisão de literatura sobre os principais pontos de tensão dentro do recorte histórico proposto, na tentativa de criar um mosaico compreensivo sobre a dimensão política da criptografia.

Palavras-chave: criptografia; regulação; cypherpunks; privacidade; vigilância.

ABSTRACT

Restrictions and freedoms on the use of cryptography - and the act of encryption, specifically, giving secrecy to communications - follow (or even precede) the popularization of the use of the Internet and, more broadly, are closely related to technological development. If, until the second half of the twentieth century, the use of encryption techniques was largely restricted to States, from the mid-seventies onwards a cryptographic revolution came into the scene with the public-key encryption to promote a redistribution of power and, consequently, lead to political and regulatory conflicts involving industry, State, academia and civil society. On the one hand, the use of strong encryption means the establishment of reliable and resilient information security systems, in addition to symbolizing the resumption of autonomy, privacy and informational self-determination of the individual, associating itself with the guarantee of fundamental rights in times of expansion of governmental surveillance programs and abusive markets of personal data. On the other hand, the democratization of techniques of secrecy has provoked reactions by law enforcement, since the ability to intercept communications and access to personal devices and communications is challenged, causing impacts on the investigative culture of producing evidence and traditional forms of social monitoring. Three WhatsApp shutdowns in national territory (with repercussions in neighboring countries), between 2015 and 2016, two constitutional actions in progress at the Brazilian Supreme Court and a series of Bills that aim to make the strength of encryption more flexible are some of the sociopolitical facts that illustrate the debate in Brazil. At the international level, among the most recurrent political agendas of the Federal Bureau of Investigation (FBI) and, to a large extent, of the U.S. Department of Justice in recent years are attempting to create legal means to force platforms to insert solutions of "exceptional access" to encrypted communications on their systems. As a result, a historical and persistent dispute of narratives is intertwined over the last three decades, generating activist movements based on the freedom to encrypt, scientific articulations for ethics and social responsibility in cryptographic work, and geopolitical coalitions represented, on the one hand, by law enforcement agencies, and on the other, organized civil society entities. Therefore, this work critically carried out a literature review on the main points of tension within the proposed historical framework, in an attempt to create a comprehensive mosaic about the political dimension of encryption.

Keywords: encryption; regulation; cypherpunks; privacy; surveillance.

LISTA DE ABREVIATURAS

ABIn - Agência Brasileira de Inteligência

ANPD - Autoridade Nacional de Proteção de Dados

CGI.br - Comitê Gestor da Internet no Brasil

CIDH - Corte Interamericana de Direitos Humanos

DOJ - Department of Justice

ENDES - Estratégia Nacional de Desenvolvimento Econômico e Social

FBI - Federal Bureau of Investigation

FEBRABAN - Federação Nacional de Bancos

FEM - Fórum Econômico Mundial

GSI - Gabinete de Segurança Institucional

IBCCRIM - Instituto Brasileiro de Ciências Criminais

INTI - Instituto Nacional de Tecnologia da Informação

LGPD - Lei Geral de Proteção de Dados

ICP-Brasil - Infraestrutura de Chaves Públicas do Brasil

IoT - Internet das Coisas

MCI - Marco Civil da Internet

MCTIC - Ministério de Ciência, Tecnologia, Inovações e Comunicações

MIT - Massachusetts Institute of Technology

MPF - Ministério Público Federal

NSA - National Security Agency

NCMEC - National Center for Missing and Exploited Children

NIC.br - Núcleo de Informação e Coordenação do Ponto BR

NIST - National Institute of Standards and Technology

OCDE - Organização para Desenvolvimento e Cooperação Econômica

OEA - Organização dos Estados Americanos

P2P - Peer-to-peer

PD&I - Pesquisa, Desenvolvimento e Inovação.

PKE - Public Key Encryption

PNSI - Política Nacional de Segurança da Informação (Decreto nº 9.637/2018)

STS - Science and Technology Studies

TLS - Transport Layer Security

UIT - União Internacional de Telecomunicações

UNICEF - United Nations International Children's Emergency Fund

SUMÁRIO

1 INTRODUÇÃO

> Within the larger field of ethics, [secrecy] plays an oddly unexplored role. It is not merely a subcategory of ethics more generally, but mirrors it, bringing parts of it into sharper focus and illuminating some of its most secluded recesses. The study of how one learns to deal with secrecy sheds light on the paths to becoming more aware of one's self among others, and thus of the possibility of moral choice.
>
> ***Secrets: on the ethics of concealment and revelation*** (Sissela Bok, 1983).

Entre os atos de informar e não informar estão contidas decisões de natureza política e técnica. Notícias jornalísticas, leis, instruções, artigos científicos, bulas de remédio, livros de história, revistas, poemas e, enfim, comunicações privadas consideram, em alguma medida, o que quer ser comunicado, como, para quem e a partir de que permissões tecnológicas e restrições de ordem regulatória. Políticas da informação são sintomas do desenvolvimento técnico e de como os atores públicos e privados, individuais e coletivos, encaram as possibilidades comunicacionais de um determinado tempo e espaço.

Como peça-chave desse mosaico de políticas da informação, que reúne camadas decisórias governamentais (planejamento econômico, geopolítico e de segurança pública), acadêmicas (investigação e desenvolvimento científico), comerciais (mercantilização da técnica) e sociais (exercício de liberdades e direitos fundamentais), a criptografia representa os cruzamentos e conflitos entre os interesses dos variados setores. Essas interconexões - que envolvem, a grosso modo, uma ciência política relativa ao desenvolvimento tecnológico e os interesses multissetoriais impressos - compreendem o que, atualmente, convenciona-se chamar de Governança da Internet[1]. Essa governança é sintomática dos níveis de apropriação das técnicas por esses atores, ora representando

[1] Ainda que a criptografia encontre amplo desenvolvimento em uma sociedade pré-Internet, a presente dissertação buscou, sempre que possível, contextualizá-la a partir de uma perspectiva que ora agrega e ora contrapõe perspectivas setoriais - portanto de abordagem "multissetorial" - que leva em consideração as construções de políticas de tecnologias de interesse público e que melhor se enquadra em uma ciência política advinda da Governança da Internet (Kurbalija, 2015; DeNardis, 2014).

uma considerável convergência de interesses, ora um conflito inter-setorial duradouro que pode resvalar, entre outros efeitos, em restrições ao desenvolvimento tecnológico, em expansão de potencialidades de vigilância dos Estados e em violações ao ecossistema de direitos humanos em âmbito global. A criptografia, portanto, inscreve-se em uma arena de interesses relativos a essa governança.

Phillip Rogaway (2015), em seminal ensaio sobre o "caráter moral do trabalho criptográfico", é assertivo ao afirmar que a "criptografia rearranja o poder: estabelece quem pode fazer o que, a partir de que". Isso torna a criptografia uma ferramenta inerentemente política e confere à área uma dimensão intrinsecamente moral. Os conflitos em torno da resistência contra a democratização da criptografia podem significar, portanto, uma reação de proporções globais e sociotécnicas contra um rearranjo de poder que tensiona um *status quo* histórico caracterizado pela imposição da transparência aos governados e pelos gargalos de opacidade informacional aos governantes.

Para os fins deste trabalho, portanto, propõe-se partir da história das cifras para representar as origens (se é que seria possível cravar um marco inicial) das políticas da informação no que diz respeito às suas potencialidades de afastar o acesso por atores indesejados. Interessa, igualmente, lançar uma lupa sobre os fatos históricos narrados, na tentativa de encontrar aspectos políticos no uso das cifras, quer dizer, atentando para como o jogo de cifragem e decifragem de informações e comunicações dizem respeito a disputas e relações de poder.

No entanto, antes de resgatar a história, "começar pelo fim" pode ser pedagógico para melhor compreensão do lugar da criptografia em uma sociedade em rede e conectada, a qual encontra revoluções comunicativas e fluxos de informações ubíquos (Weiser, 1991). Importa notar que essas revoluções, se potencializam as possibilidades industriais, sociais, econômicas e governamentais, por outro lado, geram vulnerabilidades diversas que acompanham o uso da Internet. Para responder a essas fragilidades, a

criptografia se encontra entre as técnicas que melhor representam os esforços para se alcançar um fluxo de dados confiável e seguro pela rede (Internet Society, 2017).

Dessa forma, seria possível afirmar que a criptografia está para o sistema conectado e tecnológico como os anticorpos para o sistema imunológico: caso não esteja suficientemente presente, o corpo - ou a rede - se torna fraco e, nesse caso, suscetível a interferências externas?[2] A confiabilidade de transações financeiras online; certificação de contratos digitais; integridade dos dados em uma cadeia de fornecimento de energia para uma cidade; sigilo para os dados armazenados em um celular ou em um banco de dados comerciais de dimensão multinacional; privacidade sobre o tráfego de informações na Internet, seja um mecanismo de busca, troca de mensagens, conferência de vídeo ou edição de texto; ou autenticidade de usuários para acesso a dispositivos conectados. O dia a dia online, para ser verdadeiramente seguro, depende da criptografia[3].

[2] Posto de outra forma, “We think we're whispering, but we're really broadcasting. A potential antidote exists: cryptography”. (Levy, 2002)

[3] Uma timeline interessante de um “dia a dia” do ponto de vista do uso da encriptação pode ser encontrada no artigo “Your day with Encryption”. (Polk; Fronek, 2019) e na Cartilha “A importância social e econômica da criptografia” (Ramiro; Canto, 2020)

2 REFERENCIAL TEÓRICO E METODOLOGIA

O paradigma teórico de uma ciência política de onde ressalta as históricas fricções que tem por eixo a *encriptação* e o *sigilo* proporcionado (o objeto de análise e seu qualificante) pode ser derivado da Governança da Internet, termo cunhado no âmbito da Cúpula Mundial sobre a Sociedade da Informação. Propõe, portanto, uma abordagem complexa e multissetorial, mensurando diferentes perspectivas, demandas e entendimentos de uma variedade de setores, como o governamental, o mercadológico, o acadêmico e o da sociedade civil organizada. Como consequência, essa abordagem pode ser alocada para um objeto de estudo ainda mais específico - como a própria encriptação - fazendo uso do mesmo método de observação de demandas, discursos e políticas para equacionar quais interesses estão em jogo.

Como referencial de análise de conflitos tendo em vista um ecossistema de governança (bem como os eventuais pontos de equilíbrio entre poderes), portanto, os trabalhos e de Jovan Kurbalija (2016), Laura DeNardis (2014) e Wolfgang Kleinwachter e Virgílio Almeida (2015) foram fundamentais.

De modo a planificar um terreno comum, necessário para estabelecer os pontos de partida relacionados às terminologias técnicas que serão utilizadas ao longo do trabalho, especialmente sobre a ciência da encriptação - e da criptografia de modo geral - uma taxonomia básica foi construída tendo em vista os trabalhos de Dan Boneh e Victor Shoup (2017) e Bruce Schneier (1996). Os nomes são de notório saber mundial no ensino da criptografia e os livros são comumente utilizados em cursos superiores em todo o mundo.

Para resgatar a história da criptografia, exercício que será necessário para dimensionar posteriormente, o ineditismo das regulações modernas e as consequentes reações, o trabalho pioneiro de David Kahn (1973) foi o marco inicial para lançar uma lupa sobre a história da criptografia. Em segundo plano, a atualização necessária dessa

história foi encontrada em Simon Singh (2002). Esses são os dois marcos teóricos mundialmente reconhecidos na narração da história - e das *estórias* - da criptografia.

Quando esse curso histórico encontra as pretensões regulatórias governamentais, sobretudo nos Estados Unidos na passagem dos anos oitenta para os anos noventa, o trabalho de Whitfield Diffie e Susan Landau (2001) documentam com detalhes políticos e técnicos os meandros das tentativas de criar, inventivamente, embargos à encriptação. Será essencial, por exemplo, para entender as propostas do *Clipper Chip* e "custódia de chaves".

Em um salto temporal para a segunda década do século 21, tendo como epicentros dos fatos políticos que irão reacender e conferir novas qualidades às *cryptowars*, ou seja, as revelações de Edward Snowden, o embate entre FBI e Apple e os bloqueios do WhatsApp no Brasil, foram agregadas as contribuições, em primeiro plano, do indispensável Abelson et al (2015), do Center for Strategic and International Studies (2017), do Open Technology Institute (2015) - entre outros *think tanks*, centros de pesquisa e ONGs que irão oferecer análises aplicadas, transversais e altamente qualificadas de políticas públicas - e as contribuições da Audiência Pública convocada pelo Supremo Tribunal Federal (2017). Do ponto de vista das agências de investigação, que irão capitanear as pressões político-legislativas para inserir vulnerabilidades em sistemas de encriptação e, para tal, articular narrativas e metáforas, foram extraídas declarações, principalmente, do *Federal Bureau of Investigation*, do *Department of Justice*, da Polícia Federal e do Ministério Público Federal do Brasil entre 2014 e 2019.

Em seguida, para trabalhar, precisamente, como as narrativas anti-criptografia se articulam e se enquadram em termos linguísticos, políticos, metafóricos e mesmo morais, foram referenciadas as obras de Lakoff e Johnson (1980) e Ervin Goffman (1986). Essa análise aplicada às disputas pela encriptação e, de forma macro, pela privacidade por parte de movimentos e pela comunidade científico-acadêmica, foram extremamente úteis os trabalhos de Phillip Rogaway (2015) e Colin Bennett (2008).

Para pintar um quadro sobre os movimentos sociopolíticos ativistas organicamente construídos no acordar da Internet no começo dos anos noventa, especialmente os *cypherpunk*, os manifestos de Timothy May (1988), Eric Hugues (1993) e Philip Zimmerman (1999) são bastante sintomáticos. No entanto, os trabalhos verdadeiramente biográficos de Steven Levy (2002) e Andy Greenberg (2012) ofereceram uma história detalhada sobre as origens da comunidade, bem como seus esforços e articulações para sustar restrições ao uso da criptografia.

Então, uma estrada foi trilhada para que fosse possível mergulhar no mosaico de leis que regulamentam a proteção ao sigilo no Brasil - que será basilar para, enfim, a projeção legal da encriptação - o referencial dogmático de Tércio Sampaio Ferraz Júnior (1993) é fundante na hermenêutica da Constituição Federal sobre as hipóteses de suspensão ao sigilo. Contemporaneamente, sob o pano de fundo das disputas de entendimento constitucional e infraconstitucional em torno da encriptação e dos bloqueios do WhatsApp no Brasil, os escritos de Rafael Mafei (2002; 2018), Jacqueline Abreu (2018) e Veridiana Alimonti (2018) foram essenciais e, até onde se pôde perceber, os que melhor oferecem ferramentas para enquadrar legal e politicamente os episódios de bloqueios.

Finalmente, para abrir um leque sobre a importância da criptografia para o ecossistema econômico nacional, entre relatórios, levantamentos e estatísticas, foram utilizados, principalmente, documentos da Federação Brasileira de Bancos (FEBRABAN), da Organização para Cooperação e Desenvolvimento Econômico (OCDE) e do Ministério de Planejamento, Desenvolvimento e Gestão. E, no campo, da importância de sistemas robustos de criptografia para o planejamento da cibersegurança nacional, foram utilizados documentos da União Internacional de Telecomunicações (UIT), Agência Brasileira de Inteligência (ABIn) e Gabinete de Segurança Institucional (GSI) da Presidência da República.

Em termos metodológicos, a pesquisa lançou mão de investigação teórica e foi amplamente baseada em revisão de literatura, a partir de abordagem analítica qualitativa e de natureza fundamentalmente interdisciplinar. Sempre foi buscada a interseção e indicação de pontos de contato, por exemplo, entre a literatura proveniente da ciência da computação e aquela produzida pela dogmática jurídica, interseccionando comentários e contextualizações com discursos, relatórios e estudos produzidos por organizações governamentais e não-governamentais.

Foi reservado, sempre que possível, espaço para a análise crítica da documentação, sempre respaldando conclusões com as devidas referências. Além disso, métodos de leitura estrutural foram fundamentais para que fosse possível apresentar um panorama dos trajetos argumentativos dos autores e representações governamentais trazidos como referência dos conflitos em torno da encriptação. Por fim, como uma das transversais do trabalho foi a análise de narrativas, foi pretendido traçar uma história do discurso político - que se dará, pelo menos, em um *continuum* desde o fim da década de oitenta até os dias atuais -, compreendendo seus principais atores e interlocutores, linguagem e o *background* sociotécnico e socioeconômico.

3 A CRIPTOGRAFIA ENTRE A TÉCNICA E A POLÍTICA

3.1 Preparando o terreno: conceitos básicos da criptografia moderna e aplicações cotidianas

Começar pelo fim, como prometido, busca, pelo menos, duas finalidades: dimensionar as aplicações cotidianas da criptografia, em tempo de centralidade das redes digitais para uma inumerável quantidade de atividades da vida em sociedade, e criar um contraste necessário quando ilustradas as disputas políticas cotidianas derivadas das tentativas de representações de segurança pública e investigações criminais em enfraquecer a criptografia. Como resultado, será possível (ao menos se espera) chamar atenção para a seriedade dessas iniciativas das forças policiais e os riscos que oferecem à segurança de infraestruturas conectadas, ao ecossistema de direitos - desde a garantia de direitos individuais e coletivos até devido processo legal - e, enfim, à economia digital.

Em segundo lugar, é proposta uma taxonomia resumida dos termos e recursos centrais no contexto da encriptação de mensagem - onde irá se sobressair o sigilo -, que poderá ser utilizada como glossário técnico. Assim, será possível preparar o terreno básico para, enfim, lançar o desenvolvimento da criptografia na arena das tensões políticas, sociais e processuais.

3.1.1 **Dois conjuntos taxonômicos da criptografia**

O campo taxonômico da criptografia é consideravelmente vasto. No entanto, alguns conceitos são especialmente importantes para se mapear o desenvolvimento dos recursos de sigilo, das suas correlações com o poder computacional disponível para encriptação e decriptação e quais atributos de caráter algorítmico foram conceitualizados para se gerar um fluxograma compreensível sobre as partes de uma comunicação, considerando, principalmente, a segurança do canal de transmissão.

Dessa forma, encontrando terminologias e descrições de significados especialmente em Dan Boneh e Victor Shoup (2017) e Bruce Schneier (1996),[4] chegando-se a um denominador comum entre os autores, temos:

- **Criptografia**: a ciência dedicada às técnicas de manter as mensagens seguras, seja quanto ao sigilo, à integridade, ou à autenticidade, entre agentes que se comunicam por um canal inseguro. E a **criptanálise** se constitui por seu avesso correspondente: a ciência de quebrar o sigilo, a integridade, ou a autenticidade do cifrotexto, seja por força bruta (tentativa e erro) ou por engenharia reversa do algoritmo de cifragem. À criptografia são, frequentemente, associadas as seguintes funções: proteção (i) ao sigilo do conteúdo (ninguém além das partes credenciadas irão vê-lo); (ii) à integridade (o conteúdo chegará ao receptor tal qual foi enviado pelo emissor); (iii) à autenticidade (é garantido que emissor e receptor são, realmente, quem dizem que são); e (iv) à não-retratabilidade[5] (incapacidade de negar que o emissor é, de fato, o autor daquela mensagem). Por fim, a **criptologia** consiste no campo da matemática que assimila ambas a criptografia e a criptanálise;

- **Cifrotexto e purotexto:** cifrotexto é a mensagem em sua forma encriptada; purotexto é a mensagem em sua forma "limpa", decifrada;

- **Encriptação:** aqui, temos uma dupla semântica: é tanto "o problema de como duas partes podem se comunicar em segredo na presença de um adversário" como, simplesmente, o ato de cifrar uma mensagem ao tornar sigiloso seu conteúdo;

- **Decriptação:** o ato de decifrar uma mensagem com a utilização de uma chave privada;

- **Cifra:** é o algoritmo criptográfico, a função matemática utilizada para cifrar ou decifrar uma mensagem (geralmente, há uma função para cada ato). Normalmente, a

[4] Eventuais traduções foram feitas de forma livre. A grande maioria, no entanto, foi selecionada a partir de como a literatura em português vem as utilizando.

[5] A função de não-retratabilidade, um atributo mais contemporâneo à criptografia, é bastante usual em assinaturas digitais, por exemplo.

lógica de funcionamento do algoritmo é mantido em segredo e a revelação dessa função é dada por uma chave, que pode ser pública ou privada;

- **Chave pública:** chave de encriptação cujo algoritmo de cifragem de uma mensagem é disponibilizado publicamente. Qualquer um poderia fazer uso dessa chave para encriptar uma mensagem para uma pessoa que tenha a chave privada de decifragem correspondente. Um sistema criptográfico composto por uma chave pública e uma privada é também chamado de criptografia **assimétrica**;

- **Chave privada:** Chave de encriptação e/ou decriptação cujo conhecimento seja apenas do emissor ou destinatário de uma mensagem Um sistema criptográfico composto por uma chave privada única para encriptação e decriptação é também chamado de criptografia **simétrica.** Como descrito, caso a chave privada seja utilizada apenas para a decriptação de um mensagem encriptada com chave pública, a criptografia é assimétrica;

- **Backdoor:** método de superar ou desviar das formas de autenticação ou outros protocolos de controle de segurança com o objetivo de acessar um sistema computacional ou os dados nele contidos. Especificamente em sistemas de criptografia, é um recurso inserido de forma intencional, como forma de gerar uma vulnerabilidade que pode ser explorada para acessar o purotexto;[6]

Adicionalmente, vale mencionar uma taxonomia à parte, construída por Narayanan (2013), de natureza teleológica, baseada no "propósito" e que articula considerações de contextual político para identificar *para que* determinadas aplicações criptográficas se apresentam. Ainda que, tecnicamente, possam ter as mesmas bases de funcionamento, seriam diferentes a nível social:

- ***Crypto-for-security*:** associada às transações financeiras, por exemplo, para assegurar integridade, autenticidade e sigilo diante dos cartões de crédito. Uma chave, igualmente, para o desenvolvimento do *e-commerce*. Aqui, tem-se um alinhamento de

[6] Essa definição, excepcionalmente, está em Wysoal e Eng (2010).

perspectivas e coincidem as demandas entre setores, havendo mais incentivo e sucesso na manutenção - e avanço - de sua robustez.

- ***Crypto-for-privacy***: normalmente carrega objetivos políticos e sociais e, por isso mesmo, traz divergências setoriais quanto aos incentivos para que se mantenha. Essa categoria ainda se subdivide em duas outras: ***pragmatic crypto,*** o emprego de criptografia que compreende que a migração de atividades cotidianas para ambientes online se inserem em uma lógica de vigilância e monitoramento, acarretando riscos à sociedade. Portanto, busca *manter* um nível de privacidade de um mundo pré-digital ao afastar esse perigo através da criptografia; e a ***cypherpunk crypto***,[7] a materialização de uma visão ideológica que busca, através da criptografia, *provocar* mudanças sociais, econômicas e políticas estruturais, desestabilizando um histórico poder governamental e de instituições tradicionais.

3.1.2 **Criptografia e sociedade: ubíqua, cotidiana e essencial**

A criptografia é tão presente nas dinâmicas sociais e econômicas de uma sociedade quanto forem presentes a Internet e o acesso a tecnologias de forma geral. Desde a estabilidade de sistemas de informação industriais, de entidades governamentais ou sociais, incluindo a transmissão e o armazenamento de dados em servidores próprios ou contratados, passando pelo tráfego cotidiano de dados na Internet entre serviços, provedores de conteúdo e usuários (Polk; Fronsec, 2019), a cada transações bancárias efetuada no ecossistema financeiro ou para proteger a liberdade de expressão de cidadãos: a criptografia é ubíqua (Weiser, 1991) enquanto elemento chave nos protocolos de segurança da informação embarcados em sistemas.[8]

---

[7] Uma análise mais atenta sobre o movimento *cypherpunk* pode ser encontrada no tópico 3.4.

[8] A extensão das aplicações de criptografia são tão vastas que não caberia, nesse momento, uma taxatividade exemplificativa e extensiva. De toda forma, um levantamento de sua importância para os setores econômico e de cibersegurança, especialmente, foi endereçado no Capítulo 7.

Nem sempre, no entanto, isso acontece de forma deliberada: idealmente, em termos de protocolos de proteção de dados, a encriptação do tráfego e do armazenamento de dados é fornecida *por padrão* e *desde a concepção* (European Commission, 2021) em serviços tecnológicos. Quer dizer que há um elemento *cultural* no uso da criptografia, ou seja, o ecossistema da Internet, complexo, multifacetado e composto por incontáveis atores de interesse, elenca, como boas práticas operacionais, a existência de processos e técnicas que garantam a resiliência e a confiabilidade da rede (Internet Society, 2016) Ainda assim, tecnologias de criptografia podem ser agregadas a serviços como recursos adicionais de segurança, a exemplo da encriptação do conteúdo de e-mails através de PGP (*Pretty Good Privacy*) (Zimmerman, 1999) ou através de aplicações de criptografia de discos rígidos, seja de celulares ou computadores. Caso os e-mails sejam extraviados, acessados por terceiros maliciosos, ou os dispositivos sejam furtados, haveria uma camada extra de segurança afastando o acesso não autorizado.

Resgatando os atributos elementares oferecidos pela criptografia - sigilo, integridade, autenticidade e não-retratabilidade - a revolução tecnológica e a inovação exponencial simbolizada pela digitalização de serviços e disrupção provocada por novas formas de informação e comunicação simplesmente não se cumpririam. Ausentes as formas de proteger a integridade das informações, ordens e transações bancárias seriam mais facilmente adulteradas, mapas de tráfego aéreo ou terrestre poderiam causar colisões, o provimento de energia de uma cidade poderia colapsar; ou a contagem de votos de uma eleição manipulada, levando a uma crise democrática (Aranha et al, 2018). Não protegida a autenticidade e a não-retratabilidade de mensagens, a identidade de consumidores poderia ser facilmente falsificada e, com isso, cartões de crédito clonados; e-mails e comunicações em outras aplicações poderiam ser enviados em nome de terceiros; contratos assinados digitalmente seriam questionados na justiça, esvaziando os negócios jurídicos e seus elementos de confiança; a autenticação de assinaturas digitais seriam adulteradas, podendo gerar crises imobiliárias, eleitorais, cartorárias e processuais de forma geral (Trinta; Macedo, 1998).

Por fim, o sigilo assegurado pela encriptação de mensagens, caso não garantido, levaria a chantagens de caráter econômico, psicológico ou físico em razão de informações sequestradas; governos autoritários exerceriam mais facilmente o monitoramento das comunicações para restringir conteúdos, discursos e silenciar dissidências políticas, erodindo o debate democrático (Global Partners Digital, 2017).[9] Logo, a privacidade, cuja efetivação é fortalecida - e tornada essencial - através do sigilo criptográfico, seria diluída. O objeto de proteção aqui, portanto, é a essência formadora da subjetividade, da personalidade e da identidade (Bruno, 2013).

Por isso mesmo, o sistema tecnosocial da encriptação agrega elementos tão complexos que a projeta como uma tecnologia, fundamentalmente, tecnopolítica. Então galvaniza potencialidades pautadas na autonomia informacional para fazer um contraponto a desigualdades estruturais, como aquelas observadas na relação entre indivíduo e Estado, entre o indivíduo e o capital privado, sendo o indivíduo, aqui, unidade hipossuficiente diante da máquina administrativa governamental e do poder econômico. Portanto, sob um paradigma social democrático, é possível mirar a encriptação enquanto constelação tecnológica ampla, que põe em jogo questões sobre como tecnologias "contestam" e se relacionam com questões relativas à democracia, privacidade e relações de poder (Monsees, 2020).

O próximo tópico, portanto, inicia uma jornada histórica para desaguar nos desafios contemporâneos que tem por eixo as políticas de encriptação. Na medida em que uma reestruturação de poder é provocada em razão da popularização da criptografia - e, assim, pelo re-balanceamento dos níveis de opacidade (comumente levada à cabo pelo Estado) e transparência (geralmente exigida à população)[10] informacional, o Estado

---

[9] Duas metáforas literárias são oferecidas por Daniel Solove para explorar um Estado de vigilância total (que aqui pode facilmente ser identificada como o sigilo das comunicações violado). Um é *orwelliano*: diante de um monitoramento totalitário obsessivo, o indivíduo é levado à completa inibição; o outro é *kafkiano*: diante da construção de dossiês ocultos sobre indivíduos, cujos dados e inferências são desconhecidos, gera-se sentimentos de incapacidade, frustração e desesperança (Solove, 2011).

[10] A filosofia por trás da falácia argumentativa de que "quem não deve não teme" ou de quem, ilusoriamente, alega "não ter nada a esconder" é curiosamente desenvolvida pelo que ficou conhecido como o "Filósofo da NSA", um promotor da "transparência total". Interessantemente, após minucioso trabalho de

reagirá com recursos reguladores e retóricos. Diante das "respostas às reações", forma-se uma rede de tensões que resultarão em projetos de lei, decisões judiciais e articulações político-econômicas que desafiaram a resiliência da encriptação.

3.2 *Fiat codex; et facta est potere*[11]: uma breve história das cifras e suas relações de poder

Para se chegar aos conflitos modernos em torno da criptografia, sobretudo àqueles mais notadamente evidentes dentro dos últimos quase trinta anos, propõe-se uma espécie de "arqueologia das políticas de criptografia". O enquadramento do uso de cifras na história nem sempre resultou em tentativas de regulação ou intervenção política. Mesmo assim, é possível lançar, no mínimo, um olhar sobre a linha do tempo e sobre a literatura que resgata a história das cifras e perceber que, com o passar dos séculos, é amplificada sua associação com as relações de poder na medida em que torna mais restrito acesso desautorizado a informações e comunicações de caráter privado.

3.2.1 Civilizações da idade antiga à idade moderna

David Kahn (1967), autor pioneiro na documentação e historiografia da criptografia,[12] aponta que o primeiro registro do uso de cifras remonta do Egito Antigo, há cerca de 4.000 anos, em forma de hieróglifos - sistema de escrita baseado em signos pictográficos: um escriba buscou registrar a história de seu mestre "e, fazendo isso, deu início à história documentada da criptologia. Uma linguagem cifrada, então, é instrumentalizada como técnica de registro de um "dossiê" sobre alguém, o registro de

jornalismo investigativo sobre sua real identidade, é tomado por sentimentos de constrangimento e reclusão (Maass, 2015).

[11] "Haja código; e houve poder". Permito-me propor o neologismo.

[12] É interessante notar que a própria publicação pioneira do livro histórico de David Kahn, em 1967, época em que muito pouca documentação era disponível sobre o tema, é um marco na popularização da criptografia para um grande público que sequer tinha conhecimento da tecnologia, como relata Whitfield Diffie (Schneier, 1996).

um perfil biográfico cujo acesso seria restrito a quem tivesse acesso ou conhecimento à simbologia da cifra aplicada.

Gerhard Strasser (2016) ainda documenta que data de 3.500 anos atrás, da região da Mesopotâmia, o registro codificado de uma receita de matéria prima para a confecção de cerâmica, material economicamente valioso à época. Primórdios, poderia-se dizer, da proteção ao segredo de negócio, da propriedade industrial ou de meios para se garantir a competitividade econômica ou mesmo o monopólio desse setor comercial.

Por volta de 5 a.C., ainda durante a Antiguidade Clássica marcada pela civilização grega, espartanos desenvolveram o que se tornou o primeiro dispositivo intencionalmente fabricado para transmitir mensagens criptografadas. A *cítala*, como ficou conhecido o artefato, baseava-se em uma *cifra de transposição*: consistia em um bastão de diâmetro pré-determinado, ao redor do qual uma fita de couro ou papiro, onde era gravada a mensagem, se envolvia; caso o diâmetro do bastão não coincidisse exatamente com o modelo usado para encriptar a mensagem, essa não faria sentido a quem a interceptasse - ou mesmo ao receptor.

Outro registro memorável de modelo de codificação de mensagens na Antiguidade Clássica é a Cifra de César, como ficou conhecida devido ao seu mais notável usuário, o Imperador Júlio César. Diferente da cítala, a técnica não carregava um artefato, mas uma *lógica* de encriptação e decriptação*,* consistindo em uma *cifra de substituição*[13]*:* a letra da mensagem original era substituída por outras três posições à frente no alfabeto; logo, $c = f$, $m = p$, $t = v$ e assim por diante, muitas vezes com o auxílio de um "quadro de checagem".

David Kahn (1996) nota que o desenvolvimento da criptografia é consideravelmente interrompido no Ocidente - onde, mais tarde, irá encontrar franco progresso na Europa de língua latina - com a queda do Império Romano e vê seu ressurgimento apenas em meados dos anos 1.400 d.C., período promissor em termos de

[13] Descrita pela primeira vez pelo escritor grego Polyibus, ainda que seu primeiro registro de uso tenha sido de Júlio César.

avanços em modelos criptográficos, na documentação de técnicas e na consolidação da criptologia enquanto área de estudo aplicada. Mas, até lá, a criptografia, assim como as artes e o desenvolvimento científico de forma ampla, ficou estagnado, ao uso de cifras restando associações com "artes ocultas". Kahn ainda observa que isso se deve, em grande parte, a seu uso limitado a manuscritos de rara aparição, na maioria das vezes relacionados ao ocultamento de informações por agentes religiosos e "místicos" associados a ciências pouco populares, como a alquimia e atividades como profecias, adivinhações e feitiços. O estigma perdurou e, até hoje, a cultura popular relaciona o surgimento de textos cifrados a artes ocultas, espionagem ou narrativas de ficção científica.[14]

No entanto, ainda que o uso de cifras remonte a civilizações da antiguidade, a descoberta e documentação sistemática da criptologia, com o registro de métodos de encriptação criptanálise, é devida à cultura árabe. Segundo a história traçada por Kahn (1967), a incursão do povo árabe à Europa, a partir dos anos 600 a.C., sobretudo à península ibérica, onde encontrou o alfabeto latino, fez florescer ciências médicas, a matemática, a produção artística, experimentos científicos, a administração - e a criptologia. A própria etimologia do verbete *cifra* - ou *cipher,* em inglês - deriva da união, a princípio, de *cifr* ("zero", em árabe) e, depois, *cifre* (também "zero", em francês antigo), palavra que irá ganhar terreno a partir de 1.400 a.C. Em compensação, o radical de "criptografia" e "criptologia", *cript-*, resgatam o grego *kryptos* e *kryptein* (para, respectivamente, o adjetivo "escondido" e o verbo "esconder"). Daí derivam palavras como *cripta, encriptação* ou *críptico.*

Kahn (1967) chama atenção para o que seria, até então, o primeiro registro escrito descritivo de conhecimentos sobre criptografia e que esteve presente em uma robusta enciclopédia do ano de 1.412 a.C., de 14 volumes, o *Subh al-a 'sha.*[15] O livro, que

[14] Basta notar obras da literatura como o *Escaravelho de Ouro* (Edgar Allan Poe, 1843); *O Nome da Rosa* (Umberto Eco, 1980); *O Código Da Vinci* (Dan Brown, 2003); ou, mais recentemente, *Cryptonomicon* (Neal Stephenson, 1999), para ficar apenas nos livros. No cinema, *Sneakers* (Phil Alden Robinson, 1992); *Uma Mente Brilhante* (Ron Howard, 2002); ou *Pi* (Darren Aronofsky, 1998), para citar só alguns.
[15] Para informações mais detalhadas, ver Al-Suwaiyel (2018).

buscou cobrir variadas áreas do conhecimento, contava com uma seção de criptologia chamada “Sobre a ocultação em palavras de mensagens secretas”.[16] No entanto, Al-Kadit (2012) sustenta que a contribuição dos árabes, de acordo com manuscritos mais recentemente descobertos, é ainda mais antiga do que o registro de Kahn: as origens da criptologia remontariam ao cientista árabe do século 9, Al-Kindi, o mais antigo registro documentado em livro, além de ser o mais antigo registro do uso de inferências estatísticas (Broemeling, 2012), método básico de criptanálise.

A esta altura, interessa notar que a prática criptográfica, em maior ou menor grau a cada período histórico, esteve associada a codificação de mensagens governamentais relativas a estratégias de guerra, segredos de negócio, sigilo de informações de caráter religioso ou ocultamento de registros científicos, registros de informações biográficas de altas cúpulas do poder e outras expressões culturais que conotam relações políticas entre civilizações e territórios. O uso de cifras significava, portanto, um ferramental político que provia a capacidade de determinar quem teria acesso a determinadas informações. Se para Langdon Winner (1986) artefatos são codificados, construídos e pensados a partir de um ponto de partida político e moral determinável, a criptografia, portanto, não é uma ciência “apolítica”, fria, “higienizada” ou um mero quebra cabeça para deleite dos matemáticos, como sugere Rogaway (2015), mas guarda estreitas correlações com um desenho político de sociedade pretendido.

Isso se torna mais claro a partir da análise do papel das relações diplomáticas para a burocratização do uso da criptografia, o que consolidou a importância da encriptação de comunicações para a geopolítica internacional, sobretudo em tempos de conflito entre nações (Kahn, 1967). Em meados dos séculos 15 e 16, cidades italianas, em especial Veneza, eram bastante representativas na institucionalização de setores da administração pública dedicados exclusivamente ao desenvolvimento de novas cifras, à decriptação e à encriptação de mensagens. Essa burocratização é claramente representada com a criação de “secretarias de cifras” (Iordanou, 2018; Kahn, 1967).

[16] Tradução livre.

Considerando a crescente funcionalidade da criptografia nas práticas comunicativas da administração pública, também é consideravelmente documentado seu uso pelos Estados Papais, ainda na região italiana e durante o mesmo período histórico, sendo o primeiro manual europeu sobre criptografia uma compilação de cifras que teria servido ao papado de Clemente VII (Britannica, 2021). Gradualmente, os manuais sobre o vocabulário de códigos, chamados "nomencladores"[17], espécies de memorandos de cifras, ganharam cada vez mais espaço nas atividades políticas e os setores de comunicação diplomática de basicamente todos os Estados europeus, durante o século 20, contavam com os seus (Britannica, 2021).

Como relatado, a relação entre o desenvolvimento da criptografia e as atividades de caráter político, administrativo e burocrático se estreitaram na medida em que os meios de interceptação e criptanálise se tornam mais sofisticados, pondo em risco o sigilo de comunicações sensíveis e estratégicas. Ao longo dos séculos 19 e 20, sobretudo nos espaços marcados por guerras e tensões geopolíticas de conflito, essa correlação se torna, seria possível dizer, indissociável, sobretudo quando relacionada ao desenvolvimento e massificação do uso de tecnologias de comunicação como o rádio e o telégrafo. Como sugere Kahn (1967), sem as grandes guerras e as disputas diplomáticas, a criptografia não teria influenciado tanto os eventos globais.

3.2.2 **Centralidade da criptografia em tempos de guerras**

Além do contexto sociopolítico entre Estados enquanto motor de transformações em sistemas cifras e dispositivos criptográficos, o advento de novas infraestruturas de comunicação igualmente revolucionaram o status da criptografia. Desde a comunicação escrita em pedras e madeira, como descrito, passando pelo telégrafo, rádio e, então, Internet, a praticidade sobre o trânsito de mensagens é reconfigurado e, consequentemente, as capacidades de interceptação das comunicações são renovadas.

[17] Tradução livre. "Nomenclators", no original em inglês.

Isso ocorre em razão da quantidade e da natureza dos intermediários para a administração desses sistemas de transmissão.[18]

Durante a segunda metade do século 19, o telégrafo foi naturalmente instituído como meio de comunicação da época e, para Kahn (1967) "fez da criptografia o que ela é hoje".[19] Muito disso se deve a sua função central durante a Guerra Civil Americana - com destaque para o uso das cifras de disco, além do surgimento das "cifras de campo". O acesso às redes telegráficas foi um importante condicional à vitória da União sobre os Confederados (Wilhem, 1999), bem como o amplo uso de mensagens encriptadas por essas redes, detidas principalmente pela União, em Washington (Benson, 2011).

Mesmo assim, a própria natureza técnica do meio telegráfico - através de fiação - tornava a comunicação ainda "grampeável", o que fez com o que a tecnologia estimulasse o desenvolvimento de novos métodos de criptanálise. Ao mesmo tempo, refletia-se sobre meios de comunicação menos dependente de infraestruturas físicas. Além disso, o sistema físico de fiação do telégrafo abria possibilidades de sabotagem no curso de conflitos, por exemplo.

Comunicações por telégrafo ainda foram consideravelmente utilizadas durante a Primeira Guerra Mundial (The National Archives, 2021). Ao passo que esses canais de comunicação se tornavam cada vez mais interceptáveis, o papel dos criptanalistas durante a Guerra foi determinante para o desfecho dos conflitos. Destaque dessa importância foi a decifragem de uma mensagem alemã, no episódio que ficou conhecido como o "Telegrama de Zimmerman", crucial para o envolvimento dos Estados Unidos na guerra e, consequentemente, decisivo para a vitória dos Aliados sobre as potências Centrais

[18] Assim, é levantada a questão: dada uma certa tecnologia de mensagens, o canal de comunicação - elemento central nas soluções criptográficas - gera confiança entre as partes? Essa pergunta alimenta a ideia, na criptografia moderna, de afastamento do intermediário entre dois pontos de comunicação.

[19] O "hoje" de David Kahn se refere à criptografia pós-Segunda Guerra Mundial. De toda forma, o impacto da frase traduz como o telégrafo implicou na sofisticação da criptografia, considerando as guerras pelas quais passou, bem como a sua contribuição para a popularização da cifragem de mensagens: *"The great and widely felt need for secrecy awakened the latent interest in ciphers that so many people seem to have, and kindled a new interest in many others. Dozens of persons attempted to dream up their own unbreakable ciphers. Their contributions enriched it with dozens of new cipher systems"* (Kahn, 1967)

(Holler, 2009). Para Barbara Tuchman (2016), a decifragem da mensagem alterou o curso da história.

Enquanto o desenvolvimento da criptografia passava por um "intervalo" quanto à criação de novas cifras, outra revolução comunicacional, mais uma vez, reiniciou o jogo político e recarregou as possibilidades de encriptação de mensagens. No desfecho do século 19, o rádio tomou a cena das tecnologias comunicacionais, reduzindo consideravelmente os custos com manutenção de infraestruturas físicas - afinal, não demandava milhares de quilômetros de fiação e manutenção de aparatos de segurança ao longo de sua extensão. Singh (2001) narra a chegada e a centralidade do rádio a partir da perspectiva, em especial, dos militares, pois a técnica possibilitaria, por exemplo, que generais se comunicassem com batalhões em movimento a partir de seus postos de comando, assim como comandantes navais poderiam se comunicar, de terra, com suas frotas.

Singh (2001) assinala que a potencialidade do rádio, por sua natureza técnica baseada em ondas no espectro eletromagnético, também seriam sua maior fraqueza: mensagens não só chegariam a seus destinatários, mas também poderiam ser recebidas por potenciais inimigos que tivessem descoberto as frequências de transmissão. Ou seja, facilita a comunicação, torna-a mais prática - e facilita sua interceptação.[20] Essa realidade alimentaria a necessidade de uma comunicação segura a partir de um método criptográfico suficientemente resiliente, ou seja, indecifrável pelos intermediários e receptores indesejados.

A comunicação por rádio foi dominante para as atividades militares durante toda a Segunda Guerra Mundial (Gagliarducci, 2020). Adicionalmente, revoluções históricas para a criptografia foram observadas no período. A década de vinte do século vinte e um foi marcada por uma série de desafios postos por inventores de máquinas de cifragem que levaram a um sólido desenvolvimento em técnicas de encriptação e criptanálise.

[20] Uma característica que se tornará padrão com as demais tecnologias que ganharam maior desenvolvimento durante o século 20, das redes de telecomunicações à Internet. E, curiosamente, a partir das quais o uso da criptografia se tornará mais fundamental - e problematizado.

(Britannica, 2021). As "máquinas de rotor", em especial, se destacaram no desenvolvimento de tecnologias de criptografia, sendo desenvolvidas em paralelo em várias países, como nos Estados Unidos, por Edward Hebern, e por pesquisadores europeus, como Hugo Kock, na Holanda, e Arthur Scherbius, na Alemanha - este último dando origem à conhecida máquina Enigma, utilizada pelas forças do Eixo, especialmente pelo Estado Nazista (Crypto Museum, 2021).

Interessa notar que, após a Primeira Guerra, políticas nacionais de pesquisa e fabricação criptográfica se destacaram, respectivamente, em dois países europeus[21] (para além do envolvimento inglês, que será narrado mais à frente). Na Polônia - em difícil condição territorial, cercada pelo regime comunista russo em franca ascensão e pela Alemanha nazista com claras pretensões expansionistas - foi criado o *Biuro Szyfrów* (Departamento de Cifras); na Alemanha - recém derrotada e tendo visto suas comunicações continuamente interceptadas pelos ingleses - com a política industrial de fabricação em massa da máquina Enigma e sua inclusão por padrão em comunicações do exército, da marinha e da aeronáutica nazistas, resultando na manufatura de mais de trinta mil máquinas ao longo das décadas de 30 e 40 (Kahn, 1973; Singh, 2001)[22] A Alemanha se tornou a potência em segurança comunicacional durante anos, influenciando, em larga escala, o sucesso de sua campanha durante a Segunda Guerra Mundial.

A política polaca baseada na criptanálise foi liderada pelo matemático Marian Rejewski, responsável pela engenharia reversa que desvendou o funcionamento básico inicial da Enigma e pelo desenvolvimento inicial das *bombs,* máquinas de decifragem das chaves criptográficas do sistema de comunicação alemão que viriam a desvendar mensagens durante anos a fio, antes do início da Segunda Guerra.[23] Singh (1999) aponta

---

[21] Após a Primeira Guerra, segundo Whitfield Diffie, os Estados Unidos também passam a realizar contribuições fundamentais à criptografia, principalmente a Marinha e o Exército norte-americanos (não coincidentemente, mar e terra serão os campos onde o sigilo comunicacional é crucial - e sensível - na guerra) (Schneier, 1996).

[22] Fato curioso é que a própria publicação pioneira do livro histórico de David Kahn é um marco na popularização da criptografia para um grande público que sequer tinha conhecimento da tecnologia (Schneier, 1996).

[23] Optou-se por não detalhar os processos lógico-matemáticos que desenharam o passo a passo para a superação da Enigma, ou mesmo o funcionamento técnico de seus *scrambles, plugboards* e refletores,

três critérios socio-históricos que mantiveram os polacos determinados em avançar com o investimento em criptanálise: o medo de uma investida alemã sobre seu território; o emprego de matemáticos como centro da execução dessa estratégia; e o papel central da espionagem. Isso por que as primeiras informações que chegaram aos polacos acerca da arquitetura da Enigma foram repassadas por um espião alemão chamado Hans-Thilo Schmidt, codinome "Asche" (Paillole; 2016). Para a Polônia, o investimento em políticas de criptografia era fator-chave para a resistência e manutenção de seu território e de sua soberania.

O aprendizado adquirido pelo Departamento de Cifras foi, eventualmente, herdado pelas forças aliadas, em especial pelos ingleses, quando Hitler invadiu o território polaco. A partir daí, a história é largamente documentada:[24] no Bletchley Park, principal centro de comando para a quebra da criptografia de mensagens nazistas, foi montado um diverso time de matemáticos, enxadristas, linguistas e adictos em quebra-cabeças que chegaram a uma solução final para resolver a lógica da Enigma. Dos profissionais, é amplamente conhecido o papel central de Alan Turing - não somente conhecido como o pai da computação, mas também como um dos maiores expoentes da criptanálise da história (crédito menos reconhecido, na cultura popular, a Turing).

Os avanços derivados da "quebra" da Enigma deram origem a projetos de inteligência de guerra que foram indispensáveis ao desmonte do avanço nazista sobre a Europa e consequente vitória das forças aliadas. É bem documentada, por exemplo, a operação Ultra. Segundo Winterbotham (apud Kahn, 1974), as quebras de mensagens encriptadas (não limitadas às alemãs, mas também às italianas, japonesas etc.), sob

---

principais mecanismos da máquina. Mas pretendeu-se descrever brevemente as principais viradas do jogo em direção à superação do sistema de criptografia usado pelo regime nazista, passando pelos seus principais agentes.

[24] Uma vasta literatura sobre o Bletchley Park e o processo de decifragem da Enigma relacionado ao fim da guerra pode ser encontrada, por exemplo, em Codebreakers: The Inside Story of Bletchley Park (Alan Stripp e Harry Hinsley, 1993); Enigma: The Battle for the Code (Hugh Sebag-Montefiore, 2000); The Secret Life of Bletchley Park: The WWII Codebreaking Centre and the Men and Women Who Worked There (Sinclair McKey, 2010); e *Codebreakers' Victory: How the Allied Cryptographers Won World War II* (Hervie Haufler, 2003). E em filmes como O Jogo da Imitação (Morten Tyldum, 2015) ou Enigma (Michael Apted, 2001).

responsabilidade da operação, foram responsáveis por sabotar as linhas de suprimentos das forças nazista na campanha de Erwin Rommel do norte da África; por prover informações suficientes para a resistência das forças aliadas em praticamente toda a região do Mar Mediterrâneo; além de fornecer detalhadas informações, meses antes do "Dia D", sobre a posição das tropas nazistas ao longo da costa francesa, para citar apenas alguns resultados.

É seguro concluir que as políticas de guerra baseadas no desenvolvimento e uso de recursos criptográficos foram determinantes para, por um lado, o relativo sucesso da expansão das forças do Eixo durante boa parte da Segunda Guerra. Ao mesmo tempo, seria igualmente correto assumir que também foram fundamentais para o arremate das forças aliadas e, consequentemente, para o fim da Segunda Guerra. Na realidade, a observação da criptografia enquanto elemento chave de estratégias nacionais e geopolíticas de expansão e resistência territorial podem ser vistas em toda a história, desde a antiguidade clássica, passando pela Idade Média, até encontrar a sociedade de modelo econômico-industrial do século 20.

O jogo político informacional permitido pela matemática das cifras carrega o poder de influenciar o curso da história e está intimamente relacionado às possibilidades tecnológicas - estas associadas ao desenvolvimento matemático do poder computacional, ao processamento de informações e à segurança - autenticidade, confidencialidade e integridade - dos sistemas comunicacionais. Essa acepção é bem compreendida, com mais nitidez, com o término da Segunda Guerra, e vai influenciar políticas regulatórias do uso da criptografia durante a Guerra Fria, cenário esse que irá conferir um estigma bélico à criptografia durante décadas a fio. Como será analisado, esse cenário passa a ser revolucionado pela capilarização da Internet comercial, por demandas mercadológicas civis e por divisores de água científicos que irão reconfigurar o acesso à criptografia durante a segunda metade do século XX.

4 A INTERFERÊNCIA ESTATAL NO CÓDIGO E A CRIPTOGRAFIA ENQUANTO OBJETO DE REGULAÇÃO

4.1 Pós-guerra fria: a matemática regulada como munição bélica

No pós-Segunda Guerra, uma herança militar recaiu sobre a criptografia e implicou em um modelo de controle industrial de desenvolvimento tecnológico, durante toda a Guerra Fria, centrado nos Estados Unidos, principal potência econômica à época. Esse modelo baseava-se, em grande parte, em uma mentalidade de desenvolvimento econômico voltado à segurança nacional, o que acabou por estabelecer controles sobre discursos, mídia e desenvolvimento científico - este último representado por restrições rígidas ao desenvolvimento e exportação da criptografia (Diffie; Landau, 2001). Em razão da conjuntura histórica do pós-Segunda Guerra, que posiciona os Estados Unidos na liderança da economia e da indústria mundial, este sub-tópico, portanto, busca focar nas características regulatórias da criptografia tomando como ponto de partida o cenário norte-americano.

Por muito tempo, a criptografia de ponta era de uso e propriedade, em grande medida, exclusivos do poder militar. Por essa razão, o modelo regulatório dos primeiros anos do pós-guerra a colocava na categoria de *munição*, estando sob responsabilidade do *Department of State* o regime de controle de exportação de sistemas de criptografia. Esse controle se concentrava, mais especificamente, no *Office of Defense Trade Controls* - antes chamado de *Munitions Control Board* - do qual participava a *National Security Agency* (NSA) (Grimmet, 2001). Sua regulação, portanto, era mais severa do que produtos mais diretamente associados a uma destinação comercial.

O modelo de controle passou, gradualmente, a deixar de fazer sentido na medida em que a revolução comunicacional passou a desempenhar considerável papel na indústria norte-americana. Ocorre que, seria possível argumentar, a criptografia não confere uma importância primordial à comunicação analógica, face a face, a qual pode

fazer uso de técnicas de autenticação e sigilo mais elementares, como o reconhecimento de voz, dupla conferência de números de identidade e dados cadastrais, entre outros. Caso essa fosse a realidade da comunicação, poderia-se justificar uma restrição governamental uma vez que a criptografia não seria tão central à segurança da comunicação de massa. Por outro lado, para a comunicação entre softwares e hardwares - em aceleração exponencial no *background* industrial dos Estados Unidos à época (e em outras regiões do mundo também, como na Europa e na Ásia) - sistemas de segurança e robustos algoritmos de criptografia passaram a ser uma necessidade elementar e expandida.

Paralelamente, a regulação sobre determinadas tecnologias, de forma a limitar seu acesso e torná-lo mais seletivo, impõe desafios de ordem econômica e geopolítica para os Estados. Isso quer dizer que nem sempre é eficaz tornar seu acesso restrito puramente em razão de uma competitividade tecnológica com outros países. Eventualmente, outros Estados nacionais produzirão pesquisa e desenvolvimento científico que levarão a sua autonomia quanto ao acesso, por exemplo, de softwares e hardwares suficientemente seguros[25], encabeçando, inclusive, mercados internacionais e domésticos. Os Estados Unidos assumiram essa conjuntura histórica e relaxaram suas regras, entre outros motivos, para não frear sua liderança na indústria de computadores (Diffie; Landau, 2001).[26]

Essa realidade impôs uma revisão do status de "munição" da criptografia: torna-se mais claro seu caráter de "uso duplo"[27] em função de uma considerável e crescente destinação civil à criptografia, o que diluiria sua conotação militar para também ser considerado o uso comercial. A partir do caráter de "uso-duplo", testes de ponderação

[25] Esse argumento se mantém fazendo sentido em conflitos envolvendo desenvolvimento e aplicação de criptografia mais contemporâneos, como os narrados nos capítulos seguintes.
[26] Mais alguns fatores são citados como justificativas para a revisão do modelo regulatório. Entre eles, para uma empresa de software e hardware norte-americana se verdadeiramente competitiva, deve ter um bom alcance no mercado internacional; para que o produto seja confiável, é importante que o sistema de segurança seja construído *by design*, não sendo recomendável agregá-lo *a posteriori*; é bastante custoso e complexo fabricar duas versões de um produto (um para o mercado internacional e outro para o doméstico, por exemplo), além de passar a mensagem, para o consumidor internacional, de que a empresa não está oferecendo seus melhores produtos.
[27] *Dual-use,* na categoria original para o regime regulatório da época.

poderiam ser feitos a cada produto criptográfico analisado, levando-se em conta a destinação comercial do produto, e passa a ser mais célere e simples o processo administrativo para concessão de licença. Caso identificada a destinação "não militar", o processo era transferido para jurisdição do *Department of Commerce*, flexibilizando os mecanismos de controle (Landau e Diffie, 2001). Fator que contribuiu para esse relaxamento foi o término da Guerra Fria entre o fim dos anos oitenta e começo dos anos noventa, baixando a pressão da atmosfera bélica e da tensão armamentista que habitava a racionalidade geopolítica norte-americana.

Mesmo assim, o papel das agências de inteligência, em especial da NSA, eventualmente buscaram frear o uso e aplicação plenamente livres da criptografia, propondo políticas públicas que impusessem limites à sua robustez. Essa será a gênese da entrada das políticas de encriptação no debate público.

4.2 Políticas públicas medidas em *bits* e *backdoors*

> "Somos a favor da criptografia forte, da criptografia robusta. O país precisa disso, a indústria precisa disso. Apenas queremos ter a certeza de que teremos um alçapão e uma chave sob a autoridade de algum juiz, através da qual poderemos acessar se alguém estiver planejando um crime."[28]

Se, em termos de competitividade industrial, passou a ser desafiador convencer o público de que seria necessário manter rígidos controles sobre a exportação, outras formas de interferência passaram a ser mais palatáveis por sua discrição, especificamente a partir de políticas de interferência direta no código criptográfico. Ainda haveria espaço, portanto, para advogar por um progresso dos algoritmos de criptografia que não "esvaziassem", completamente, poderes de inteligência governamental.

Uma das tentativas de acompanhar a massificação do uso da criptografia sem ameaçar capacidades tradicionais de inteligência e controle do Estado se deu a partir de

[28] Discurso do então Diretor do FBI, Louis J. Freeh, em 1995 (Cohn, 2014).

uma articulação entre a *National Security Agency* e a *Software Publishers Association* (SPA). Para que os produtos recebessem uma aprovação de exportação simplificada, suas chaves de encriptação não poderiam exceder 40 *bits*.[29] A "solução" passou longe de pacificar os interesses e desafios envolvidos no uso de criptografia no mercado de massa: críticos apontavam que a medida não passava de uma falsa sensação de segurança (Garfinkel, 1992).

Ao mesmo tempo, considerando a cultura policial, em um cenário em que uma parcela mínima da população civil utiliza criptografia, agências de investigação podem agir de forma a marcar como "suspeitas" comunicações encriptadas, estabelecendo, portanto, um critério simplório para determinar se uma comunicação seria interessante para fins de interceptação. Mas, ao passo em que sistemas de comunicação encriptadas se massificam, ainda que com um algoritmo fraco, a lógica da suspeição perde o sentido (ou, pelo contrário, todas as comunicações passam a ser suspeitas)[30], o que extrapolaria as capacidades técnicas de interceptação. Logo, a liberação de uma encriptação fraca ainda ameaçava uma cultura tradicional de investigação que facilitava, tecnicamente, o acesso às comunicações.

Como resultado - após controles de exportação e limitações ao tamanho da chave criptográfica - a *National Security Agency,* em 1993, uma vez mais apresenta proposta que, a uma só vez, parece avançar em termos de segurança e mantém a NSA um passo à frente de todos: propõe um algoritmo de encriptação com tamanho de chave de 80 *bits*[31] para as comunicações - teoricamente mais seguro do que o padrão da época - com uma porta dos fundos, ou um *backdoor*, uma entrada excepcional para acesso permanente do

[29] O tamanho ou o comprimento da chave, medido em *bits*, é um dos principais parâmetros de segurança de um sistema criptográfico. Geralmente, as recomendações técnicas em termos de exigências de segurança passam por sugerir comprimentos mínimos para que um sistema seja considerado suficientemente confiável (BlueKrypt, 2021; ICP-Brasil, 2020).

[30] Seria possível sugerir que esse raciocínio é a gênese de uma racionalidade de inteligência governamental que leva a programas de vigilância em massa, que pode ser encarada como um produto da saturação - ou do surto - das tradicionais capacidades técnicas de vigilância associadas a questionáveis critérios de suspeição. Esse raciocínio pode ser complementado em Diffie e Landau (2001).

[31] Uma crítica de fôlego, tendo como ponto de partida o tamanho da chave criptográfica, pode ser encontrada em publicação de cientistas da computação especialistas em criptografia à época (Blaze et al, 1996).

governo. A iniciativa ficará conhecida como o *Clipper Chip* e dará os contornos das "guerras criptográficas" (comumente conhecidas como *Cryptowars)* que perduram até os dias de hoje.[32]

Diffie e Landau (2000) narram que, entre 1996 e 1998, nova política foi proposta, segundo a qual produtos com sistemas de criptografia que não excedessem 56 *bits* poderiam ser exportados livremente - o que soaria como uma concessão política. Porém, haveriam de se submeter à condição de que as chaves de decriptação fossem previamente depositadas - sistema que ficou conhecido como *key escrow ("custódia de chaves")* - ou que houvesse meios de reter uma chave para acesso governamental - batizado de *key recovery.*[33] Sem sustentação política suficiente e devido à ampla oposição sofrida, tanto proveniente do mercado, quanto por parte dos defensores dos direitos civis e da comunidade acadêmica e científica especializada, as propostas fracassaram. A abordagem regulatória baseada na limitação do comprimento das chaves já se encontrava defasada do ponto de vista industrial e, cada vez, mais do ponto de vista dos direitos dos usuários. Além disso, o mercado internacional já considerava que os produtos deveriam oferecer chaves de encriptação com 128 *bits*.

No relatório publicado pela *National Academy of Sciences* em 1996 - aguardado pela administração de Bill Clinton e resultante de investigação de fôlego, com contribuições de nomes como Martin Hellman e de ex-membros do governo norte-americano - chega-se à conclusão de que a estratégia de política de criptografia do governo era inadequada à "sociedade da informação" da época, colocando a seguinte questão: qual o grau de garantia que o governo pode oferecer de que essas chaves seriam acessadas apenas sob circunstâncias legalmente autorizadas? (Dam; Lin, 1996). Abelson et al (1996), outra publicação paradigmática da época,[34] de co-autoria de alguns dos mais

[32] As disputas narrativas e legais inauguradas com as *Cryptowars* serão melhor exploradas nos capítulos seguintes.

[33] No fim do dia, ambas as expressões significam o mesmo projeto: a inserção de uma vulnerabilidade proposital para acesso governamental.

[34] A publicação será uma antecipação ao seminal estudo "*Keys under doormats*", que conta com a co-autoria de boa parte dos especialistas do estudo de 1996. Não deixa de ser interessante que, vinte anos depois, a disputa sobre o acesso excepcional se repete e será necessário reafirmar os argumentos.

notáveis especialistas em segurança e computação da época, sustenta, detalhadamente, que um sistema de custódia ou resgate de chaves seria inerentemente mais inseguro, mais custoso, e muito mais difícil de ser operacionalizado, implicando em um sacrifício à segurança.

Logo o comprimento das chaves de encriptação deixam de ser um critério central para controle de produtos embarcados com criptografia e, a partir de 2000, softwares destinados ao varejo encontram terreno menos restritivo para exportação (White House, 2000), com poucas exceções.[35] A Electronic Frontier Foundation, das mais notáveis organizações da sociedade civil a antagonizar as restrições à criptografia, avisava, desde o início, que a política simbolizada pelo *Clipper "*é um beco sem saída e aqueles de nós que estão preocupados com a privacidade digital ganharam uma nova oportunidade de moldar uma melhor política".[36]

A saga norte-americana não foi, necessariamente, acompanhada das abordagens regulatórias internacionais. Certos países mantiveram restrições rígidas para o comércio de produtos com encriptação de dados. Outros, em alguns casos, não chegaram sequer a verdadeiramente a considerar a criptografia algo suficientemente popular a ponto de gerar necessidade de regulação (Baker; Hintzel, 1997)[37] Eventualmente, as diferentes abordagens políticas sobre a criptografia poderiam tornar a exportação impraticável, dado que um produto com criptografia de chave de 56 *bits* que tiver permissão para ser exportado em um determinado país pode encontrar regras de importação limitadas a chaves de 40 *bits* em outro país.

---

[35] As regras exportação foram relaxadas, mas o governo norte-americano ainda restringia o comércio de produtos com criptografia a países considerados associados ao terrorismo, como Cuba, Irã, Iraque, Líbia e Sudão (Sanger; Clausing, 2000).

[36] Tradução livre. No original: "Clipper is a dead end, and those of us who are concerned about digital privacy have won a new opportunity to shape a better policy" (Electronic Frontier Foundation, 1994).

[37] Um elemento que traçava uma linha regulatória similar em alguns países era serem membros do acordo de Wassenaar Arrangement (Controle à Exportação de Armas e Bens e Tecnologias de Dupla Utilização), acordo que endereçava uma uniformidade inicial para o controle de munições e de produtos de "uso duplo". Do acordo participavam (e ainda participam) países como Estados Unidos, Japão, Canadá e boa parte da Europa Ocidental (University of Edinburgh, 2021).

Até o ano de 2000 na França, por exemplo, uma empresa que quisesse exportar produtos com criptografia para fins de autenticação ou assinatura digital deveria submeter uma "declaração" ao *Service Central de la Sécurité des Système d'Information*, ao passo que produtos com criptografia para fins de sigilo de dados haveria de submeter um pedido de autorização. Levando em consideração o comprimento de chave, havia necessidade de autorização expressa para criptografia com chaves de 40 *bits* e, caso excedesse, uma análise específica precederia a possibilidade de autorização. O Reino Unido não controlaria o uso de produtos destinados ao mercado de massa e não abordaria o comprimento das chaves. Em compensação, o *Department of Trade and Industry* estabeleceria que o uso de criptografia seria livre desde que houvesse o fornecimento de chaves quando demandado pelo *Secretary of State.* A Rússia estabeleceria um dos regimes mais rígidos sobre produtos com criptografia, controlando sua exportação, importação, uso, venda, e desenvolvimento, podendo banir produtos sem a devida licença e processar aqueles que desrespeitassem as regras (Baker, Hintze, 1997).

Uma visão panorâmica das sucessivas políticas públicas que levassem em consideração o comprimento das chaves sugere que essas estariam fadadas ao anacronismo, invariavelmente, em algum momento. A robustez de um algoritmo criptográfico é medido, entre outros fatores, pelo poder computacional em operação à época de um dado padrão criptográfico. Não seria razoável esperar que a atualização das políticas públicas tenha o mesmo ritmo que a Lei de Moore sugere no que diz respeito à tendência de aceleração exponencial no poder de processamento de computadores. Regulações nesse sentido, dado o passo da sofisticação tecnológica, levaria a um dos caminhos: à ineficiência do próprio regime regulatório, que seria ignorado pela prática comercial, ou à insegurança expansiva dos sistemas informáticos.[38]

[38] Importa notar que regimes de regulação da criptografia baseados em um "teto" para o tamanho de chaves não se esgotam na década de noventa. Mesmo atualmente, o modelo é perseguido em alguns países. Um bom panorama pode ser encontrado no *World Map of Encryption,* da *Global Partners Digital* (Global Partners Digital, 2021) e no *Cryptomap*, do Centro de Ensino e Pesquisa em Inovação da Faculdade Getúlio Vargas - CEPI (FGV Direito SP, 2021).

5 OS MÚLTIPLOS ENQUADRAMENTOS DA ENCRIPTAÇÃO: DA CRIMINALIZAÇÃO AO SÍMBOLO DO EXERCÍCIO POR DIREITOS HUMANOS

5.1 Contexto em três atos: Snowden, FBI *vs.* Apple e bloqueios do WhatsApp

Após os primeiros embates no caso *Clipper Chip* acima narrado - entre representações das forças de investigação norte-americanas, empresas de tecnologia e ativistas - as disputas em torno da criptografia foram reaquecidas em, pelo menos, dois episódios paradigmáticos.[39] Esses fatos políticos se inserem dentro de um contexto mais amplo, de sensibilização generalizada provocada pelas revelações de Edward Snowden.

Como amplamente documentado, em 2013, Edward Snowden, ex-funcionário a serviço da NSA, veio a público denunciar detalhes de programas de vigilância em massa empregados pela agência, como o *PRISM* e o *Bullrun* – este específico para decriptar mensagens - se tornando o *whistleblower* de maior projeção das últimas décadas. Denunciou abusos empregados de forma indiscriminada em forma de monitoramento de milhões de cidadãos norte-americanos e, muitas vezes, de cidadãos estrangeiros (Greenwald, 2014). Autoridades políticas internacionais chegaram a ser alvos de vigilância, a exemplo da ex-presidenta Dilma Rousseff e da chanceler alemã Angela Merkel. O caso Snowden terá o poder de multiplicar o uso de tecnologias pró-privacidade, como a criptografia, gerando um efeito em cadeia e uma demanda, no mercado de tecnologia, por aplicações comprometidas com o sigilo irrestrito das comunicações.

Em 2016, o FBI buscou o auxílio da Apple para ter acesso ao disco rígido criptografado de um iPhone pertencente a um dos responsáveis pelo atentado ocorrido na cidade de San Bernardino, um tiroteio de caráter extremista que deixou 14 mortos. A

[39] Foram eleitos dois enquanto recorte metodológico para esse trabalho: um deles contextualiza o debate a nível global em razão da influência geopolítica dos Estados Unidos; e outro porque insere o Brasil enquanto ator central na dinâmica conflituosa da criptografia.

empresa, então, recusou-se a desenvolver uma solução tecnológica específica para reverter a criptografia empregada em seus aparelhos. Uma disputa político-judicial foi travada, reacendendo o ânimo das agências de investigação norte-americanas para pressionar formuladores de políticas públicas a tornar obrigatória a existência de mecanismos de "acesso excepcional" a sistemas com criptografia. Em outras palavras, um *backdoor* mandatório deveria acompanhar a criptografia em celulares como o iPhone.

No cenário brasileiro, não a criptografia de disco protagonizou a tensão no âmbito de investigações criminais, mas a criptografia ponta-a-ponta utilizada em aplicativos de mensageria. Entre 2015 e 2016, o WhatsApp foi bloqueado por três vezes em território nacional como resultado de ordens judiciais. A penalidade foi resultado da impossibilidade do provedor em fornecer o conteúdo de comunicações em sua plataforma, uma vez que, com a criptografia ponta-a-ponta, apenas mensageiro e receptor das mensagens têm acesso ao conteúdo. As ordens judiciais, no entanto, encararam a impossibilidade como negativa, buscando compelir a empresa através da sanção. O entendimento judicial sobre os bloqueios ainda segue vivo em duas ações que tramitam perante o Supremo Tribunal Federal: a Ação de Descumprimento de Preceito Fundamental nº 403 e a Ação Direta de Inconstitucionalidade nº 5527, que serão tratadas mais adiante.

Apesar de pontos de partida relativamente distintos (criptografia de disco e criptografia ponta-a-ponta), os episódios em ambos os territórios confluíram para o mesmo denominador: o ressurgimento de narrativas "anti-criptografia", baseadas em imaginários distópicos de crise na segurança pública. Os discursos serão bases diretas para a proposição de políticas públicas, em forma de projetos de lei, tanto no Brasil quanto nos Estados Unidos, que buscarão a obrigatoriedade para que autoridades de investigação tenham acesso a dados e comunicações encriptadas.

Por outro lado, os episódios também irão re-energizar a incidência política de organizações da sociedade civil em defesa da privacidade e da liberdade de expressão conferida pela criptografia e, ao mesmo tempo, irá mobilizar setores da comunidade

científica e acadêmica que irão se aproximar dos embates políticos. Esse movimento chama, também, uma "dimensão ética" ao desenvolvimento tecnológico representado pela criptografia e busca consolidá-la enquanto tecnologia fundamentalmente sociopolítica, da qual depende, em última análise, um sistema político democrático.

5.2 A construção do imaginário governamental sobre encriptação: crise permanente e o pretenso colapso da segurança

5.2.1 **Teoria do enquadramento e a metáfora moral da criptografia**

Como outros fenômenos sociais[40], o significado da criptografia não é "auto-apresentado" e sua acepção pode variar a depender de variadas expressões culturais, acadêmicas e, o mais importante para este trabalho, setoriais. Como forma de trazer a variabilidade de percepções, sobretudo em agendas políticas, sobre um dado fenômeno enquanto método de análise, incluindo a forma como é "apresentado" em reformas sociais e agendas políticas, Erving Goffman (1974) desenvolve a concepção de "enquadramento". Em resumo, a teoria do enquadramento sugere que a forma como algo é apresentado a uma audiência tem poder sobre as escolhas que irão tomar sobre um dado fenômeno. No campo da política, por exemplo, a forma como a mídia noticia uma ação governamental influencia a popularidade dessa e, consequentemente, gera uma narrativa própria que pode ser absorvida pela coletividade e, assim, influencia as derivações de uma política pública.

No campo das relações entre privacidade e tecnologia, por exemplo, Colin Bennett (2008) assume que a privacidade não é um fenômeno auto-definido, mas um conceito profundamente contestado e que enquadra uma série de questões sociais e de políticas públicas inter-relacionadas. Bennett irá realizar uma "etnografia" dos defensores da privacidade, sejam organizações ou indivíduos, em variadas localidades do mundo e a

[40] E aqui se defende que a criptografia seja um fenômeno sociotécnico por essência.

partir de distintas agendas políticas (por exemplo, a privacidade como um elemento essencial aos valores liberais ou como direito que se opõe ao capitalismo), explorando, assim, como "enquadram" os desafios impostos à privacidade frente ao desenvolvimento tecnológico e como alcançar políticas protetivas.

Como resultado, tecnologias que se encontram na fronteira protetiva da privacidade, ou do sigilo das comunicações e dos dados, mais precisamente, também irão ser objeto de disputa narrativa, como a criptografia.[41] O ponto de partida para a pressão, por parte das autoridades policiais, em favor de uma criptografia "menos forte" se ancora na justificativa de que investigações criminais estão perdendo suas capacidades de coletar evidências e construir acusações. Isso porque os protocolos criptográficos que vêm sendo empregados em celulares e em aplicações de mensageria não permitem, como em iPhones ou aplicativos como o WhatsApp, que os próprios provedores tenham acesso aos dados armazenados ou interceptem as comunicações.

Logo, a metáfora construída pelo FBI - que será o carro-chefe das investidas contra a criptografia e que será resgatada categoricamente por outras agências de investigação - se pauta na ideia de "obscurecimento"[42] das forças investigativas, ou seja, nada mais conseguiriam ver, estariam ficando "no escuro".

James Comey, então diretor do FBI, e Rod Rosenstein, Procurador-Geral Adjunto do Departamento de Justiça dos Estados Unidos sustentam, respectivamente, que

> *Privacy and security are inherently in conflict. As you strengthen one, you weaken the other. We need to find the right balance. (...) Modern communications technology has destroyed the former balance. It's been a boon to privacy, and a blow to security. Encryption is especially threatening. Our laws just haven't kept up. (...) Because of this, bad guys may win. The bad guys are terrorists, murderers, child pornographers, drug traffickers, and money launderers.105 The technology that*

[41] Tive a oportunidade de me debruçar sobre a visão sociopolítica subjacente às narrativas governamentais sobre criptografia no trabalho "A Construção de Imaginários nas Narrativas Governamentais sobre Criptografia" (Ramiro, 2019). O ponto de partida foi a ideia de que a performática desses discursos constituiriam "imaginários sociotécnicos", conceito cunhado por Sheila Jasanoff (2015).
[42] *Going dark*, no original.

> *we good guys use|the bad guys use it too, to escape detection. (...) At this point, we run the risk of* ***Going Dark****. Warrants will be issued, but, due to encryption, they'll be meaningless. We're becoming a country of unopenable closets. Default encryption may make a good marketing pitch, but it's reckless design. It will lead us to a very dark place. (Comey, 2014)*

> *But the advent of* ***"warrant-proof" encryption***[43] *is a serious problem. Under our Constitution, when crime is afoot, impartial judges are charged with balancing a citizen's reasonable expectation of privacy against the interests of law enforcement. The law recognizes that legitimate law enforcement needs can outweigh personal privacy Concerns (...) But there has never been a right to absolute privacy. (...) Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety. Encrypted communications that cannot be intercepted and locked devices that cannot be opened are law-free zones that permit criminals and terrorists to operate without detection by police and without accountability by judges and juries (...) When encryption is designed with no means of lawful access, it allows terrorists, drug dealers, child molesters, fraudsters, and other criminals to hide incriminating evidence.* (Rosenstein, 2017)

Rogaway (2015) argumenta que os esforços do FBI para relaxar a criptografia fazem parte de um esforço de enquadramento que aposta e lança uma atmosfera do *medo* sobre a audiência: medo do crime, medo de perder a proteção de pais sobre os filhos ou mesmo medo do escuro. Na opinião do autor, um engano bem elaborado, em forma de narrativa, é, em si, uma habilidade.

A fabricação discursiva da crise é recurso explorado por acadêmicos (Danblon, 2017) e se aplica para a análise de políticas públicas, especialmente aquelas da área de segurança pública. Essa narrativa serve como base à ideia de crise permanente, de caráter processual-investigativo, e que se inclina ao futuro, no rompimento social iminente, simbolizado pela impunidade e liberdade que abre caminho para a barbárie (entre abusadores de menores, terroristas e traficantes de drogas). A criptografia romperia,

[43] Aqui, Rod Rosenstein se refere à criptografia por padrão empregada pela Apple nos iPhones. O discurso vem no bojo da disputa entre Apple e FBI em 2015, considerada a "nova rodada" das *Cryptowars* após a disputa do *Clipper Chip.*

supostamente, com as possibilidades de segurança pública diante de uma ameaça. A sustentação de uma "crise", portanto, terá o poder de catalisar o debate.

Dessa forma, haveria uma performatividade para ressignificar a tecnologia: além de refazer o paradigma da criptografia ao associá-la com um gatilho de crise social, insere-se novas metáforas para requalificar o debate e a cognição do público. No seminal trabalho de Lakoff e Johnson (1980), há uma minuciosa análise sobre como metáforas imprimem significados que vão além da estética ou do poder descritivo, mas têm o poder de dar forma à realidade. Sua aceitação, como resultado, dão base a inferências como criar inimigos hostis, gerar energia para reestruturações políticas ou mesmo convencer a população a aceitar certos sacrifícios.

Sob essa perspectiva, chama atenção a tentativa de emplacar novos rótulos à “encriptação forte” ou à “encriptação por padrão”. No trecho acima, Rosenstein (2017) “re-enquadra” os termos tecnicamente empregados no campo da computação para servir a uma sensibilização do público: “encriptação à prova de mandados”. Da mesma forma, Rosenstein (2017) se refere à encriptação que *permite* acesso às autoridades, mediante um *backdoor,* como “encriptação responsável”, sugerindo que outras formas seriam “irresponsáveis” e assim introduzindo um elemento de “moralidade cívica” à aplicação criptográfica. Ao substituir a robustez da criptografia pela irresponsabilidade, é animada uma disputa moral cuja responsabilidade recai sobre as plataformas, aos defensores da privacidade ou, em última análise, aos criptógrafos. No que seria possível responder: responsável para quem? (Pfefferkorn, 2017)

5.2.2 **Muda-se o inimigo, mantém-se o dilema**

Desde a década de noventa, longa batalha foi travada a respeito da regulação da Internet, encarada ora como “terra sem lei” ora como “utopia libertária” (Evangelista, 2018), levando a perspectivas largamente otimistas à cultura que poderia ser destravada daí (Levy, 2010). A maior ou menor presença do Estado, legislando sobre a rede

inclusive através da criação de mecanismos de monitoramento dos usuários e da criação de tipos penais, foi encarada com suspeição por parte de ciberativistas e da sociedade civil organizada, levando, por exemplo, à publicação da "Declaração de Independência do Ciberespaço", do icônico ativista John Perry Barlow (1996).

A criptografia esteve, em vários momentos, como um dos pontos de partida para uma "visão penal" sobre a Internet[44], uma vez que democratizaria as possibilidades de se alcançar o sigilo de dados e comunicações mesmo a civis. Resgatando desde a década de noventa, incluindo o capítulo *Clipper Chip,* diversos "adversários" foram eleitos na construção de argumentos que justificariam a criação de tipos penais, que autorizaram um maior aparato de vigilância estatal e, por fim, a criação de *backdoors* em sistemas criptográficos.

Padrões foram sendo tecidos nesse conjunto de narrativas: sempre estariam presentes o combate ao tráfico de drogas, às redes de pedofilia, sequestradores, terroristas, à pirataria, à lavagem de dinheiro, pornografia, aos exploradores sexuais ou, mais atualmente, à desinformação. As figuras, que encabeçariam a retórica por mais punitividade e vigilância na rede, seriam chamadas de "Cavaleiros do Infocalypse" por Timothy May (1994). "Qual particular cavaleiro está em voga depende do momento e das circunstâncias" (Schneier, 2019).

Caberia, portanto, explorar e contextualizar algumas das principais figuras presente e historicamente convocadas nas propostas de *backdoor* ou de outras "soluções" que orbitam as tentativas de burlar o sigilo criptográfico.

[44] Curioso notar que as primeiras tentativas de regular a Internet, com frequência, partiam da perspectiva penal, a *ultima ratio,* ao invés de se estabelecer um "marco zero civilista". A construção do Marco Civil da Internet é uma resposta a essa crítica, inclusive dado a rota penalista que estavam tomando as iniciativas legislativas brasileiras ao fim da primeira década do século vinte (Lemos; Souza; 2007)

5.2.2.1 ***Encriptação sob a sombra do terrorismo***

Ainda em 1991, o atual presidente dos Estados Unidos, à época Senador, Joe Biden, acrescentou uma passagem, a pedido explícito e com o auxílio do FBI, no então projeto de lei anti-terrorismo norte-americano:

> It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plaintext contents of voice, data, and other communications when appropriately authorized by law. (Kehl; Wilson; Bankston, 2015)

À época, a Internet ainda estava nos primórdios da escalada rumo à ubiquidade, mas a resistência governamental à flexibilização da regulação sobre a exportação e uso da criptografia encontrava variados e dinâmicos dispositivos legais para sustar o acesso a aplicações de criptografia. A inserção da previsão de "acesso excepcional" ao puro texto vai aparecer, portanto, antes mesmo do "*Clipper",* sem que houvesse um gancho explicativo do por quê da necessidade da medida para o combate ao terrorismo ou mesmo a oitiva de organizações interessadas (Kehl; Wilson; Bankston, 2015). O ocorrido, a propósito, será um dos fatores "aceleradores" da distribuição do PGP por Phil Zimmerman. (Levy, 2002)

A partir do *Clipper*, propriamente, mantém-se acesa, de forma mais sistemática, a pauta da segurança nacional a partir da suposição de uma ameaça terrorista, figurando em notas oficiais da Casa Branca à imprensa entre 1993 e 1994. As declarações, não raro, vêm desacompanhadas de indícios que sugerem o envolvimento direto de organizações terroristas e meios de comunicação encriptados. Pelo contrário, a ameaça terrorista é incluída entre os riscos de forma genérica:

> *While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals*
>
> *(...)*
>
> *The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists* (White House, 1993)
>
> *if encryption technology is made freely available worldwide, it would no doubt be used extensively by terrorists* (White House, 1994)

No irromper da mobilização da campanha em torno do "*Going Dark"* - a retórica do obscurecimento das investigações, capitaneada inicialmente pelo FBI e posteriormente mobilizada em pela alta cúpula do Departamento de Justiça - o terrorismo também se encontra no eixo central. Ainda em 2014, James Comey, então diretor do FBI, interliga diretamente a suposta perda das capacidades investigativas com a ameaça terrorista:

> With Going Dark, those of us in law enforcement and public safety have a major fear of missing out (...) missing out on a terrorist cell using social media to recruit, plan, and execute an attack. Criminals and terrorists would like nothing more than for us to miss out. (James Comey, 2014)

O enquadramento da encriptação sob as lentes do "obscurecimento", mais precisamente do terrorismo, irá ser predominante a partir da disputa processual entre FBI e Apple, em 2015. Diferentemente da década de noventa, esse período se alicerça precisamente em um atentado terrorista, o de San Bernardino, para provocar o efeito político que correlaciona uma suposta "privacidade irrazoável" e o premente risco de novos atentados. Entre 2015 e 2017, em quatro dos principais discursos de James Comey que endereçam essa suposta correlação, somam-se 49 menções à criptografia e 54 ao terrorismo (James Comey, 2015; 2016a; 2016b; 2017), números que revelam em um

evidente esforço estruturado e institucional, por parte do FBI, para fortalecer uma chave de significado que associa o sigilo criptográfico ao terror.

As narrativas de representações das forças de investigação e inteligência nacionais sugerem trilhar o mesmo caminho, mesmo com a tímida presença de ameaças terroristas no Brasil se comparadas com o cenário internacional. Em artigo publicado por oficiais da Agência Brasileira de Inteligência (ABIn), em análise da Operação Hashtag (A; O; S, 2017) - investigação de desmonte de suposta célula terrorista durante os Jogos Olímpicos de 2016, no Rio de Janeiro - o processo de radicalização de facções terroristas no Brasil atravessaria o abandono de grupos de discussão em redes sociais e, paralelamente, a adoção de aplicações de mensageria criptografadas. Quanto mais radicais eram os indivíduos, mais rapidamente abandonavam grupos de discussão em redes sociais e partiam em direção a "aplicativos móveis criptografados". (A; O; S, 2017)

Por fim, do ponto de vista de articulações geopolíticas plurinacionais, também é possível identificar esforços conjuntos, "coalizões anti-encriptação", simbolizadas, na maior parte das vezes, pelo que se convencionou referir como "Five Eyes", articulação dos Estados Unidos, Canadá, Reino Unidos, Austrália e Nova Zelândia. Segundo nota publicada em 2020, em conjunto com os governos do Japão e Índia (Patel et al, 2020)[45], uma suposta encriptação "à prova de mandados" seria utilizada sobretudo por terroristas e minaria a habilidade da polícia de proteger as vítimas. Além disso, nota publicada pelo do G7, de 2019, dedica-se especialmente a gerar esforços para se alcançar o "acesso legal" a conteúdos encriptados, tendo como pano de fundo o combate ao terrorismo (G7, 2019). Por fim, no plano doméstico, em associação com cooperações investigativas internacionais, o Brasil realizou em 2019 o I Simpósio Going Dark Brasil[46], resultando na declaração de concordância do país ao "*Statement of Principles on Access to Evidence and Encryption"* e na "Declaração Going Dark Brasil", co-assinada pelo então Ministro

[45] Diversas outras notas foram publicadas no âmbito dos Five Eyes ao longo dos últimos anos, mantendo ativa uma coalizão de países que irão explorar as propostas de enfraquecimento da encriptação a partir de uma abordagem geopolítica (Estados Unidos, 2017; Austrália, 2018).

[46] Seria possível inferir que a própria escolha do nome para o evento leva a compreensão de que um discurso "ready-made" é instrumentalizado para inserir o país em uma articulação internacional encabeçada, em ampla medida, pelos Estados Unidos historicamente

da Justiça, Sérgio Moro, e pelo *Associate Deputy Attorney General* dos Estados Unidos, Sujit Raman, tendo o combate ao terrorismo uma de seus pretextos (Brasil, 2019b).

Não é incomum, no entanto, que as propostas de flexibilização à criptografia venham desacompanhadas de dados que justifiquem que a criptografia seja recurso sem o qual atividades terroristas seriam efetivamente coibidas. Se falta às investidas das agências de investigação a publicação de dados que corroborem que a encriptação seria o principal fator que distancia a resolução de atentados e a captura de terroristas, há indícios de que o enfraquecimento da encriptação estaria longe de solucionar a questão, sendo, pelo contrário, uma medida inócua do ponto de vista da prevenção e investigação criminal.

Do ponto de vista cultural sobre o uso de tecnologias, documentos disponíveis sobre notáveis atentados apontam, inicialmente, para uma desconfiança de terroristas em relação à criptografia e serviços de tecnologia e comunicação ocidentais, segundo estudo do Center for Strategic and International Studies (Louis; Zheng; Carter, 2017). Apostariam, pelo contrário, em outras formas de escapar da vigilância, como mais notavelmente no episódio dos atentados em Paris, por exemplo, em que aparelhos celular descartáveis foram mais utilizados (Moody, 2016). A publicação aponta, também, que nenhum indício permite concluir que a criptografia tenha cumprindo um papel determinístico em atentados de grande relevo internacional, como em Mumbai, Londres, Boston, San Bernardino, Paris e Bruxelas ou mesmo em tentativas ocorridas em Nova York ou Koln. Antes disso, os atentados apostariam mais no elemento de "surpresa e confusão" para atingir seus objetivos (Louis; Zheng; Carter, 2017).

Corroborando com o argumento da evasão às tecnologias associadas ao ocidente e repercutindo diretamente na estratégia organizacional de facções terroristas, documentações vêm concluindo que grupos como a Al Qaeda, por exemplo, utilizam ferramentas de criptografia de fabricação própria (Site Intelligence Group, 2013), ainda que, muitas vezes, menos seguras e baratas do que aplicações fabricadas e disponíveis livremente (Schneier, 2008). Logo, do ponto de vista do levantamento de dados

disponíveis sobre a centralidade de tecnologias com criptografia, especialmente aquelas associados com a indústria e a sociedade ocidental, como o WhatsApp em termos de aplicações, ou o iPhone para falar em dispositivos e criptografia sobre discos rígidos, a sustentação da narrativa governamental aparenta se deter aos discursos.

5.2.2.2 ***Diante das redes de exploração infantil***

A associação da criptografia com atividades criminais também passa, comumente, pelo sigilo que a tecnologia confere a comunicações de redes de pedofilia, questão delicada e que repercute através de diversas entidades cujo trabalho se baseia na dedicação ao combate à exploração de crianças.

Estima-se que um terço de todos os usuários da Internet é composta por menores de 18 anos. Ao mesmo tempo, da mesma forma que a rede multiplicou as potencialidades de acesso à informação e comunicação, também possibilitou novos níveis de disseminação de material relacionado à pedofilia. Atualmente, por exemplo, há serviços customizados de acesso a conteúdo de abuso sexual infantil, de acordo com raça, gênero e idade, ou mesmo exibição em *streaming* de violações em tempo real segundo a United Nations Office on Drugs and Crime (United Nations, 2015).

A interpretação de algumas entidades de defesa à criança e combate à exploração infantil, como é o caso da estadunidense National Center for Missing and Exploited Children (NCMEC), vem associando, diretamente, a expansão dos casos de compartilhamento de imagens sexuais infantis com a implementação de criptografia em aplicações. Em campanha em favor da filtragem de conteúdos abusivos em plataformas de comunicação, é ressaltado o *slogan*: “encriptação ponta-a-ponta: ignorar abusos não irá cessá-los”. Além disso, a entidade atesta que “a encriptação ponta-a-ponta irá fechar as cortinas online, tornando plataformas criptografadas ambientes sem lei, onde a falta de

visibilidade e fiscalização sobre atividades criminais irá empoderar abusadores" (National Center for Missing and Exploited Children, 2019).[47]

Em território europeu, no Seminário "*Preventing and combating child sexual abuse & exploitation: towards an EU response*", a Comissária Ylva Johansson pediu por uma solução técnica ao que ela descreveu como o "problema da criptografia" (O'Brian, 2020). Ainda em 2020, foi vazado documento, produzido no âmbito da Comissão Europeia, no qual eram endereçadas possíveis soluções no campo do combate à violência infantil online, entre elas, medidas que ensejassem a superação do sigilo oferecido por plataformas e lograssem a filtragem de conteúdos relacionados ao abuso infantil (Europena Commission, 2020).

Da mesma forma as narrativas de combate ao terrorismo, o combate à exploração infantil também é trazido à baila na esteira da campanha mobilizada por setores de investigação. No evento *Lawful Access Summit*, todo dedicado às formas de desviar da criptografia, o atual diretor do FBI, Christopher Wray (2019), traz em seu discurso delicadas descrições de casos de pedofilia para, em suma, demandar por soluções criativas, genericamente, por parte das empresas de tecnologia. Em outra oportunidade, alega que, diante da possibilidade do Facebook agregar criptografia ponta-a-ponta em seu aplicativo de mensagens, a plataforma se tornaria um "sonho que se torna realidade" para pedófilos (Shortell, 2019).

No entanto, além dos imperativos tecnológicos que alertam para um risco monumental para todo o ecossistema no caso de exceções ao sigilo criptográfico, mais à frente explorados, um dissenso é criado a partir do momento em que são expostas as preocupações de organismos multilaterais quanto à exposição de crianças e adolescentes na Internet devido à crescente presença do público em espaços de interação online, situação que repercutiria em dimensões como segurança, proteção de dados, privacidade e liberdade de expressão.

[47] Traduções minhas.

A UNICEF vem abordando as relações entre plataformas digitais, direitos fundamentais e a proteção da criança e do adolescente em variadas publicações, pronunciamentos e relatórios, como o *Children's Online Privacy and Freedom of Expression*, onde expõe que o debate político sobre o uso da Internet e a infância tem girado largamente em torno da proteção contra a violência e exploração. Ainda que esse foco seja essencial,

> *yet may also risk overlooking how children exercise their full range of rights online, including their rights to privacy and freedom of expression. Against this backdrop, it is important to consider how children's rights to privacy and freedom of expression – as recognized in the United Nations Convention on the Rights of the Child (CRC) – are realized in a digital world.* (Unicef, 2018)

Nesse ínterim, a Convenção sobre os Direitos das Crianças, das Nações Unidas, estabelece que crianças possuem liberdade para se expressar livremente, tanto na procura, na recepção quanto na divulgação de informações e ideias de todos os tipos, bem como o direito do acesso das crianças a informações e materiais procedentes de diversas fontes, sejam elas nacionais e internacionais, uma vez que é uma forma de promoção de seu bem-estar e saúde física e mental. Dados da "TIC Kids Brasil 2019" apontam que, no Brasil, cerca de 48% das crianças entre 9 e 17 anos usam a Internet mais de uma vez por dia considerando as classes A, B, C, D e E, e 42% do público entre 9 e 10 anos afirma que os pais permitem que, sem supervisão, elas possam enviar mensagens instantâneas (Comitê Gestor da Internet no Brasil, 2019).[48]

Dada a amplitude de comunicações e dados pessoais do público jovem que trafega em plataformas, o documento da Unicef (2018), supracitado, alerta que medidas de segurança de dados do ponto de vista técnico e organizacional devem estar presentes, sob risco de vazamento de dados, interceptação dessas informações e fraudes. É, igualmente, categórico em alertar que todos os dispositivos onde trafegam dados pessoais de crianças

[48] Uma coleção de dados sobre o uso da Internet pelas crianças e suas correlações com a segurança da informação e a criptografia pode ser encontrado em Inês (2021)

devem ser equipados com o estado da arte em termos de hardware e software que assegurem proteção suficiente, além da necessidade de sua constante atualização.

A essa altura, seria oportuno assinalar que as soluções propostas pelo FBI ou NCMEC, em certa medida, caracterizam o exato oposto às recomendações da UNICEF: ao pleitearem brechas à criptografia, ainda que para acesso excepcional, geram uma demanda pelo regresso ou criação de vulnerabilidades em termos de segurança da informação. Da mesma forma, criam brechas que deslocam a questão sobre *se* atores maliciosos irão explorar essas fraquezas para *quando* irão explorar.

Para concluir, na publicação *Encryption, Privacy, and Children's Right to Protection from Harm,* grupo de trabalho da UNICEF assinala que o debate em torno da criptografia envolve uma discussão tecnológica complexa. Reconhece que soluções de "acesso excepcional", como *backdoors*, podem estar vulneráveis a acessos não autorizados, bem como dão margem a abusos por parte do próprio Estado, o que acarretaria mais fragilidades para o público jovem e para a sociedade em geral (Unicef, 2020).

5.2.2.3 ***A encriptação na encruzilhada da polarização política: a desinformação***

Enquanto o abuso sexual infantil e o terrorismo são conhecidos fenômenos aparelhados ao debate em torno da criptografia em um recorte histórico mais amplo, outras conjunturas mais atuais, associadas a uma agenda de combate ao crime inclusive mais polarizada politicamente, vão servir de atualização narrativa para os agentes de investigação. É o caso da desinformação, que irá assumir facetas muito similares, apesar de ocorrerem em territórios cultural e legalmente distintos, e do combate à corrupção, elemento polarizante de facções políticas, caro inclusive à disputa eleitoral no Brasil. Resgatando a expressão anteriormente utilizada por críticos às brechas à criptografia, pode-se dizer que a desinformação e a corrupção seriam companheiros que se somam, atualmente, aos primeiros "Cavaleiros do Infocalypse" (ou mesmo sua nova geração) e

expandem a margem argumentativa em políticas públicas que afetam o pleno funcionamento da criptografia.

No contexto do combate à desinformação, é amplamente documentado o papel central que aplicativos de mensageria, como o WhatsApp e o Telegram, desempenham (Spagnuolo, 2021; Marés, Becker, 2018), sobretudo no Brasil. Ato contínuo, a criptografia será novamente posta no centro do tabuleiro, uma vez que garante o sigilo das comunicações e dificulta, quando compartilhadas/encaminhadas informações, o mapeamento regressivo em direção ao autor original da mensagem. O problema dialoga com o desafio basilar do combate à desinformação: seria possível creditar a alguém em específico, em uma rede infinita de replicações em múltiplas plataformas, a gênese da manufatura e publicação primeira de um conteúdo desinformativo?

De toda forma, a fricção entre desinformação e criptografia são emblemáticos, pelo menos em dois países: no Brasil e na Índia. Nesse último, a sensibilização teve início com uma série de linchamentos, que levaram à morte cerca de trinta indivíduos, ocasionados por conteúdos editados e distorcidos sobre uma suposta onda de sequestro de crianças. Os materiais eram compartilhados pelo WhatsApp. Diante do fracasso em capturar os responsáveis, o governo indiano passou a culpar a criptografia ponta-a-ponta da plataforma. Dado esse cenário e considerando a então proximidade das eleições de 2019, ainda em 2018 o governo indiano propôs mudanças às regras de responsabilidade de intermediários no país (conjunto de regras que delimitam em que casos uma rede social, por exemplo, seria responsável por conteúdos produzidos por terceiros, usuários), para obrigar a plataforma a inserir mecanismos de “rastreabilidade das mensagens” e, assim, coibir a desinformação (Mohanty, 2019).

Mais recentemente, em 2021, as propostas de monitorar e aumentar o poder de polícia através das plataformas, sob o ponto de partida do combate à desinformação, voltaram a ganhar fôlego em uma nova versão (Índia, 2021) das regras apresentada pelo Ministro de Tecnologia da Informação do país, baseadas em rastreamento de mensagens e retirada automática de conteúdos considerados ilegais. Além do background indiano, com

frequência relacionado a recentes repressões e retiradas de conteúdos críticos ao governo (Singh, 2021), além de bloquear o acesso à Internet para minar o alcance da liberdade de expressão de informação no contexto de protestos, analistas argumentam que as novas regras minam a segurança de usuários no país ao demandarem que o servidor intermediário tenha algum conhecimento sobre o conteúdo das mensagens, algo incompatível com a criptografia ponta-a-ponta.

Em grande medida, a proposta se assemelha com a linha interpretativa de parte dos esforços, em termos de políticas públicas, para coibir a desinformação no Brasil. Ainda em 2018, análise da Agência Lupa propunha que a criptografia ponta-a-ponta seria responsável pela "capacidade de viralização" de conteúdos desinformativos. Na mesma época, pesquisador associado ao Centro de Responsabilidade para Mídias Sociais, do MIT, também responsabilizava a criptografia por não permitir um dimensionamento real da desinformação (Ribeiro 2019).

Cerca de dois anos depois, a agenda dos direitos digitais no Brasil é pautada pelo Projeto de Lei de Liberdade, Responsabilidade e Transparência na Internet (PL nº 2630/2020), destinado a legislar sobre regras de combate à desinformação e gerar diretrizes de transparência à moderação de conteúdo por provedores de aplicação. Um de seus mecanismos de combate à desinformação tange precisamente o artifício indiano: implementar recursos, mesmo em plataformas criptografadas, para permitir a rastreabilidade dos compartilhamentos de mensagens. Além das mesmas considerações e críticas provenientes do contexto indiano, que dizem respeito a um "andar para trás" em termos de segurança da informação, organizações e analistas nacionais (Instituto de Pesquisa em Direito e Tecnologia do Recife; Coding Rights, 2020) e internacionais (InternetLab, 2020) comentam que a regressão ao mensageiro inicial não garante que se chegará ao verdadeiro responsável (o conteúdo poder ter migrado de outra plataforma), além de que, ao propor a identificação de encaminhamentos de mensagens, a medida atentaria frontalmente com as garantias aos direitos fundamentais derivados do uso

íntegro da criptografia ponta-a-ponta ao propor um rastreamento ainda que de metadados. [49]

5.3 A matemática volta às trincheiras: a comunidade acadêmico-científica no tabuleiro tecnopolítco

> *The problem with notions of a "middle ground" is that cryptography is mathematics and law enforcement is policy. The laws of mathematics are not something that can be compromised, they just are*. (Schneier, 2018)

O cânone básico da criptografia - de como, efetivamente, manter uma "comunicação privada e segura na comunicação de um adversário" - não esgota (ou não traduz) suficientemente os desafios políticos implicados em um eventual "tropeço" em se alcançar esse objetivo. A figura do adversário, da mesma forma, se ramifica entre tantos quanto possíveis, desde organizações criminosas, *brokers* de dados pessoais e agentes estatais. Associando o cânone do desafio criptográfico, por exemplo, ao "adversário estatal", é possível assumir que a vigilância em massa representa um fracasso espetacular em se alcançar a segurança nas comunicações proposta pela criptografia (Rogaway, 2014). Ato contínuo, se o sigilo das comunicações também é positivado enquanto direito fundamental, na medida em que é instrumental à eficácia de outros direitos (como a liberdade de expressão, reunião, associação e manifestação), aparatos de vigilância em massa são a antítese do Estado Democrático de Direito.

[49] Não é raro ver compreensões segundo as quais o sigilo conferido constitucional e infraconstitucionalmente às comunicações não se estenderia às garantias também aos metadados. São leituras bastante afeitas às correntes que se inclinam ao monitoramento de usuários e deixam a desejar em termos de acobertar, com a devida aplicação das leis que regulamentam a proteção de dados pessoais e a excepcionalidade da suspensão do sigilo, também os metadados (dados igualmente pessoais na medida em que potencialmente identificam seu titular). No contexto do "PL das Fake News", ver Data Privacy Brasil (2020).

5.3.1 **O estopim dos anos noventa**

No campo da comunidade técnico-científica, ainda na década de noventa, a contraposição a propostas de políticas públicas pautadas em formas de "*key recovery*", "*key escrow"* ou "*trusted third-parties"* foram o gatilho inicial para que fosse articulada a mobilização do setor em torno de uma argumentação que buscava uma advocacia pela segurança da informação progressiva do ponto de vista do computacional. A contribuição da comunidade ao debate da época pode ser simbolizada pela publicação do *The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption* (Abelson et al, 1997), que reuniu a opinião de especialistas de referência em criptografia e segurança computacional, incluindo um dos criadores da criptografia de "chave pública", Whitfield Diffie.

Três pontos serão centrais na publicação e serão a gênese de contrapontos a políticas futuras: os pré-requisitos necessários a um programa de "custódia" ou "depósito de chaves" seriam excessivamente custosos e potencialmente um sacrifício considerável para muitas aplicações e usuários finais; os sistemas eventualmente desenvolvidos seriam demasiadamente complexos e estariam além da experiência e competência da área; e essa infraestrutura iria requerer extraordinários níveis de confiança, em um cenário em que indivíduos ou grupos de indivíduos, por ideologia, ganância, ou chantageados poderiam abusar da autoridade lhes conferida (Abelson et al, 1997).

Enquanto no "*The risks of key recovery"* houve uma explícita escolha por não abordar os direitos e liberdades em questão - ainda que reconheçam as camadas sociais e políticas envolvidas em propostas de acesso excepcional - professores associados a faculdades de direito norte-americanas agregaram uma abordagem sócio-jurídica à discussão. Em carta aberta ao congresso norte-americano por ocasião de uma emenda elaborada pelo FBI ao *Security and Freedom through Encryption Act* (SAFE) - decreto originalmente editado para flexibilizar as então rígidas regras de exportação de produtos com criptografia - juristas, entre eles o professor Lawrence Lessig, problematizavam o

sistema de custódia de chaves e declararam que o direito de se expressar livremente inclui não apenas falar *o que* se quer, mas também *como* se quer falar (Aoki et al, 1997).

Um dado ordenamento jurídico, portanto, não deveria regular através de qual técnica - ou software - deve ocorrer uma comunicação ou influenciar como desenvolvedores deveriam escrever códigos, uma vez que a programação também é uma linguagem que, fundamentalmente, faz parte das formas de se comunicar e se expressar. Exigências dessa natureza extrapolariam, então, os poderes delegados ao governo na Constituição e invadiriam liberdades civis. Na carta, os professores expressam que

> *Never in peacetime has our government attempted so completely to monopolize a single form of communication; never has it required, in effect, a license to exercise the right to speak. (...) By imposing requirements on cryptographic programs used by individuals and corporations to protect the privacy and security of their papers and telephone or e-mail conversations, it would in effect be mandating the code software writers may write (...) This forced speech, we believe, takes the government's power too far* (Aoki et al, 1997).

Episódio emblemático, em 1995, foi a decisão no âmbito do caso *Bernstein vs. Department of Justice*, a organização Electronic Frontier Foundation representou um estudante de matemática da Universidade da Califórnia, em Berkeley, que desejava publicar o código-fonte de seu recém-desenvolvido sistema de criptografia (Electronic Frontier Foundation, 2001). A Nona Corte de Apelações decidiu que o código-fonte de um software estaria acobertado pela Primeira Emenda (relativa à liberdade de expressão) e que a interferência governamental sobre sua publicação seria inconstitucional. [50]

[50] No que se refere à criptografia, à época dos bloqueios ao WhatsApp no Brasil, Danilo Doneda chama atenção para o fato de que “qualquer proibição equivaleria também a impedir a utilização da própria matemática, algo que não chega a ser inédito — em 1976, em plena ditadura argentina, o governador da província de Córdoba proibiu o ensino da Teoria dos Conjuntos por considerá-la "abertamente subversiva", pois que "evidentemente tende a massificar e provocar as multidões". A proibição não teve efeito.” (Doneda, 2017)

5.3.2 **Vinte anos depois, as chaves debaixo do tapete**

Cerca de vinte anos depois, em uma atualização contextual do trabalho por ocasião da disputa judicial entre a Apple e o FBI entre 2015 e 2016 e, consequentemente, da campanha *going dark* estabelecida pelo FBI, o mesmo time de autores, com a adição de outros nomes de especialistas em políticas de segurança da informação, como dos professores Susan Landau e Matthew Green, publicaram o seminal *Keys Under Doormats - Mandating Insecurity by Requiring Government Access to All Data and Communications* (Abelson et al, 2015).[51] O artigo pode ser, atualmente, considerado a "pedra angular" quando se tratando dos riscos e inseguranças infraestruturais e político-administrativas resultantes do advento de um eventual método de acesso excepcional ao conteúdo encriptado por parte do Estado, e responde, em linhas gerais, à seguinte pergunta: seria possível tal acesso excepcional sem que fosse criado um risco inaceitável?[52]

No referido estudo, é consolidado o entendimento de que não haveria garantias de que uma brecha inserida nos mecanismos de encriptação restaria, efetivamente, em mãos unicamente de um terceiro de confiança, seja o Estado ou uma entidade privada. Seria crescente o risco potencial de exploração dessas permissões por particulares maliciosos ou mesmo outras nações.

---

[51] O artigo ganhou uma tradução em território brasileiro organizada pelo Instituto de Internet e Sociedade (ITS) do Rio de Janeiro.

[52] A pergunta parece tocar em um ponto nevrálgico do debate: não estariam as agências de investigação e formuladores de políticas dimensionando suficientemente os riscos envolvidos nas propostas de acesso excepcional? Ou estariam e, mesmo assim, estariam dispostos a arcar com o sacrifício? O encaminhamento do debate parece depender dessas respostas para ser endereçado a partir de um denominador comum. Em 2020, tive a oportunidade de entrevistar Riana Pfefferkorn, então Diretora Associada do Center for Internet and Society da Universidade de Stanford. Diante dessa possível "bifurcação", diz que *"embora a falta de conhecimento técnico seja certamente um problema, não é a única explicação para por que os legisladores e membros da polícia continuam a fazer propostas de políticas para enfraquecer a criptografia. Para aqueles que entendem as razões técnicas para não enfraquecer a criptografia, mas de toda forma fazem essas propostas, acredito que há várias motivações. Uma significa que eles compreendem os riscos de enfraquecer a criptografia, mas acreditam que, na balança, isso compensa. Eles sabem que enfraquecer a criptografia põe os dados de todo mundo em risco e que um "backdoor para os bons mocinhos" também será descoberto e explorado pelos "vilões". Mesmo assim, quando pesam esses danos colaterais em contraposição com os benefícios esperados diante do enfraquecimento da criptografia, em termos de detectar e investigar atividades criminais e coletar evidências, eles decidem que estão de acordo com essa troca."* (Instituto de Pesquisa em Direito e Tecnologia do Recife, 2020)

Em segundo lugar, proporcional à complexidade de viabilizar mecanismos de custódia de chaves é a dificuldade de administrar as relações entre serviços, aplicações e autoridades investigativas ou policiais, o que acarretaria enormes custos operacionais e tecnológicos na administração do acesso. A cada novo recurso integrante de um sistema de criptografia há uma nova rede de interações com os recursos básicos pré-existentes, criando novas camadas de vulnerabilidades inesperadas: "a complexidade é inimiga da segurança", concordam.

Logo, é conclusivo em dizer que, antes de qualquer avanço em termos policiais-investigativos, mecanismos de acesso excepcional criariam vulnerabilidades estruturais à própria segurança pública da coletividade, a qual agências de investigação, justamente, alegam querer proteger. Enfim, essa racionalidade permite estampar um caráter "agnóstico" ao *backdoor*: não há como estabelecer um controle de restrição utópica sobre sua instrumentalização.[53] Da mesma forma, a qualidade agnóstica também se estende à própria encriptação: protege as informações de ativistas, advogados, instituições financeiras e políticos da mesma forma que protege exploradores sexuais e terroristas (Gill, 2018). Não é uma situação tão diferente de ferramentas mais elementares: o transporte público também é utilizado de forma agnóstica, tanto por criminosos quanto por crianças e adolescentes. Qualquer regulação que pretenda controlar o acesso, portanto, estaria fadada ao fracasso.

5.3.3 **"Criptógrafos do mundo todo: uni-vos!"**

No subcategoria do desenvolvimento técnico-científico, o campo do trabalho criptográfico *per se* assume crucial papel no tabuleiro das políticas de encriptação. A

[53] Vladimir Aras, Procurador da República, alega que "quando nós estamos diante de uma alegação de que não há meios para conferir acesso ao Estado a esses dados, essa é uma afirmação bastante curiosa, porque esses instrumentos foram criados por homens. E, se que foram criados por homens, podem ser desenhados de forma diferente" (Supremo Tribunal Federal, 2017) Como sugere Cory Doctorow (2018) seria uma espécie de "segurança baseada na fé".

integridade ou excepcionalidade, a segurança progressiva ou concessão política, a criptanálise como auditoria descentralizada ou como método de exploração de vulnerabilidade: há uma ética científica que resgata uma discussão herdeira do pós-guerra e que se estende às disputas contemporâneas em torno da criptografia.

A contribuição de Phillip Rogaway (2015) ao debate faz um resgate histórico do quão estaria sedimentada uma noção de responsabilidade social da comunidade de cientistas e engenheiros para, enfim, desaguar no trabalho criptográfico. Busca um ponto de partida no Manifesto Russell-Einstein[54] - documento que galvanizou uma articulação de caráter humanista frente às ameaças postas pelo desenvolvimento de armas nucleares - para apontar duas questões: que o trabalho técnico, por si só, pode implicar escolhas políticas; e que alguns cientistas, em resposta, assumem papéis abertamente políticos, como o caso de Bertrand Russell.[55] No entanto, o fato de haver representações científicas abertamente políticas não quer dizer que outras categorias não estejam sujeitas a uma responsabilidade social que acompanha o desenvolvimento técnico. Não seria, tampouco, necessário falar em armas nucleares para chamar atenção para essa relação na medida em que os cruzamentos entre técnica, política e sociedade são rotineiramente explorados e ressaltados pela comunidade acadêmica[56] e encontra reflexos no "mundo prático". O trabalho criptográfico, portanto, se encontraria precisamente no meio dessa encruzilhada relativa a uma "ontologia da técnica":

> *Technological advances are usefully considered not only from the lens of how they work, but also why they came to be as they did, whom they help, and whom they harm. Emphasizing the breadth of man's agency and technological options, and borrowing a beautiful phrase of Borges,*

[54] O propósito do manifesto vem no bojo do movimento desarmamentista e humanista do pós-guerra. "*Shall we put an end to the human race; or shall mankind renounce war? (...) We appeal, as human beings, to human beings: Remember your humanity, and forget the rest. If you can do so, the way lies open to a new Paradise; if you cannot, there lies before you the risk of universal death."* (Born et al 1955) (trecho).

[55] Bertrand Russell foi o pivô da publicação do manifesto.

[56] Passando pelo trabalho de autores como Langdon Winner, Bernard Stigler, Bruno Latour, para citar só alguns dos diversos autores associados ao campo do que se convencionou chamar de *Science and Technology Studies* (STS).

> *it has been said that innovation is a garden of forking paths* (Rogaway, 2015). (grifos como no original)

O Manifesto Russell-Einstein citado por Rogaway encontra eco em reflexões em grande medida existencialistas de cientistas no pós-guerra. O "balanço ético" do físico Robert Oppenheimer - líder da equipe do Projeto Manhattan responsável por desenvolver as bombas atômicas lançadas sobre Hiroshima e Nagasaki em 1945 - é sintomático de uma revisão autocrítica derivada do desenvolvimento tecnológico que encontra uma "moralidade justificável" (Anderson, 2018) sob enquadramentos de "excepcionalidade" diante de "tempos de crise", mas que lançam a comunidade científica a uma "ressaca" revisionista sobre seu papel político e responsabilidade social: *"I remembered the line from the Hindu scripture, the Bhagavad-Gita. Vishnu is trying to persuade the Prince that he should do his duty and to impress him takes on his multi-armed form and says, 'Now, I am become Death, the destroyer of worlds."*. (Hart, 2007). Oppenheimer acreditava que tinha sangue em suas mãos em razão de seu papel na Segunda Guerra.

Um paralelo possível poderia ser traçado entre o programa técnico do Projeto Manhattan, que, diante do expansionismo nazista, teria sido norteado por uma permissividade que levaria à relativização ética e, portanto, ao emprego de armas nucleares de destruição em massa; e o robustecimento de arquiteturas de vigilância em massa diante do choque provocado pelos atentados de 11 de setembro de 2001. O *leitmotiv* de Edward Snowden para contribuir à montagem dessa arquitetura, despertando em si um estímulo patriótico, parece ser uma repaginação do estado de espírito do próprio Oppenheimer, que se dizia horrorizado com a queda da França em 1940 e acreditava que a bomba atômica, portanto, teria o potencial de acabar com a guerra (bem como prevenir futuras) e salvar a civilização ocidental (Hijyia, 2000). Ocorre que o patriotismo se converte, nesses casos, em nacionalismo autoritário e avança sobre liberdades individuais, tendo a tecnologia como meio propulsor.

> *Depois do 11 de Setembro, a CI [Comunidade Americana de Inteligência] sentiu uma culpa imensa por não ter protegido os EUA, por ter permitido que o ataque mais devastador e destrutivo ao país desde Pearl Harbor ocorresse debaixo de seu nariz. Em decorrência disso, seus líderes procuraram construir um sistema que impedisse que fossem pegos de surpresa de novo. Na base desse sistema estava a tecnologia, coisa alheia a seu exército de especialistas em ciências políticas e mestres em administração empresarial. As portas das agências de inteligência mais secretas foram abertas para jovens tecnólogos como eu.* (Snowden, 2019)

Não coincidentemente, as revelações de Edward Snowden são o ponto de partida para a contribuição de Phillip Rogaway, do ponto de vista científico, da comunidade de criptógrafos, às disputas em torno da criptografia. Essa contribuição chama por correlações (ainda que não faça menção a Oppenheimer) entre uma necessária revisão moral contemporânea, baseada no que a Internet vem se tornando, e àquela feita no pós-guerra.

> *Com algumas exceções, os cientistas atômicos que trabalharam no desarmamento não foram os mesmos indivíduos que construíram a bomba. Seus colegas - companheiros físicos - o fizeram. Criptógrafos não tornaram a Internet um instrumento de vigilância total, mas seus colegas - cientistas da computação e engenheiros - o fizeram. E criptógrafos têm a capacidade de ajudar.* (Rogaway, 2015).

Ainda que a criptografia não resolva, sozinha, as violações resultantes das multicamadas de vigilância que permeiam as interfaces entre humanos de dispositivos, uma chamada pública pela união da categoria de criptógrafos, em nome da segurança e da privacidade sem exceções, portanto, pode ser encontrada no trabalho de Rogaway. Em uma atualização contextual do Manifesto Russell-Einstein, há um alerta contra a negligência (ou ignorância deliberada) da responsabilidade social na esteira do desenvolvimento tecnológico. E se a criptografia, sozinha, não resolve todo o problema,

ao menos responderia à pergunta: “como podemos tornar a vigilância mais custosa?” (Rogaway, 2015)

5.4 *Cypherpunks, cryptorebels:* a criptografia como bandeira de direitos e liberdades

Como proposto ao longo desse trabalho, o uso de cifras para a encriptação de mensagens e comunicações guarda relação, histórica e politicamente, com a distribuição - ou detenção - de poder. Se, desde a antiguidade até meados da segunda metade do século 20, a criptografia parecia ser “monopólio” do Estado - reservada às altas cúpulas governamentais e às autoridades diplomáticas para fins de comunicações estratégicas e sensível - uma revolução nos meios de acesso às técnicas de criptografia deu origem a uma dupla reação: a oposição governamental, capitaneada pelos Estados Unidos, à abertura e publicização das técnicas de criptografia e, como consequência, um movimento de emancipação social baseado na privacidade ou, mais especificamente, no sigilo das comunicações simbolizado pela criptografia.

A década de setenta, precisamente a criação da criptografia de chave pública, foi paradigmática em termos de viabilidade técnica para que a criptografia se tornasse de mais fácil emprego para os setores de produção tecnológica. Até lá, “um silêncio ensurdecedor prevalecia sobre essa espetacular tecnologia” (Levy, 2002). A criptografia de chave pública, portanto, veio inicialmente a público por meio do trabalho “*New Directions in Cryptography”,* de Whitfield Diffie e Martin Hellman (1976). Propunham uma solução para o “problema da distribuição de chaves”[57] ao inaugurar o seguinte modelo: a chave de encriptação, para “fechar” a comunicação, poderia ser pública, conhecida. O receptor usaria uma chave privada, apenas por ele sabida, para decriptar a

[57] Até então, prevalecia o modelo “simétrico” de distribuição de chaves, uma chave privada haveria de ser utilizada tanto para encriptar uma mensagem quanto para decriptá-la. No entanto, como dois pontos da comunicação podem “combinar” uma chave privada se o canal de comunicação pode estar comprometido? O maior esforço, portanto, residia em tornar o canal de comunicação seguro para, inicialmente, combinar a chave privada para os dois pontos da comunicação, o que tornava a dinâmica dispendiosa. Logo, como combinar uma chave para encriptar uma mensagem *mesmo* que o canal esteja comprometido?

mensagem, “abrindo” a comunicação.[58] Dessa forma, os custos de manter seguro o canal de comunicação caem drasticamente, facilitando o acesso a técnicas de criptografia através do sistema de chave pública[59].

Como descrito ao longo desse trabalho, sucessivas investidas governamentais buscaram embargar a flexibilização das regras sobre uso e exportação de criptografia - e consequente disponibilização comercial e civil - passando por limitar a robustez, medida em tamanho das chaves, dos produtos de criptografia, ou propor políticas baseadas na existência de *backdoors* em serviços de encriptação de dados e comunicações. Como relatado, as tentativas de enrijecer o acesso à criptografia não vingaram após ampla disputa durante a década de noventa.

5.4.1 **Uma lista de e-mail na hora certa e no lugar certo**

A reação social que esteve na linha de frente da batalha ficou cristalizada na figura dos *cypherpunks*, propulsores do uso de técnicas de encriptação como ferramentas de efetivação dos direitos civis e geradores do que, aqui, convém chamar de *cipher-ativismo* - ou seja, a articulação de uma agenda política cujo centro gravitacional localizava-se na encriptação das comunicações e nas liberdades daí resultantes. Tem-se, então, o *cypherpunk* enquanto sujeito político,[60] unidade formativa de um movimento de articulação sócio e tecnopolítica representado pelo cipher-ativismo.

Credita-se ao trabalho *Security Without Identification: Transactions Systems to Make Big Brother Obsolete***,** de David Chaum (1985), o primeiro ensaio do que já foi chamado de "sonho criptográfico” (Narayanan, 2013) um ideal social que favorece a

---

[58] Uma metáfora comumente utilizada é da caixa de correio: é fácil depositar um envelope, mas só o legítimo dono da caixa tem a chave certa para abri-la. O modelo ficará conhecido como “distribuição de chaves Diffie-Hellman”.

[59] A criptografia de chave pública será fundada sobre o “problema da fatoração”: é simples encontrar o produto de dois números primos grandes, mas, dado o produto, é difícil chegar a seus fatores apenas por tentativa e erro (Schneier, 1996)

[60] O Oxford English Dictionary (2021) define o termo *cypherpunk* como “pessoa que usa a encriptação quando acessa uma rede computadores com o objetivo de assegurar sua privacidade, especialmente contra autoridades governamentais.”

autonomia individual - através da garantia do direito ao anonimato - em detrimento de um Estado total. A utopia vinha na esteira de recentes inovações no campo da criptografia que prometiam revolucionar a segurança e a privacidade sobre as comunicações, entre elas a criptografia de chave pública e os protocolos *Data Encryption Standard* e RSA. Chaum, especificamente, advogava pela ideia de que sistemas criptográficos poderiam distribuir os protocolos de autenticação sem, necessariamente, violar a privacidade, transformando radicalmente a sociedade. A ideologia, no entanto, correu para além do "*Secrets Without Identification"*, sendo desenvolvida por aqueles que se tornariam os expoentes da projeção da encriptação enquanto ferramenta de resistência política e transformação social.

Em 1988, Timothy May, engenheiro elétrico então associado à Intel, apresentava o desenvolvimento das ideias de Chaum em um rascunho intitulado *The Crypto Anarchist Manifesto* (1988), onde esticava a inclinação política de um suposto sistema distribuído de autenticação e proteção à privacidade e iniciava uma advocacia por uma visão *tecno-libertária* da criptografia. Lia-se que

> *Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. (...) The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. (...) The State will of course try to slow or halt the spread of this technology, citing national security concerns… (...) But this will not halt the spread of crypto anarchy.*

Com o objetivo expandir o público diante de um esforço de articulação social entre a comunidade tecnológica, entusiastas da criptografia e adeptos de multifacetadas utopias cibernéticas, May se associa, então, a Erich Hughes e John Gilmore pra lançar, em 1992, uma lista de e-mail para agregar, de forma exponencial, um maior público.[61]

[61] Greenberg, pág 77.

Herdando uma derivação morfológica e conceitual do movimento literário que melhor respondia às inquietações desse público à época, o *cyberpunk* (cujos expoentes são nomes como William Gibson, Bruce Sterling e Neal Stephenson)[62], a lista de e-mail é batizada de *Cypherpunk Mailing List.*[63]

O espírito que percorria criptógrafos, engenheiros, matemáticos, cientistas da computação e, mais tarde, advogados e defensores dos direitos humanos, é expresso em uma nova rodada comunicação vibrante aos seus interlocutores, simbolizada pelo *A Cypherpunk's Manifesto* (1993), de Erich Hughes:

> Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. (...) We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information.

Hughes relaciona, uma autonomia e autodeterminação informacional com o exercício do anonimato para falar de uma contemporânea dimensão da privacidade que toma como ponto de fricção a ideia de que sua governança, caso apenas tutelada por corporações e pelo próprio Estado, periga cair nas mãos de interesses econômicos e totalitários se não apropriada pelos próprios indivíduos, incluindo suas associações sociais e comunitárias. "*We must defend our own privacy if we expect to have any",* diz, para concluir que *"[c]ypherpunks deplore regulations on cryptography, for encryption is*

---

[62] Ver, por exemplo, Neuromancer (1984), Islands in the Net (1988) e Snow Crash (1992), respectivamente. O gênero irá se basear, a grosso modo, na criação de cenários distópicos, decadentes e hiperconectados, cujos protagonistas são personagens socioeconomicamente marginais e que antagonizam grandes corporações e monopólios tecnológicos em ambientes, muitas vezes, extremamente virtuais. Portanto, nada mais próximo do que a virtualização da experiência, à época, do que uma lista de e-mail.

[63] O jogo de palavras, aqui, é claro: ao invés de *cyber*, agrega-se *cypher*, simbolizando *cifra* criptográfica, e mantendo o espírito de crítica social do gênero literário

fundamentally a private act. The act of encryption, in fact, removes information from the public realm." Os "*cryptorebels",* como coloca Steven Levy (2002), iriam, de forma orgânica, se tornar consideravelmente influentes e grandiosos, fazendo brotar um gênero inédito de "heróis" populares dos direitos civis, "profanos e ranzinzas", "criptógrafos hostis" e frenéticos como o ritmo informacional gerado pela Internet exigia.

O *timing* da mobilização perseguida pelo cipher-ativismo, encabeçado pelos cypherpunks, parece ter surgido de uma convergência astral, o que igualmente assegura a atualidade e sensibilidade política da comunidade para com os desafios que o desenvolvimento tecnológico provocava no ecossistema social. De certa forma, já havia uma agenda contra a qual protestar e buscar reformas políticas, quer dizer, a flexibilização das regras para publicação e exportação de algoritmos criptográficos, as quais eram lançadas sobre diferentes alçadas governamentais e ilustravam a resistência dos Estados Unidos em ver verdadeiramente popularizado o uso técnicas de encriptação. Mas em abril de 1993, cinco meses depois da criação da lista de e-mail (documenta-se que foi lançada em setembro de 1992),[64] o *Clipper Chip* é proposto (sob o nome de *Escrowed Encryption Standard)* e irá concentrar a maior parte do debate público em torno da criptografia naquela década. E, da parte dos criptógrafos, defensores da privacidade e da sociedade civil de forma geral, já havia um modesto, mas enérgico e habilidoso exército já mobilizado para resistir às *cryptowars.*

5.4.2 **Cypherpunks vs. Uncle Sam[65]**

Como narrado, o *Clipper Chip* foi uma tentativa de política de vigilância em massa que consistia em aparelhar *backdoors* nas comunicações da população norte-americana sob a fachada de torná-las mais seguras. Além da resistência do setor

[64] Uma "Questions & Answers" detalhada foi mantida por Timothy May durante anos (1994).
[65] Tomei emprestado esse título do instrutivo artigo documental de Levy (1995)

industrial tecnológico, do ponto de vista da concorrência econômica, a sociedade civil deu origem a uma coalizão que representou um poderoso elo no bloqueio à proposta.

Em face do *Clipper*, Timothy May irá escrever um comunicado-chamado na lista de e-mail dos *cypherpunks,* em 1994, com o título "*The Coming Police State",* onde alerta que

> *The war is upon us (...) The Cypherpunks fill an important niche that none of the other major groups [como a Electronic Frontier Foundation ou a American Civil Liberties Union] wants to or are able to fill. (...) Plenty of problems face us, but we have plenty of talent, too. And of course we have justice and the inevitability of technology on our side* (May, 1994).

A expressão maior da máxima "cypherpunks write code", do manifesto Eric Hughes, foi explorada por Phil Zimmerman (Greenberg, 2012), o contraponto tecnológico de um debate que girava, em grande medida, em torno de distintas narrativas e abordagens sobre políticas públicas. A tecnologia que irá antagonizar o projeto político do *Clipper*, portanto, será o *Pretty Good Privacy* (PGP), criado por Zimmerman em 1991, uma ferramenta portátil de encriptação forte de dados (atualmente, é um standard para o envio de e-mails criptografados). O PGP radicalizou o acesso a técnicas de encriptação uma vez que foi distribuído como software livre e incorporava a criptografia de chave pública, possibilitando a encriptação da comunicação de entre duas partes que jamais haviam se encontrado.

Em um texto inspiracional, Zimmerman irá abordar o contexto tecnológico e político que girava em torno dos Estados Unidos, pontuando episódios como a espionagem antidemocrática através de grampos em integrantes de movimentos anti-guerra e grupos ligados aos direitos civis, como Martin Luther King, culminando em um estigma que não irá inspirar confiança. Portanto, nos anos noventa Zimmerman irá se dedicar ao desenvolvimento de técnicas de encriptação, enquanto símbolo do que os

cypherpunks[66] consideravam *tecno-libertário*. Na declaração "Why I Wrote PGP", explica que:

> *Throughout the 1990s, I figured that if we want to resist this unsettling trend in the government to outlaw cryptography, one measure we can apply is to use cryptography as much as we can now while it's still legal. When use of strong cryptography becomes popular, it's harder for the government to criminalize it. Therefore, using PGP is good for preserving democracy. If privacy is outlawed, only outlaws will have privacy.* (Zimmerman, 1999)

Após longa desconstrução argumentativa e denúncia dos gargalos técnicos e legais que o *Clipper* carregava, a proposta caiu em amplo descrédito com a população. Segundo levantamento da CNN, 80% dos norte-americanos não apoiavam a iniciativa. Dois terços dos entrevistados também responderam que seria mais importante proteger a privacidade em comunicações por telefone do que preservar a habilidade de interceptação dos agentes policiais (Elmer-Dewitt. 2001) Ainda que profundamente construído sob a égide da "lei e ordem", o *Clipper* parece não ter conseguido sensibilizar o público de que era mais importante vulnerabilizar as comunicações de toda a população em detrimento do combate ao terrorismo, ao tráfico de drogas e outras peças no repertório argumentativo do FBI. Resta imaginar como a população reagiria a um levantamento da mesma natureza, em tempos de Internet ubíqua - monopólios tecnológicos, colossais vazamentos de dados, desinformação e revelações de vigilância em massa.

Por fim, já foi apontado que são os *cypherpunks*, não os criptógrafos, os maiores defensores da criptografia (Rogaway, 2015). Mais amplamente, seria possível creditar os *cypherpunks* ou o movimento cipher-ativista como um dos pilares inaugurais da estruturação teórica e estratégica do ciberativismo e da recente história dos direitos

[66] Interessante notar que uma associação de Zimmerman com o movimento *cypherpunk* apenas se tornou mais orgânica quando o PGP se tornou o contraponto ao *Clipper* segundo a mídia. Antes disso a postura mais branda, menos anárquica e anti-governo de Zimmerman não o permitia se aproximar ideologicamente dos *cypherpunks.*

digitais. O laboratório oferecido pelos anos de *Clipper* ainda é paradigmático para batalhas legais futuras (Kehl; Wilson; Bankston, 2015), como o FBI vs. Apple ou os bloqueios do WhatsApp no Brasil. Sendo assim, cabe concluir que os *cypherpunks* não se restringem a círculos fechados em listas de e-mails ou aos anos noventa, mas são todos aqueles e aquelas que estão, hoje, na linha de frente da defesa pelos direitos e liberdades na rede.

6 DOGMÁTICA DO SIGILO DAS COMUNICAÇÕES E SIGILO CRIPTOGRÁFICO EM DISPUTA: ENTRE A (DES)OBRIGAÇÃO E A (I)LEGALIDADE

6.1 "Espaços livres da lei": qual a novidade?

Sob a reflexão de uma filosofia do sigilo[67], seria cabida (talvez pertinente), de fato, a indagação sobre a natureza, a finalidade ou, em último caso, a legalidade dos espaços (ou técnicas, de forma geral) destinados a preservar a intimidade e a autodeterminação informacional. Isso porque a eficácia das técnicas de proteção ao sigilo, em larga medida representada pela encriptação, se colocam como ponto de inflexão das disputadas narradas até aqui, quer dizer, a provocação proveniente de forças de investigação criminal sobre o papel desempenhado pela criptografia em uma sociedade que quer ver preservadas as liberdades individuais perante o poder do Estado e de sua agenda executiva de políticas de segurança pública.

Mais uma vez, pontos de partida exemplares para essa reflexão - que irá desaguar na análise à luz do arcabouço constitucional e infraconstitucional brasileiro - são os entendimentos vocalizados por atores investigativos. Ainda que sejam performados, muitas vezes, em espaços extra-judiciais (simpósios, discursos institucionais, entrevistas), irão refletir a demanda e entendimento processual, por exemplo, de promotorias e magistrados em casos que envolvam a produção de provas através da tentativa de suspensão do sigilo criptográfico. Independentemente do fenômeno criminal explorado para justificar o posicionamento (vide os enquadramentos acima narrados), irão apontar, fundamentalmente, para a questão: ao fim e ao cabo, o emprego de encriptação forte padece de legalidade?

---

[67] A "filosofia do sigilo" é, fato, uma sub-área da literatura sociológica, da ética e das ciências política. Não será explorada, contudo, a fundo, mas apenas utilizada como ponto de partida para a provocação sobre os meandros do entendimento legal, do ponto de vista jurisprudencial e dogmático, sobre os limites (se é que há) do sigilo.

Essa pergunta, certamente, é posta (e respondida) de outra forma pelas representações de agências investigativas quando buscam emplacar comunicações encriptadas como[68] "encriptação à prova de mandados" (Rosenstein, 2017); "zonas livres da lei" ou "ilimitadas áreas do mundo digital que são imunes ao escrutínio do sistema judiciário" (Rosen, 2019); espaços sem lei criados por donos de grandes empresas (Wray, 2019); "paraísos digitais" (Aras, 2019); ou "cenário livre na criminalidade, cenário livre!" (Leal, 2017). "Nunca houve espaços de absoluta privacidade" (Rosenstein, 2017), argumentam. Seu avesso seria, então, factível? Ou seja, já houve "espaços de absoluta vigilância"? (Pfefferkorn, 2017)

Este capítulo, portanto, sugere um breve resgate teórico sobre a construção da tutela da privacidade no Brasil para, em seguida, relacioná-la com o sentido normativo constitucional do sigilo e, paralelamente, com a trilha de possibilidades de suspensão do sigilo percorrida no mosaico legal de caráter procedimental. Esse objeto flutua sobre um entendimento legal pedregoso, ainda em disputa, que herda disciplinas sobre a regulação de telecomunicações no país e, em sua "tradução" - ou atualização - para endereçar a suspensão do sigilo diante de novas tecnologias, tropeça, encontrando incoerências analíticas e desafios de governança.

6.2 A construção teórica da suspensão ao sigilo

Para edificar a conceituação e previsão legal da privacidade no Brasil, a contribuição de Tércio Sampaio Ferraz Júnior é paradigmática. Em 1993, publica o ensaio *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado,* onde, da promulgação da Constituição Federal de 1988, traça um entendimento sobre o direito e a tutela da privacidade, correlacionando-os com o direito à

[68] Postas em sequência, é curioso notar que há uma "marca" distintiva pautada na repetição, sugerindo, verdadeiramente, uma estratégia persuasiva.

inviolabilidade do sigilo de dados. O trabalho, vale notar, localiza-se em um contexto temporal onde o impacto ocasionado pela Internet ainda não seria tão revolucionário tal como hoje o é, tampouco o impacto futuro era suficientemente mensurado.

Sampaio Júnior (1993), da observação do art. 5º, incisos X[69] e XII[70] da Constituição Federal, traça uma categorização em camadas do que se constituiria o direito à privacidade, elencando a dimensão do que se relacionaria com seus aspectos do indivíduo em sociedade, distinguindo-o (e.g. através do nome e imagem) em sua autonomia; a intimidade, em sua capacidade de "estar só"; e, por fim, o segredo, cujo direito será perseguido através do sigilo das comunicações. A privacidade deveria, portanto, ser observada através do "princípio da exclusividade", que a disporia em níveis distintos.

Dessa disciplina emanaria o art. 5º, inciso X, acima citado, ao assegurar o "domínio exclusivo" ao indivíduo. Em seguida, acoplado à *dimensão comunicativa* do direito à privacidade, haveria sentido o desenvolvimento do inciso XII do mesmo artigo, garantidor do direito à inviolabilidade do sigilo das comunicações, especificamente correspondência, comunicações telegráficas, dados e comunicações telefônicas. A esta última, em razão de sua natureza transitória (ao menos que gravada, uma comunicação por telefone se perde logo após que ocorre, já que acontece em fluxo, em trânsito), encontraria sentido a ressalva do inciso XII ao prever possibilidade de interceptação. As demais formas de comunicação não mereceriam a ressalva da suspensão do sigilo[71] na

---

[69] "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

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

[71] Há um debate hermenêutico, ainda, a respeito da interpretação semântico-gramatical do inciso XII do art. 5º. Há quem defenda que a expressão "em último caso" poderia ser traduzida por "em última circunstância" (*ultima ratio)*, e não como uma locução *em + o último caso*, o que restringiria a exceção apenas às comunicações telefônicas (citadas ao final). Essa leitura abriria caminho para que a excepcionalidade se estenda não somente às comunicações telefônicas, mas também a todas as comunicações elencadas no inciso. Sem me aprofundar na disputa interpretativa, este trabalho não se filia a essa interpretação simplesmente porque não há que se enxergar equívoco gramatical ou semântico na construção constitucional, tampouco essa leitura dialoga com a "volatilidade" do conteúdo, necessária a ensejar a previsão da suspensão do sigilo, como apontado por Ferraz Jr. Além disso, a regulação trazida pela Lei de

medida em que deixam rastros, vestígios e, logo, seriam passíveis de coleta no âmbito de investigações (via busca e apreensão, por exemplo, cumprido o devido processo legal), gerando as provas necessárias (Ferraz Jr. 1993). Frise-se, no entanto, que o postulado geral da garantia constitucional à privacidade se estende à obediência ao inciso XII, quer dizer, há de se estabelecer controles e garantias rígidas que efetivem a proteção à privacidade (Doneda, 2014)

6.2.1 **Interceptação na esfera das telecomunicações**

Em um salto contextual para o debate presente, essa distinção será fundamental diante da seguinte pergunta: a comunicação efetuada via Internet, encriptada ponta-a-ponta, dá-se em trânsito ou repouso? Mas antes de respondê-la, dando um passo atrás, é interessante considerar a norma procedimental sobre a suspensão do sigilo acima narrado, relativo às telecomunicações, ou seja, em trânsito.

A consequência direta à previsão de suspensão do sigilo, "nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" do mencionado inciso XII, será, em primeiro plano, a Lei de Interceptações (Lei nº 9.296/1996). Os termos que condicionam a interceptabilidade também farão parte do procedimento pré-estabelecido, exigindo-se que, por exemplo, a prova não possa ser obtida por outros meios disponíveis e que haja ordem judicial a requerimento de autoridade competente, demonstrada suficientemente a necessidade. O art. 7º da mesma Lei, como resultado, prevê que "para os procedimentos de interceptação de que trata essa Lei, a autoridade policial poderá requisitar serviços técnicos especializados às concessionárias de serviço público." O setor de telecomunicações, portanto, é o destinatário definitivo do procedimento (Abreu, 2017).

Interceptações abre seu art. 1º, justamente, com "A interceptação de comunicações telefônicas (...)", deixando claro o que quer endereçar. Nesse sentido, ver Mafei (2018).

A esse ponto, interessa notar que há *previsão técnica* estabelecida em um conjunto normativo para que os serviços de telecomunicações sejam *capazes* de suspender o sigilo de comunicações em trânsito. Portanto, compreenda-se que, ao menos, quatro elementos compõem a viabilidade de um *grampo*: (i) *previsão legal* de que haja (ii) *capacidade técnica* para que (iii) serviços *concessionários de telecomunicações* (iv) interceptam comunicações que ocorram *em trânsito.*

Resoluções da Agência Nacional de Telecomunicações (ANATEL), entidade reguladora do setor, então irão disciplinar a previsão de que as prestadoras de serviços de telecomunicações mantenham disponíveis meios tecnológicos para que as comunicações de usuários sejam acessíveis, via interceptação, em específicas circunstâncias processuais.[72] Em outras palavras, para fins de interceptação de comunicações telefônicas no Brasil, há uma previsão de que as prestadoras mantenham à disposição um *backdoor* em caso de requisição, por autoridade competente, de suspensão do sigilo mediante ordem judicial.[73]

---

[72] Um excelente levantamento normativo que trilha o caminho entre a exceção do art. 5º, inciso XII, até as resoluções da ANATEL, tendo como pano de fundo a disputa em torno da criptografia, pode ser encontrada em Abreu (2017)

[73] A previsão de necessidade de "habilidade e procedimento" para interceptação não deve ser vista de forma singela ou meramente tecnicista. Como toda análise deste trabalho, a transversal política também se apresenta na *práxis* da interceptação telefônica no país. Em 2009, a Corte Interamericana de Direitos Humanos (CIDH) da Organização dos Estados Americanos (OEA) condenou o Brasil a indenizar grupos de trabalhadores rurais associados ao Movimento dos Trabalhadores Rurais Sem Terra (MST) do Estado do Paraná, alvos de escutas injustificadas, requeridas por oficial não competente para tal, sem conhecimento do Ministério Público, e divulgação ilegal das gravações, no episódio que ficou conhecido como "Caso Escher". (Organização dos Estados Americanos, 2009). No mesmo caminho, comunicações estabelecidas entre o ex-presidente Luís Inácio "Lula" da Silva e a ex-presidenta Dilma Rousseff foram grampeadas e vazadas pelo então juiz Sérgio Moro. Os trechos vazados foram colhidos em momento em que a autorização para a interceptação já havia expirado, o que resultou na anulação processual do conteúdo graves repreensões ao juiz por parte do Supremo Tribunal Federal (Borges, 2016). Ainda em 2006, também foi noticiado grampo ilegal que tinha por alvo jornalistas da Rede Gazeta, resultando na "CPI do Grampo" (Século Diário, 2012) O histórico de abusos de grampos telefônicos já rendeu ao Brasil o título de "República da Escuta", disponível em https://grampo.org.

6.2.2 **Provedores de aplicação e a suspensão do sigilo revisitada**

Interessante voltar ao inciso XII do art. 5º da Constituição Federal para compreender a proteção ao sigilo na dinâmica do fluxo de dados em redes, na Internet. "[É] inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial (...). A Internet e suas aplicações - cuja transmissão de informações se baseia na comutação de pacotes,[74] ou seja, a transferência de dados através de diversas redes - portanto, enquadrariam-se na hipótese de "comunicação (...) de dados".

Como visto, a revisão da dogmática sobre intenção do constituinte permite entender que a única possibilidade de suspensão do sigilo (que irá cumprir procedimento detalhado através da Lei de Interceptações e das Resoluções da ANATEL) e para comunicações telefônicas. Isso porque as demais formas de comunicação - incluindo a comunicação de dados - deixam vestígio que podem compor um corpo probatório através de um mandado de busca e apreensão, uma solução menos invasiva do que a arquitetura estrutural de mecanismos que permitam a interceptação de comunicações.

A compreensão do Professor Tércio Sampaio Jr. busca estressar a questão:

> *Os outros três não sofreram semelhante ressalva porque, no interesse público, é possível realizar investigações e obter provas com base em vestígios que a comunicação deixa: a carta guardada, o testemunho de quem leu o nome do endereçado e do remetente, ou de quem viu a destruição do documento, o que vale também para o telegrama, para o telex, para o telefax, para a recepção da mensagem de um computador para outro, etc. Como isto é tecnicamente possível, o constituinte não permitiu absolutamente a entrada de terceiros, ainda que e m nome do interesse público, na comunicação.* (1992)

De toda forma, *qualquer* comunicação feita via Internet, baseada em transmissão de pacotes de dados, não merece a exceção ao sigilo representada pela possibilidade de

[74] Unidade de transferência de informação entre redes e computadores (Oliveira, 2011)

interceptação prevista no inciso XII do art. 5º da Constituição Federal. Ainda que fosse possível argumentar sobre a fácil efemeridade de dados comunicados via a rede, a possibilidade de serem rapidamente deletados ou auto-destruídos, o que traria desafios às forças policiais em termos de eficácia probatória, esse não é o sentido que enseja a interceptabilidade da comunicação telefônica, mas sim a natureza da comunicação (Mafei 2018), que não permite a busca e apreensão. Ademais, a fácil destrutibilidade da prova não é inovação trazida pela comunicação por dados via Internet já que sempre foi possível queimar as próprias correspondências ou vestígios de crimes deixados em papel: lista de propinas, diários, arquivos, entre outros. Nem por isso foi permitida a suspensão do sigilo desses tipos de comunicação, já que ficam armazenadas, tal como as realizadas via TCP/IP.[75]

6.2.2.1 ***A suspensão do sigilo no terreno da inconstitucionalidade***

Isso nos leva ao "coringa" trazido pelo art. 1, § 1º, da Lei de Interceptações: "O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática". Compreende-se que o legislador se antecipou à revolução comunicacional por vir, não se limitando a uma tecnologia única e dando certo grau de resiliência à Lei. Mas, ora, se a regulação da interceptação apenas guarda relação com as comunicações telefônicas em razão da sua natureza volátil, necessário seria haver uma extensão interpretativa delimitada do dispositivo.

Dois caminhos se bifurcam na hermenêutica que aplicará a previsão de interceptação de comunicações informáticas e telemáticas: um deles apontará que apenas aquelas comunicações por dados que em nenhuma hipótese fiquem armazenadas em servidores, sejam pessoais ou de parte do provedor de aplicação, poderão ser objeto de aplicação do dispositivo (aqui se entende, por exemplo, ligações via VoIP[76]); outra

[75] Protocolo básico de transmissão de pacotes e funcionamento da Internet.
[76] *Voice over IP.* Ainda que essa interpretação guarde maior grau de fidelidade ao texto constitucional, isso não significa dizer que provedores de aplicação que ofereçam serviços de VoIP devam carregar meios

caminhará para uma interpretação expansionista afeita à permissividade para que interceptações sejam possíveis em qualquer comunicação telemática, mesmo que em sistemas que envolvam o armazenamento de dados nas pontas da comunicação.[77] A terminologia "fluxo" da redação parece não cravar uma interpretação pacífica simples, já que tanto telefonemas quanto comunicações que serão armazenadas envolvem, em alguma medida, um fluxo informacional.

No caso da primeira delas - ainda que problemática do ponto de vista da fragilidade da massa de usuários na rede, envoltos e sendo objetos de mercantilização em mercados de dados pessoais, além da exponencial variedade de ataques por terceiros maliciosos - parece guardar alguma razoabilidade por respeitar o pré-requisito de que as comunicações aconteçam em trânsito. No segundo caso, haveria uma patente confusão sobre as bases técnicas sobre as quais os serviços via Internet se estabelecem, quer dizer, em sua grande maioria envolvem o registro do teor das comunicações. Como conclusão, não seria possível interpretar o art. 1, § 1º, da Lei de Interceptações para concluir aquilo que a Constituição jamais quis. Caso a gênese dessa previsão queira equiparar as comunicações "informáticas e telegráficas" para fins de interceptação, o dispositivo é inconstitucional.

6.2.3 **Interceptabilidade da encriptação ponta-a-ponta e os bloqueios do WhatsApp**

Apresentado o paradigma legal para limitar a violação do direito ao sigilo no contexto das aplicações de Internet, fica limpo o caminho para alocar a encriptação em um mosaico tecnológico, legislativo e processual. Isso porque os incidentes que irão atiçar bloqueios sobre a funcionalidade de plataformas em função de situações de "ininterceptabilidade" não somente provocam o exercício de uma revisão teórica, mas também terão que se deparar com a dinâmica re-contextualização tecnológica (que

capazes de interceptar as comunicações de seus usuários uma vez que não são regulados de forma a carregar *backdoors* mandatórios.

[77] Ver, por exemplo, a construção oferecida pelo Ministro Alexandre de Moraes em seu livro Curso de Direito Constitucional (2003).

envolve tanto avanços sobre as técnicas de sigilo quanto de interceptação e exploração de vulnerabilidade), a qual anda a passos largos.

6.2.3.1 ***Contexto jurídico-processual***

Entre 2015 e 2016, houve a determinação de quatro ordens de bloqueio ao aplicativo WhatsApp em território nacional, sendo as três últimas efetivamente cumpridas.[78] Em duas delas, de 2015, as ordens de bloqueio se deram em razão do descumprimento da plataforma em fornecer dados de seus usuários à justiça. Em 2016, outras duas ordens de bloqueio ocorreram em função da negativa - ou incapacidade - da plataforma em interceptar comunicações de seus usuários.

Cabe notar que a encriptação ponta-a-ponta de mensagens apenas foi implementada por padrão na plataforma, em todos os sistemas que operam o serviço, em 2016 (Ventura, 2016). Dessa forma, mostra-se especialmente pertinente para esta análise os bloqueios que ocorreram *em função* da criptografia ponta-a-ponta. Importante destacar, também, que as repercussões derivadas dos bloqueios não afetam simplesmente a plataforma, seu faturamento ou modelo de negócio, mas implicaram na suspensão do serviço para mais de cem milhões de usuários (Carneiro, 2016). Em 2015, chegou a extrapolar o território nacional e interrompeu a operação do serviço em regiões de países vizinhos da América Latina, como Chile e Argentina (Caputo, 2015).

No primeiro dos bloqueios ocorridos em 2016, as ordens foram baseadas no art. 12, inc. III[79], do Marco Civil da Internet. O juiz da Vara Criminal de Lagarto-SE, também acolheu o entendimento da Polícia Federal, de que, mesmo com criptografia ponta-a-ponta, seria possível realizar a interceptação. No episódio de bloqueio seguinte, derivado da 2ª Vara Criminal de Duque de Caxias-RJ, o WhatsApp receberia um ofício

[78] A sistematização dos bloqueios a seguir foi feita com o auxílio da documentação encontrada em https://bloqueios.info, projeto do centro de pesquisa InternetLab.

[79] Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa (...) III - suspensão temporária das atividades que envolvam os atos previstos no art. 11

que determinava que o serviço "desabilitasse" a chave de criptografia deixando de criptografar o fluxo de dados pelo prazo de quinze dias (Bloqueios,info, 2016). A juíza não fundamenta, em dispositivos legais, a ordem de bloqueio, mas assinala que "a codificação criptografada imposta às conversações online pelo WhatsApp não pode servir de escudo protetivo para práticas criminosas". Nesse ínterim, duas ações foram movidas perante o Supremo Tribunal Federal para apreciar a constitucionalidade das ordens de bloqueio: a Ação de Descumprimento de Preceito Fundamental (ADPF) nº 403 e a Ação Direta de Inconstitucionalidade (ADI) nº 5527.[80]

6.2.3.2 ***Teste de legalidade, proporcionalidade e eficácia***

A natureza dos serviços de comunicação baseados na transmissão de pacotes de dados que funcionam sobre protocolos de encriptação ponta-a-ponta, a exemplo do WhatsApp, não se confundem com telecomunicações. Esticando, ainda mais, o sentido da Lei de Interceptação, quando prevê que se aplica a comunicações telefônicas "de qualquer natureza", não haveria de incluir aplicações de Internet na medida em que essas, por constituírem "serviço de valor adicionado", não se confundem com os serviços de telecomunicações regulados pela ANATEL (Lefevre, 2017). Uma descrição distintiva, ademais, pode ser encontrada no art. 5º, incisos V[81] e VII,[82] do Marco Civil da Internet, e no art. 61[83] da Lei Geral de Telecomunicações.

Resgatando David Kaye, ex-Relator Especial das Nações Unidas para liberdade de Expressão e Opinião, Alimonti (2018) propõe um teste tripartite que poderia ser observado para medir qualquer proposta de limitação ao sigilo criptográfico, baseado nos eixos da (i) legalidade (ii) legitimidade e (iii) da proporcionalidade e necessidade da

---

[80] Até a data de publicação deste trabalho, ainda seguem em trâmite.

[81] V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

[82] VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet

[83] Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.

medida. Quanto à legalidade, o estabelecimento de um marco interpretativo que associa a regra geral da Constituição Federal e a exceção simbolizada pela Lei de Interceptações já preconiza que a possibilidade de suspensão do sigilo não se aplica ao WhatsApp, de início, em razão da natureza do serviço. Além disso, ainda que a interceptação de uma comunicação ponta-a-ponta fosse tecnicamente possível (não o é), uma ordem judicial dessa condição esbarraria no art. 2, inciso II[84], da Lei de Interceptações (Alimonti, 2018), uma vez que seria possível que o aparelho celular fosse capturado mediante uma ordem de busca e apreensão e fosse feita a extração das comunicações ali armazenadas mediante perícia técnica.

Em segundo lugar, uma proposta de acesso excepcional haveria de sopesar o conflito entre dois valores: a segurança da ordem pública, aqui representada pela garantia da eficácia das técnicas de investigação criminal que queiram ser empregadas, incluindo uma maior flexibilidade das possibilidades de suspensão ao sigilo, e, de outro lado, a segurança da informação,[85] um complexo arcabouço de proteção à confidencialidade, disponibilidade e integridade de sistemas de informação, instrumental à plena garantia da privacidade e que ganha relevância monumental em uma sociedade cada vez mais baseada e dependente de serviços públicos e privados oferecidos pela Internet. Encontraria, portanto, algum grau de "legitimidade" uma eventual proposta de *backdoor*. (Alimonti, 2018)

No entanto, um cenário resultante da prevalência das demandas das forças de segurança pública em detrimento da segurança da informação incorreria, efetivamente, na abertura exponencial de superfícies de ataque aos sistemas de comunicação. Uma analogia poderia ser feita com a banalização, já narrada, da exploração de "exceções" derivadas da *grampeabilidade* dos sistemas telefônicos. Considerando que serviços de mensageria via Internet são janelas de entrada para uma infinitude de dados pessoais

[84] II - a prova puder ser feita por outros meios disponíveis;

[85] Entende-se que esses são os termos do debate que deva ser travado, ao invés de um "natimorto" jogo entre "privacidade vs. segurança", uma vez que a governança da privacidade é transversal às técnicas de segurança, às *privacy-enhencing technologies* (PETs) e aos sistemas de caráter operacional que alocam a privacidade enquanto elemento fundamental. Mais sobre a falsa dicotomia entre "privacidade e segurança", ver Daniel Solove (2011). E sobre a falsa dicotomia no contexto da criptografia, ver Susan Landau (2018).

sensíveis, incluindo textos, fotos, áudios e vídeos, além de credenciais para múltiplos serviços acessíveis via celular, agentes maliciosos teriam ainda mais sucesso caso houvesse brechas a aplicações dessa natureza. A balança pesando a favor da "segurança" desejada por agências de investigação significa a vulnerabilização de toda a sociedade. Patentemente desproporcional, portanto, um mecanismo de acesso excepcional.

Ademais, importa repisar que, menos ainda, é sinalizado que o acesso excepcional carregaria o condão de ser necessário, vide a sustação de um eventual *backdoor* diante da leitura do Art. 2º, inciso II, da Lei de Interceptações, somado à realidade tecnológica e social, que ganha sentido diante da diversidade de técnicas capazes de produzir provas e possibilitar a vigilância operada por agentes do Estado. Sensores dispostos no espaço urbano, infiltrações em espaços físicos e digitais, coleta de metadados, operação de softwares de hacking por parte de agências de investigação, entre outros, compõem um ecossistema de técnicas que dá sentido ao que já foi chamado de "Era de Ouro da Vigilância" (Swire; Ahmad, 2011; Cardozo, 2018). Afastada, portanto, uma suposta condição de "*ultima ratio"* eventualmente creditada à interceptação de comunicações encriptadas ponta-a-ponta.

Como consequência, meios de acesso excepcional tampouco seriam eficazes no monitoramento das comunicações criminosas. Importa lembrar que o caráter transfronteiriço da Internet e suas aplicações torna disponíveis em território brasileiro uma gama de outros serviços poderiam ser oferecidos e utilizados por grupos criminosos para além do, digamos, WhatsApp.[86] Logo, a realidade sobre a acessibilidade a múltiplos serviços de criptografia ponta-a-ponta induz à compreensão de que propostas de *backdoors*, para fins de segurança pública, não passariam sequer no teste da eficácia.

Ainda, à luz do princípio da proporcionalidade trazido por Humberto Ávila (2004),[87] propostas de acesso excepcional, portanto, seriam inadequadas, uma vez que não garantiriam a eficácia de que as comunicações seriam efetivamente interceptadas

[86] Esse argumento, somado à constatação da desproporcionalidade de medidas dessa natureza, são precisamente alguns dos pontos levantados por Abelson et al (2015).
[87] Essa análise também pode ser encontrada em Ramiro et al (2020)

dada a possibilidade de evasão de criminosos das plataformas perseguidas; desnecessárias, diante da possibilidade de outros meios de coleção de evidências no processo probatório; e desproporcionais, levando ao monitoramento excessivo, criando brechas de segurança irreversíveis e, assim, soterrando o direito à privacidade e os meios de instrumentalizar sua salvaguarda. Se a privacidade flutua sobre constrições resultantes de uma realidade tecnológica sincrônica ao seu tempo (Doneda, 2017) também deve ser tutelada por soluções tecnológicas que permitam a salvaguarda dos direitos em questão, sob pena de padecer, obsoleta, sob a guarda de uma regulação desatualizada, anêmica.

6.3 Do juízo de primeiro grau ao STF: o expresso e o implícito, na lei, sobre criptografia

Dando continuidade ao sub-capítulo anterior na análise das ordens de interceptação e bloqueio do WhatsApp, em função do uso de encriptação ponta-a-ponta - e como propõem um quadro restritivo, de natureza punitivista, ao uso de novas tecnologias, remontando a uma cultura de criminalização tecnológica ao que é "novo"[88] - oferece-se, então, um contraponto plural a essa perspectiva. Busca-se apresentar não só a necessária permissão a técnicas de segurança robusta, mas também como o panorama legal brasileiro endereça o uso de criptografia como elemento de boas práticas - ou mesmo pré-requisito - sobre a governança da privacidade.

Tome-se, por exemplo, a ordem de bloqueio no terceiro dos episódios, da Vara Criminal de Lagarto, de abril de 2016. A magistrada irá /seguir uma trilha lógica ancorada no Marco Civil da Internet para concluir que o bloqueio do aplicativo seria plenamente previsto na legislação:[89]

---

[88] Associando-se aos debates como SOPA e PIPA, nos Estados Unidos, ou à Lei Azeredo no Brasil (também conhecida como "AI-5 Digital"), predecessora à construção do Marco Civil da Internet. Ver, por exemplo, Lemos e Souza (2016)

[89] Permito-me a longa citação para, friso, que a lógica da juíza seja bem assimilada. Dirimir eventuais margens indesejadas à interpretação do Marco Civil da Internet tem o potencial de evitar que prejuízos estruturais ao ecossistema da Internet e dos direitos à ela conexos ocorram, a exemplo do bloqueios de aplicações.

> Art. 10. A **guarda e a disponibilização** dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do **conteúdo de comunicações privadas**, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. (grifos da autora)
>
> §§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial** (...) (segundo grifo da autora)
>
> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> III - **suspensão temporária das atividades que envolvam os atos previstos no art. 11**[90] (...) (grifo da autora)
>
> (...)
>
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Resta concluir, portanto, que a fundamentação legal da decisão resultou no entendimento de que o MCI permitiria, em suma, "o bloqueio de aplicação que faça uso de encriptação ponta-a-ponta em caso de negativa de interceptação das comunicações." No entanto, o entendimento não guarda relação com a racionalidade da Lei, não estressa os fundamentos técnicos da criptografia ou mesmo observa a construção histórica da proteção ao sigilo no Brasil. Interessa notar que, no âmbito da audiência pública

[90] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

convocada pelo STF, especialistas tanto do campo técnico quanto da análise jurídica irão convergir na desconstrução da possibilidade do bloqueio.

Em primeiro lugar, no tocante à chamada ao Art. 10 do MCI, é curioso observar a sugestiva opção de grifos da decisão, "a guarda e disponibilização (...) do conteúdo de comunicações", inclinada ao enquadramento desejado tendente à retenção de dados. Negligencia, portanto, não somente a revisão da regra constitucional[91], mas o próprio pano de fundo finalístico do artigo, ou seja, a "preservação da intimidade, da vida privada, da honra e da imagem". Em uma leitura holística, é forçoso concluir que o artigo buscou evitar que a guarda e disponibilização de dados e conteúdos de comunicações desrespeitassem o devido processo legal (por exemplo, fornecendo *logs* de acesso e comunicações a autoridade não competentes ou carentes de ordem judicial) ou caíssem em dinâmicas de mercantilização de dados desreguladas, sem compromisso com os direitos dos titulares dos dados.

Quanto ao § 1º do mesmo artigo, ainda que a ordem judicial seja legítima, emitida por autoridade constituída de poderes para tal, não há lógica em obrigar o provedor a fornecer comunicações que não possui - e cuja tecnologia empregada carrega uma natureza que afasta, justamente, o intermediário para oferecer um *progresso* quanto à segurança da informação, reduzindo as superfícies de ataque. A criptografia forte, portanto, estabelece um limite ao cumprimento da ordem judicial.[92]

6.3.1 **Ação Direta de Inconstitucionalidade (ADI) nº 5527**

O art. 12, enfim, torna-se o epicentro da decisão de bloqueio e será o objeto, inclusive, da Ação Direta de Inconstitucionalidade (ADI) nº 5527. Com o intuito de contestar os bloqueios, a Ação julga inconstitucional o art. 12, incisos III e IV[93], do MCI,

[91] Do art. 5º, incisos X e XII, já analisados nesse trabalho.
[92] Àqueles que protestam diante desse limite imposto, para o bem ou para o mal, à presença do Estado, Demi Getschko (2016) responde que "[c]om excesso de bisbilhotagem e de quebra de privacidade, a Internet acaba encontrando formas de se defender".
[93] Uma extensão do inciso III, levando ao bloqueio das atividades previstas no art. 10.

sob o fundamento de que aplicativos mensageria, em razão da sua centralidade na dinâmica social e econômica, poderiam ser equiparados a serviços de telecomunicações,[94] merecendo, portanto, uma proteção constitucional em favor da continuidade do serviço. Qualifica esse entendimento em defesa do direito à liberdade de expressão encontrada na Constituição Federal e na Convenção Americana de Direitos Humanos (Brasil, 2016a).

Ainda que, finalisticamente, o entendimento da ADI nº 5527 busque a resiliência da rede e a proteção de liberdades da população, extensivamente afetadas pelos bloqueios, sua premissa parte do "avesso errado". Quer dizer, para pedir a inconstitucionalidade do art. 12, incisos III e IV, concorda a interpretação da magistrada sobre o fundamento do Marco Civil da Internet. Por isso mesmo, os argumentos que irão surgir a título de *amicus curiae* na ação pedirão a improcedência do pedido uma vez que houve equívoco de interpretação da Lei.[95]

Em primeiro plano, uma vez mais, a leitura seletiva, traduzida nos grifos da decisão, perde de vista o sentido panorâmico da previsão de *suspensão das atividades.* Como delimita o art. 11 do MCI, as "atividades" sobre as quais o art. 12, inciso III, refere-se dizem respeito às operações de "coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações", e não às atividades operativas e econômicas de forma generalizada, o que significaria a suspensão do serviço. A interrupção do fluxo das atividades, portanto, relaciona-se com a camada de conteúdos da Internet, e não com a camada de infraestrutura.[96] Além do mais, a opção pela "suspensão das atividades" guarda racionalidade associada às violações da privacidade, da proteção de dados pessoais e ao sigilo das comunicações quando não observados o devido

---

[94] Haveria ainda, um outro debate acerca da hipótese do WhatsApp ser um "serviço essencial" e, assim sendo, não poderia ser bloqueado. Ainda que esse trabalho assuma a desproporcionalidade do bloqueio tendo em vista a massa de usuários e a centralidade da plataforma para o ecossistema econômico, não concluo que a plataforma seria um "serviço essencial" tal como os serviços públicos ou concessionários de telecomunicações e provimento de Internet (ver, por exemplo, Idec, 2016).

[95] Por exemplo, a argumentação constante no *amicus curiae* proposto pelo Instituto Brasileiro para Internet e Democracia (IBIDEM), em parceria com o Laboratório de Políticas Públicas e Internet (LAPIN) em Brasil (2016a).

[96] É um dos entendimentos trazidos pelo ITS Rio, em sede de *amicus curiae*. A leitura se assimila consideravelmente com a da Frente Parlamentar pela Internet Livre e Sem Limites, também a título de *amicus curiae*. Ambos em Brasil (2016a).

processo legal ou os princípios que resguardam os direitos dos titulares de dados na esfera mercadológico-privada. O usuário, portanto, é o elo primário protegido na construção do MCI.

Jamais, portanto, serviços com encriptação ponta-a-ponta dariam margem tecnológica à cessão de comunicações a ações investigativas. Da mesma forma, não há previsão de suspensão do serviço ou bloqueio da aplicação em território nacional no art. 12, inciso III, do MCI.

6.3.2 **Ação de Descumprimento de Preceito Fundamental (ADPF) nº 403**

Diante do mesmo contexto de bloqueios de aplicações em função do emprego de encriptação ponta-a-ponta, é proposta a Ação de Descumprimento de Preceito Fundamental (ADPF) nº 403, de autoria do Partido Popular Socialista (PPS). A Ação tange parte da fundamentação da ADI nº 5527 ao sustentar que houve violação ao direito fundamental à liberdade de expressão e comunicação (art. 5º, inciso IX, da Constituição Federal) diante dos bloqueios, além da desproporcionalidade da medida - ainda que não queira afaste qualquer construção legal do Marco Civil, como a ADI. Pede, igualmente, que seja impedido qualquer bloqueio futuro que tenha por base os art. 10, § 2º, e o art. 12, incisos III e IV.

Os cinco pedidos de *amicus curiae* em grande medida convergem para pedir a procedência da ADPF.[97] Além dos argumentos acima desenvolvidos, a Frente Parlamentar pela Internet Livre e Sem Limites pleiteia que seja declarada inconstitucional qualquer espécie de interpretação do art. 10, caput e §2º, do Marco Civil que vá de encontro aos direitos fundamentais estabelecidos e herdados da Constituição Federal (Brasil, 2016b). Quer dizer, a guarda e a disponibilização de registros de conexão e acesso, conteúdos de comunicações e dados pessoais em geral, mesmo que deem margem de acesso a autoridades investigativas respeitado o devido processo legal, devem ter

[97] Um bom panorama dos pontos levantados pode ser encontrado em Barros (2016).

como centro gravitacional o usuário, titular dos dados. Esse espírito tem como alicerce a própria principiologia do Marco Civil, ou seja, a garantia da liberdade de expressão, a proteção da privacidade, de dados pessoais e a preservação da estabilidade, segurança e funcionalidade da rede.

6.3.3 **Os votos preliminares: um paradigma se desenha?**

Em maio de 2020, teve início o julgamento conjunto das duas Ações e foram proferidos, de antemão, os votos dos relatores, Ministra Rosa Weber (ADI nº 5527) e Ministro Edson Fachin (ADPF nº 403).

Resgatando a associação estreita entre o Marco Civil da Internet e a racionalidade que resguarda a construção sobre a proteção à privacidade e inviolabilidade do sigilo, a Ministra Weber, em suas "*Considerações sobre o direito à privacidade"* (Brasil, 2016a), resgata a construção conceitual primordial de Richard Posner e o pioneiro *The Right to Privacy*, de D. Warren e Louis Brandeis, para *atualizar* a definição de privacidade em Julie Cohen (2013), em uma abordagem "contemporânea a integradora", que parte, por si só, de uma crítica sociopolítica e econômica[98]: "a subjetividade emergente, dinâmica, dos esforços de atores comerciais e governamentais para tornar indivíduos e comunidades fixos, transparentes e predizíveis. Ela protege as práticas (…) através das quais a capacidade de autodeterminação se desenvolve." (Cohen, 2013)

Tal como a vertente que entende que devem ser relidas (e expandidas) as garantias à privacidade em função de desafios contemporâneos - "proliferação de sistemas de vigilância", "manipulação dos dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados" - propõe que há de se realizar escolhas entre suas "proteção ou exposição" em função, também, do desenvolvimento tecnológico. Essa leitura sinaliza que à medida que o indivíduo, hipossuficiente diante do aparato estatal enquanto "monitor" do fluxo de informações e

[98] Na minha leitura pessoal do voto.

da monopolização dos serviços e espaços online por grandes corporações, resta ao usuário se resguardar - ou se entrincheirar - lançando mão de novas tecnologias protetivas.

É negativa, portanto, a resposta da Ministra diante da dúvida sobre se seriam ilícitas as formas de proteção ao sigilo, mesmo aquelas que tornem inviável o cumprimento de mandados por parte de intermediários. Muito menos estariam sujeitos os agentes privados à obrigação de inserirem em seus sistemas recursos adicionais que possibilitem o acesso ao conteúdo das conversas - ou *backdoors* - ou à responsabilização em caso de descumprimento. "[N]ão pode o Estado compeli-lo a oferecer um serviço menos seguro e vulnerável", conclui a Ministra (Brasil, 2016a).

Interessa notar que há um constante esforço para realocar o debate para fora da esfera da falsa dicotomia onde usualmente o debate se anula. Logo, nota-se uma convergência, no sentido de que o debate não se dá, de fato, entre segurança pública e privacidade, já que "a mesma tecnologia que tornaria mais fácil às autoridades de segurança pública acessarem conteúdo armazenado pode – e, existindo, será – utilizada por criminosos para terem acesso a informações privadas de futuras vítimas" (Brasil, 2016a). O voto consolida o entendimento de que devem ser respeitadas as expectativas dos titulares de direitos - e que a criptografia atua, precisamente, no sentido de realizar as garantias de preservação ao sigilo das comunicações do art. 5º, XII, da Constituição.[99]

É traçado, na ADPF (lembre-se, pede a declaração de inconstitucionalidade dos bloqueios em questão e de eventuais futuros que tenham por base dispositivos do Marco Civil), um considerável alinhamento de referencial teórico-doutrinário em relação ao voto da Ministra. O Ministro parte de sete premissas para, então, desenvolver seu voto: (i) o impacto tecnológico implica na atualização do alcance de direitos e garantias fundamentais; (ii) direitos digitais são direitos fundamentais, equiparando a esfera *offline*

[99] O precedente já configura uma pedra de toque no fortalecimento das normas em defesa da privacidade e da proteção de dados no país (Canto; Ramiro; Real, 2020).

à *online;*[100] (iii) o pleno direito de acesso à Internet é condicionado à garantia da privacidade e da liberdade de expressão;[101] (iv) privacidade se relaciona com o controle as informações sobre si e de "determinar a maneira de construir sua própria esfera pública";[102] (v) a liberdade de expressão deve ser priorizada, sendo condição estruturante ao sistema democrático e (vi) e a criptografia - e o anonimato - são especialmente úteis ao compartilhamento de opiniões. A criptografia é instrumental à proteção de direitos, essenciais para a vida pública em uma sociedade democrática; (vii) há uma contradição em programar uma ideia de segurança pública e não promover uma Internet mais segura - um direito de todos e dever do Estado. Por fim, haveria de se haver uma certeza incontestável, por meio de mensuração cientificamente comprovada, de que uma insegurança eventualmente trazida com exceções à criptografia traria um ganho comparável em outras áreas.[103]

De início, é interessante notar que o Ministro se filia, em larga medida, aos argumentos trazidos pelas entidades da sociedade civil na oportunidade da Audiência Pública realizada ainda em 2017. Aborda a "demanda por criptografia" como uma espécie de legítima expectativa derivada da proteção à liberdade de expressão em um contexto social democrático. Por isso mesmo, diante do reconhecimento consolidado - tanto por organizações do terceiro setor quanto por agentes do Estado - de que a criptografia é protetiva ao ecossistema de direitos, é precisamente do interesse do Estado não buscar exceções, mas encorajar a implementação por parte de atores empresariais em suas aplicações e o consequente uso civil.

O argumento trazido pelo Ministro Fachin parece buscar uma conciliação resultante da conclusão que a segurança criptográfica também é afeita à segurança

---

[100] É bastante paradigmático que o conceito de *direitos digitais* - não plenamente positivado, mas que culturalmente abarca uma tradução necessária a localizar o debate sobre direitos fundamentais na Internet - tenha sido legitimado à nível de precedente da Suprema Corte.

[101] Em plena consonância com os pilares do Marco Civil da Internet.

[102] A premissa parece partir de um ideal contemporâneo sobre proteção de dados, pautado na autodeterminação informacional e que teria eixo no consentimento - e projeta essa premissa para a esfera social e política, para a liberdade da formação identitária perante o público.

[103] A falta de dados, estatísticas e outras comprovações metodologicamente comprovadas são uma constante nos pedidos de "acesso excepcional".

pública. Comumente, credita-se às representações governamentais um posicionamento sempre avesso à criptografia forte. Não é raro ver, por exemplo, setores da inteligência defendendo a expansão do uso criptografia:[104] no contexto do debate nos Estados Unidos, Michael Hayden, ex-diretor da NSA, alerta que "a segurança norte-americana é melhor servida com encriptação ponta a ponta inquebrável do que com portas da frente, dos fundos, laterais ou como você queira descrevê-lo; Mike McConell, também ex-diretor da NSA, Michael Chertoff, ex-secretário do Homeland Security e William Lynn, ex-Secretário Adjunto de Defesa dos Estados Unidos, atestam, em nota conjunta (McConnell; Chertoff; Lynn, 2015) que "tal sistema de encriptação [ponta-a-ponta] protegeria de ataques a privacidade individual e informações empresariais em um nível muito maior do que o que atualmente existe" e que "é essencial proteger interesses empresariais da massiva espionagem econômica. Esse imperativo deve compensar os benefícios táticos de se fazer mais acessíveis comunicações encriptadas a autoridades ocidentais".[105]

O Ministro irá pautar sua argumentação sob as bases teóricas e legislativas nacionais e internacionais da liberdade de expressão, objeto central da ADPF e, para o Ministro, direito essencialmente afetado por exceções à criptografia. As relatorias de autoria do ex-Relator Especial para Liberdade de Expressão e Opinião da ONU, David Kaye, são desenvolvidas e repisadas ao longo do voto: O receio da exposição diante do abuso governamental tolhe a potencialidade da pluralidade de opiniões na Internet, erodindo a autonomia individual (inclusive sob o ponto de vista do anonimato) e a autodeterminação informacional (Brasil, 2016b). O antídoto para o "efeito inibitório",[106] resultante do receio de exposição, estaria representada pela criptografia.

Apesar dos votos preliminares dos Ministros oferecerem uma bússola jurisprudencial sobre como a matéria será tratada na Corte, as ações seguem

---

[104] Sobre os dissensos nas narrativas governamentais sobre criptografia, ver Ramiro (2019).
[105] Com certeza, é notada a ironia em perceber a defesa de uma criptografia forte e onipresente justamente por parte da NSA, que opera massivos programas de criptanálise para fins de vigilância. Ver Auerbach e Opsahl (2013)
[106] Também conhecido como *chilling effect*. Ver Penney (2016)

inconclusivas. Restam os votos de três ministros, entre eles Alexandre de Moraes,[107] cujos pronunciamentos prévios sobre os bloqueios do WhatsApp e sobre a legalidade da criptografia o aproximam de medidas de expansão às capacidades investigativas policiais e da responsabilização de plataformas. Isso ocorreu, por exemplo, em seu apoio aos bloqueios do WhatsApp (Tecmundo, 2017) e em sua participação ativa na articulação de propostas legislativas para o acesso a comunicações encriptadas ponta-a-ponta (Passarinho, 2016).

6.4 A encriptação no Congresso

A aproximação legislativa na construção de políticas de encriptação são, em geral, respostas a sensibilidades sociais e fatos políticos que acendem a atenção da sociedade e, portanto, parlamentares buscam responder às inquietações. Ainda que pareça uma equação lógica-legislativa, políticas públicas baseadas unicamente em uma abordagem reativa pecam por não priorizarem um passo que priorize o debate multissetorial, consultas públicas, a oitiva de especialistas e, por fim, por buscarem responder a determinadas tensões à curto prazo.[108] Processos dessa natureza dificilmente medem a complexidade da rede ou anteveem o desenvolvimento tecnológico suficientemente, resultando em propostas pouco resilientes e/ou ameaçadoras em termos de respeito ao ecossistema de direitos fundamentais.

Além disso, é crucial ter em vista que o caráter transfronteiriço da Internet já não permite que as legislações que tenham por objeto novas tecnologias observem apenas a realidade doméstica. Aplicações são disponibilizadas e efetivamente utilizadas em caráter global, muitas vezes passando a compreender um recurso básico na logística econômica do país.[109] Observando - que fique claro - a soberania nacional, o respeito às instituições e

[107] Ver, também, nota de rodapé número 112.
[108] Esse entendimento é especialmente caro às políticas de cibersegurança. Ver Internet Society (2017).
[109] Ver o Capítulo 7.

o princípio da legalidade, é sedimentado no Marco Civil da Internet[110] que a disciplina do uso da Internet tem por objetivo, para citar alguns, a promoção do direito e acesso à Internet a todos, o acesso à informação, a inovação e o fomento à difusão de novas tecnologias.[111] Logo, regulações devem ser balizadas à luz de parâmetros potencializadores de uma sociedade em rede inclusiva.

6.4.1 **Projeto de Lei nº 9.808/2018: amplos poderes ao delegado de polícia**

Associando-se a uma tendência de políticas públicas de Internet de natureza reativa a sensibilidades sociais, alguns PLs no Brasil oferecem um mosaico multifacetado sobre como percebem (ou mesmo não chegam a perceber) a práxis da encriptação no País.[112] Serão apontados três projetos que parecem ilustrar suficientemente uma tendência perceptiva sobre as relações entre tecnologia e sociedade no Brasil e, em grande medida, se associam a uma agenda da "lei e ordem", afeita ao "combate à criminalidade" e com inclinações argumentativas bastante parecidas às das agências de investigação norte-americanas, quer dizer, pautadas na perda das capacidades de produzir provas e na expansão de procedimentos que viabilizem a vigilância contínua.

Nesse contexto, o Projeto de Lei nº 9.808/2018, de autoria do deputado federal João Câmara (Republicanos-GO), se destaca e sugere ser uma resposta parlamentar à fricção causada pela interpretação da Constituição Federal e do Marco Civil da Internet que resultou nos bloqueios do WhatsApp (Brasil, 2018a). A proposta, portanto, irá propor alterações no Marco Civil da Internet para permitir que agentes policiais tenham

---

[110] É imprescindível mencionar, igualmente, que o Decreto regulamentar do Marco Civil da Internet, nº 8.771/2016, estabelece expressamente que, nas operações com dados dos usuários, os provedores de aplicação deverão devem observar padrões de segurança que compreendam soluções de gestão que garantam a inviolabilidade dos dados, como a criptografia (Art. 13, § 4º)

[111] Art. 4º, incisos I, II, III e IV.

[112] Em 2020, tive a oportunidade de realizar investigação precisamente sobre as principais características dos Projetos de Lei sobre criptografia no Brasil. Aproveito para agradecer os(as) companheiros(as) de pesquisa Mariana Canto, Paula Côrte Real, José Paulo Lima e Thaís Aguiar, sem os quais o estudo não seria possível. Ver Ramiro et al (2020)

autoridade, diante de provedores de aplicação, para requisitar dados criptografados sem que haja necessidade de uma intermediação judicial.

O *background* pintado pelo autor sugere que a utilização de aplicativos via Internet vem sendo empregada como escudos por criminosos em várias localidades do mundo e, portanto, diante de flagrante de crime hediondo, o delegado de polícia teria legitimidade para decidir sobre a suspensão ao sigilo. Vejamos:

> § 5º - Encontrando-se o agente em situação flagrante de crimes definidos em lei como hediondo, de tráfico de drogas ou terrorismo, poderá o delegado de polícia acessar, **independente de autorização judicial**, os dados de registro e conteúdos de comunicação privada de dispositivo móvel, quando necessário à investigação e/ou à interrupção da ação delitiva.
>
> § 6º - No caso do parágrafo anterior, **em se tratando de dados criptografados, poderá o delegado de polícia requisitar, diretamente aos provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação, o fornecimento de chave criptográfica** que permita o acesso aos dados e conteúdos de comunicação privada de dispositivo móvel, sem prejuízo do desenvolvimento e emprego, pelas polícias judiciárias, de técnicas e ferramentas tecnológicas que atinjam esse fim específico, incluindo a utilização de dispositivos que possibilitem o acesso a conteúdo anterior à criptografia por meio de aplicativos, sistemas ou outras ferramentas (Brasil, 2018a). (grifos meus)

De início, é desafiador vislumbrar qualquer cenário em que provedores de Internet façam uso de criptografia e/ou possuam a habilidade de conceder chaves criptográficas - sequer as detém. O provimento de conexão à Internet é pautado pelo princípio neutralidade da rede, o que quer dizer que não haverá o provedor que discriminar o tráfego de acordo com o conteúdo e, portanto, não haveria de empregar técnicas de *deep packet inspection*, impedido de inspecionar a fundo a natureza dos dados em trânsito ou tomar medidas como bloqueio ou interceptação. “Autores de aplicativo” tampouco constituem uma terminologia que parece endereçar bem o problema. O WhatsApp, por exemplo, é de autoria diversa daqueles que o administram, o Facebook, o que tornaria

ineficaz demandar do "autor do aplicativo" uma suposta chave de decriptação. Ainda, caso previsse a cessão de chave de decriptação a provedores de aplicação que empregassem encriptação ponta-a-ponta, a medida seria inócua, tornaria-se uma Lei tecnologicamente anacrônica, já que não se está diante de arquiteturas de sistemas que prevejam sequer esse recurso.

O mais preocupante no PL, porém, é a previsão de que uma parte ativa na investigação - o delegado, agente investigativo - chame para si a legitimidade e imparcialidade para decidir se seu próprio pedido cumpre com os requisitos para a suspensão do sigilo.[113] O desenho proposto pelo procedimento subverte a lógica de intermediação de autoridade competente - o juiz, parte imparcial no sistema judicial - para realizar o teste de pesos e contrapesos diante de um conflito de direitos (sigilo das comunicações e persecução criminal). O PL, portanto, abre ampla margem à arbitrariedade policial e erode a racionalidade do Estado Democrático de Direito. A encriptação forte, resta dizer, surge precisamente para sustar violações contra a inviolabilidade do sigilo.

6.4.2 **Projeto de Lei nº 2.418/2019: filtragem em massa das comunicações**

O Projeto de Lei nº 2.418/2019, de autoria do deputado José Medeiros (PODE-MT), igualmente propõe obrigações operacionais a intermediários em nome do monitoramento de conteúdos criminosos - não surpreendentemente, atividades terroristas e crimes hediondos (Brasil, 2019a) A sua maneira, que positivar um sistema de vigilância

[113] Esse raciocínio, na realidade, não é novo na dogmática. O Ministro do STF Alexandre de Moraes (sobre o qual falei brevemente quando analisando as ações que tramitam no STF sobre os bloqueios do WhatsApp) considera, em seu livro "Curso de Direito Constitucional", que seria cogitável um modelo de "legalidade *a posteriori"*, onde a autoridade investigativa teria a liberdade de, por exemplo, interceptar investigações ou suspender o sigilo dos dados junto a um provedor de serviços. Depois, apresentaria à apreciação judicial, a qual julgaria sobre a legalidade da coleta da prova, aproveitando-a ou a invalidando (Moraes, 2003). Em razão de toda a argumentação desenvolvida nesse trabalho e do ponto de vista político, legal, procedimental, de direitos humanos, tecnológico, socioeconômico e tantos outros, considero essa possibilidade impensável e, de certa forma, distópica.

mandatório cuja responsabilidade recairia sobre os provedores. Quer, enfim, a alteração do Marco Civil da Internet para prever que

> Art. 21-A. Os provedores de aplicações deverão **monitorar ativamente publicações de seus usuários que impliquem atos preparatórios ou ameaças de crimes hediondos ou de terrorismo**, nos termos da Lei nº 13.260/2016.
>
> § 1º As publicações mencionadas no caput **deverão ser repassadas às autoridades competentes**, na forma do regulamento.
>
> (...)
>
> § 3º **Na impossibilidade eventual e justificada de cumprimento do disposto no caput, os provedores de aplicações deverão permitir a instalação de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para o mesmo fim**. (grifos meus)

Em sua justificativa, o PL entende que está se tornando comum a publicização de atentados terroristas na Internet, a exemplo do que ocorreu na cidade de Christchurch (BBC News, 2020). Redes sociais seriam frequentemente espaços para o planejamento de ataques extremistas, como o que ocorreu em na cidade de Suzano (G1, 2019). Não quer "regular a deep web", mas sim as plataformas que operam na superfície.

A abordagem reativa de propostas de políticas públicas dessa natureza ficam evidentes quando constatado, por exemplo, que o intervalo de tempo entre os tiroteios em Suzano (13 de março de 2019) e a propositura do PL (17 de abril de 2019) tem pouco mais de um mês, tempo impensável para uma compreensão extensiva da complexidade sociopolítica do próprio fato político e das possíveis implicações legais e tecnológicas de um monitoramento em massa das comunicações.

No mérito, o PL é duplamente delicado. Primeiro, em termos operacionais, apenas plataformas que não possuíssem encriptação ponta-a-ponta dos conteúdos produzidos por seus usuários iriam poder implementar a proposta. Do ponto de vista de um provedor que tenha encriptação ponta-a-ponta, resta-lhe duas saídas: retroceder para intermediar as

mensagens, agora sem encriptação ponta-a-ponta, e ativar um monitoramento em massa sobre o conteúdo das comunicações;[114] ou permitir, como prevê o § 3º, que autoridades instalem softwares em seus sistemas e, assim, filtrem as comunicações.

A proposta irá atuar pelas mesmas vias excessivas quando analisadas tendo em vista os princípios da proporcionalidade e da necessidade.[115] Inicialmente, objetivando detectar atividades terroristas ou extremistas, propõe uma filtragem prévia de todas as comunicações, uma abordagem largamente desproporcional e *orwelliana.*[116] Tipificando uma política de vigilância em massa *per se*, busca estabelecer uma infraestrutura que, apoiada em obrigação legal, só capturaria crimes hediondos e terrorismo a princípio, mas que já estaria armada caso conteúdos de outras naturezas entrem no radar da agenda de segurança pública.

Ademais, ao não dimensionar a extensão das violações a direitos fundamentais - aqui, a liberdade de expressão seria profundamente afetada diante de um efeito inibitório generalizado aos usuários causado pelo monitoramento ativo e permanente de suas comunicações - perde de vista a real *necessidade* da proposta, ou seja, não parece considerar outras medidas menos invasivas.

Por fim, tal como sustentado ao longo do trabalho, algumas consequências diretas do emprego de técnicas de interceptação - aqui ininterruptas e para todos - podem ser apontadas: bem como a ampliação de dados disponíveis à comercialização pelas plataformas e por *brokers* de dados, agregando mais dados sensíveis à lógica do capitalismo de vigilância; bem como a abertura de possibilidades para que as brechas sejam aproveitadas para uso indevido, ilegal ou ilegítimo tanto por parte de agentes estatais quanto por atores privados malicioso que aproveitariam a expandida a superfície de ataque, agora mandatória. Logo, a questão não é *se* ocorreria algum incidente de segurança enquanto efeito colateral de tal proposta, mas *quando.*

---

[114] Nasceria, aqui, uma nova categoria de *backdoor*, embarcado com inteligência artificial para detectar atividades suspeitas?
[115] É válido conferir o projeto "Necessary and Proportionate", da Electronic Frontier Foundation.
[116] Referência ao romance distópico "1984", de George Orwell (1948).

7 A CRIPTOGRAFIA ENQUANTO TECNOLOGIA TRANSVERSAL ÀS POLÍTICAS ECONÔMICAS, SERVIÇOS PÚBLICOS E CIBERSEGURANÇA NO BRASIL

7.1 A agenda econômica atrelada à segurança criptográfica

Desde o ecossistema de inovação tecnológica, com a criação de novos mercados, à digitalização de serviços tradicionais, a encriptação de canais de comunicação e o estabelecimento de rotinas robustas de segurança para o armazenamento de informação são alguns dos primeiros passos para a estabilidade de serviços que se localizam no campo econômico. Novos serviços com base em blockchain, certificação digital, canais de comunicação *peer to peer* (P2P), ou mesmo a administração de redes elétricas, de tráfego aéreo e o funcionamento de usinas nucleares: todas as aplicações fazem parte de um amplo leque cujo valor econômico se associa, em maior ou menor medida, à segurança de suas plataformas e sistemas. Em outras palavras, a robustez da criptografia desses sistemas agrega valor aos serviços. Como aponta pesquisa realizada pelo Niskanen Center, think tank norte-americano com foco na proteção de direitos a partir de princípios orientados para o mercado, "a economia moderna seria significativamente enfraquecida com a implementação de 'menos-do-que-ótima' segurança criptográfica em detrimento de indivíduos, dos negócios e das agências governamentais" (Hagemann; Hampson, 2015).

Já em 1997, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 1997) adotava diretrizes que traduzem a preocupação do órgão a nível de comércio global associado à emergente adoção das novas TIC, no sentido de que padrões criptográficos fossem estimulados de forma a gerar segurança ao mercado (OCDE, 1997). Atualmente, a OCDE se mantém elencando a adoção de padrões robustos de segurança, a exemplo de criptografia ponta-a-ponta, enquanto prioridade em suas diretrizes para o desenvolvimento econômico internacional, em uma associação que

busca, inclusive, endereçar desde a competitividade de mercado, à proteção de dados de usuários (OCDE, 2020), alimentando, portanto, perspectivas relativas à garantia de direitos nas dinâmicas de cooperação econômica que digam respeito à Internet.

Em diálogo com os parâmetros da OCDE, vale destacar, a essa altura, que a Lei Geral de Proteção de Dados (LGPD, nº 13.709/2018) guarda uma seção específica para a segurança da informação. Em seu artigo 46, compreende que os agentes de tratamento devem fazer todos os esforços técnicos e administrativos a seu alcance para afastar possibilidades de acesso não autorizado. Das técnicas de segurança da informação, portanto, os protocolos de encriptação são pedras angulares. Adiante, o artigo 48 vai disciplinar o ponto de partida procedimental para que os agentes de tratamento comuniquem à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de um eventual incidente de segurança. Em seu § 3º, em seguida, fica claro que a Autoridade vai averiguar a gravidade do incidente e a extensão da responsabilidade do agente de tratamento observando, entre outros fatores, se os dados afetados estavam "ininteligíveis". Ora, falar em ininteligibilidade dos dados vazados é, poderia-se argumentar, perguntar se os dados estavam criptografados.

O Fórum Econômico Mundial (FEM) também reflete, em suas arenas de discussão publicações, a relevância da criptografia no contexto do circuito empresarial-econômico internacional, inclusive dedicando uma agenda própria à produção de conteúdo sobre cibersegurança e confiabilidade digital no contexto do sistema econômico. Em relatório publicado em 2020 sobre os maiores riscos para a economia global, o FEM aponta que os ciberataques estão entre os dez maiores tanto em termos de probabilidade quanto de impacto à economia global, em uma lista que agrega ainda eventos como armas de destruição em massa e perda de biodiversidade.[117] Em

[117] Interessante notar que o FEM não se posiciona tão enfaticamente a favor de uma criptografia forte, mas chega a fazer considerações, por exemplo, sobre os benefícios econômicos de comunicações não encriptadas ponta a ponta no contexto de políticas públicas que enfraqueçam a criptografia: "However, it is important to acknowledge that end-to-end encryption threatens business models premised on monetizing individual specific attributes (...). In adopting end-to-end encryption, companies limit the ability to inspect communications. In so doing, companies limit the inferences they are capable of making regarding an individual — whether that individual is likely young or old, male or female, etc." World Economic Forum

resumo, os danos potenciais à economia mundial quando se tratando de sistemas cuja proteção depende de um confiável e resiliente plano de cibersegurança se encontram no mesmo horizonte que, por exemplo, armas nucleares.

Do ponto de vista das economias emergentes, estima-se que o e-commerce tenha movimentado 3.53 trilhões de dólares entre 2014 e 2019 (totalizando 14% do varejo neste ano) (Statista, 2020). Só no Brasil, é prevista uma movimentação que irá superar 16.7 bilhões de dólares até o fim de 2020 (Statista, 2021). Cada informação de consumo, desde o tráfego de dados sobre cartão de crédito ao armazenamento de informações em bancos de dados do prestador dos serviços, protocolos de criptografia são utilizados para os dados em trânsito e repouso. O uso de criptografia permite a integridade de transações e pode formar a base mínima para uma infraestrutura de e-commerce. Pode-se dizer que esse gênero de segurança está no centro das preocupações de todo empreendedor que solicite, armazene ou comunique qualquer espécie de informação cuja perda seja um risco grave (Palfrey, 2021).

A reinvenção de serviços tradicionais, através da digitalização de seus processos para atender a uma demanda global relativa a transações online, também buscam os requisitos de confiança mínimos derivados da segurança da informação e, aqui, os serviços bancários são exemplares. O investimento somado às despesas com tecnologias nesse setor, no Brasil, chegou a 24.6 bilhões de reais no ano de 2019 e as transações bancárias com *mobile* e *Internet banking* superaram 56 bilhões de reais no mesmo ano (Febraban, 2020). Do acesso ao aplicativo, passando por pagamentos, transferências, depósitos, empréstimos, aplicações de rendimento e armazenamento de dados nos servidores do serviço contratado, a criptografia no armazenamento e tráfego de dados assume um papel central para reduzir drasticamente o número de casos de clonagem de cartões e outras espécies de fraudes financeiras.

(2018). Ao passo que pôr as cartas na mesa, em termos de benefícios vs. prejuízos, seja interessante para um debate honesto, evidencia-se como o mercado de dados pessoais, o qual se associa a análises preditivas comportamentais, compreende um circuito econômico que seria digno de verdadeira consideração pelo FEM quanto a seus frutos econômicos. Sobre a teorização do capitalismo de vigilância, ver Zuboff (2018)

Se observada a construção de estratégias econômicas governamentais no País, as TIC aparecem no centro das políticas públicas do governo federal. Na leitura da Estratégia Nacional para o Desenvolvimento Econômico e Social de 2018 (ENDES), de responsabilidade do Ministério do Planejamento, Desenvolvimento e Gestão, e que considera o planejamento econômico nacional para o período de 2020 a 2031, fica clara a priorização da digitalização do mercado nacional, a partir de metas que envolvem

> *incentivar o desenvolvimento da economia digital, ampliando o apoio à difusão de tecnologias emergentes (interconectividade, automação, energias, nanotecnologia, novos materiais e biotecnologias) (...);*[118]
>
> *desenvolver e ampliar a difusão de tecnologias críticas, sobretudo dos setores nuclear, aeroespacial e cibernético;*[119]
>
> *(...)*
>
> *fortalecer os segmentos inovadores como possíveis eixos de desenvolvimento, tais como a economia criativa, a economia digital (...) de forma a induzir o desenvolvimento de uma economia baseada em informação, preservando os direitos individuais.*[120]

[118] A referida meta está em consonância com as mencionadas estatísticas relativas ao e-commerce, por exemplo, e o "apoio à difusão de tecnologias emergentes" também deve considerar técnicas de segurança da informação em sua implementação. A interconectividade e inteligência artificial que acompanham os carros autônomos, por exemplo, precisam contar com criptografia de ponta para que a integridade das informações não seja quebrada (por imprevisão do sistema ou ataque malicioso), ocasionando falha na comunicação com os freios, para citar apenas uma situação possível. Para uma abordagem completa, ver Chattopadhyay e Lam (2018).

[119] Para ficar com o caso da difusão de tecnologia no setor de energia nuclear (sem entrar em considerações sobre riscos ambientais ou da ética científica), vale lembrar do Stuxnet, *worm (malware* independente e replicável) descoberto em 2010 e considerado responsável por grandes danos no programa nuclear iraniano; ou da usina nuclear de Davis-Besse, nos Estados Unidos, infectada, também, por um *worm,* tornando o sistema de exibição do parâmetro de segurança inacessível para os operadores. Para esses e outros casos, a criptografia faz parte dos principais recursos de defesa. Mais em Poresky et al (2017).

[120] Em paralelo à menção à garantia de direitos no ecossistema econômico digital já percebida nas recentes diretrizes da OCDE, a ENDES também parece assimilar que as atividades baseadas na coleta de dados devem se balizar na proteção aos direitos individuais, como a proteção de dados.

Consequentemente, a integração desses sistemas chamam atenção para crescentes investimentos em recursos de segurança da informação como forma de inserção no mercado global digitalizado.

No âmbito do Ministério da Ciência, Tecnologia, Inovações e Comunicação (MCTIC), a Estratégia Nacional de Ciência, Tecnologia e Inovação, construída levando-se em conta o período de 2016 a 2022, estabelece que a segurança cibernética é tema prioritário no acompanhamento a tendências econômicas mundiais em ciência e tecnologia, como a Internet das Coisas (IoT) e a computação em nuvem, bem como eleva a competitividade produtiva nacional (Brasil, 2016c). Da mesma forma, na Estratégia Brasileira para a Transformação Digital de 2018 (E-Digital), elaborada igualmente no âmbito do MCTIC, a criptografia aparece explicitamente como prioridade de investimentos para se alcançar melhor desempenho em Pesquisa, Desenvolvimento e Inovação (PD&I) (Brasil, 2018b). A agenda econômica de variados setores do Governo Federal tem se mostrado inclinada ao avanço em técnicas de segurança da informação, as quais passam, necessariamente, pelo desenvolvimento e adoção contínua e crescente de técnicas de criptografia.

Em alguma medida, o debate público e as tensões entre os setores de investigação criminal, sociedade civil e algumas empresas pontuais, como a Apple e o Facebook, têm orbitado, de forma mais notável, em torno da privacidade e da segurança em aplicações de mensageria ponta a ponta, ofuscado, de certa forma, a dimensão econômica da criptografia para o ecossistema das TIC de forma ampla. Mas se torna patente que a defesa da estabilidade e da competitividade da indústria tecnológica nacional e do processo da digitalização de serviços passa pelo fomento dos níveis de confiança e resiliência dos serviços. Esses níveis são alcançados, em grande medida, com arquiteturas de segurança da informação, como sustenta os organismos de articulação econômica internacionais, como a OCDE. E a criptografia é a pedra angular para a segurança dessa virada econômica no que diz respeito à informatização de seus sistemas.

7.2 Diretrizes de segurança para serviços públicos e segurança nacional

A agenda do setor governamental em relação à criptografia é multifacetada. Se, por um lado, encontramos a plena advocacia em favor da criptografia, proveniente de setores relacionados à segurança nacional e da coletividade, comunicações governamentais e à inteligência, por outro lado, depara-se com representações de forças policiais, de segurança pública e investigações criminais cuja defesa do enfraquecimento da criptografia é suficientemente conhecida e vocalizada. Como essa última perspectiva foi analisada com atenção redobrada nos capítulos anteriores, este tópico buscará explorar a primeira dessas visões.

Uma vez que a plena execução de política públicas, a administração de sistemas da administração pública, o armazenamento de dados dos cidadãos, a comunicação de agentes políticos, chefes dos poderes executivos, superintendentes e diretores de órgãos e empresas públicas e tantos outros processos atinentes ao funcionamento do Estado dependem de sistemas de informação conectados, a segurança cibernética representa um eixo de investimento político-econômico fundamental para a segurança nacional, independentemente do país em questão. Para ilustrar, estima-se que os Estados Unidos irão gastar, no setor de segurança cibernética, cerca de 18.5 bilhões de dólares em 2021 (Homeland Security Today, 2020), e que a China tenha gasto 7.35 bilhões de dólares em 2019 (XinhuaNet, 2019).

Segundo o Global Cybersecurity Index de 2018, da União Internacional de Telecomunicações (UIT), o Brasil ocupa o 70º lugar em termos de comprometimento com cibersegurança (UIT, 2018) Mesmo assim, é possível resgatar a construção paulatina de planejamento, ainda que incipiente, de políticas públicas brasileiras em cibersegurança. O reconhecimento governamental de que o tema deveria ser objeto de um plano estratégico nacional específico surge com a Estratégia Nacional de Defesa, que aloca a cibersegurança como prioridade, lado a lado com os setores nuclear e espacial (Brasil, 2008). Ainda em 2010, como parte do “Plano Brasil 2022”, foi lançado “Livro Verde da Segurança Cibernética no Brasil”, reunindo diretrizes básicas, “visando iniciar

amplo debate social, econômico, político e técnico-científico sobre a Segurança Cibernética no Brasil". Entre seus diagnósticos, reconhecia que a criptografia era sub-área importante de pesquisa em segurança da informação para o país.

A essa altura, é fundamental mencionar que a Agência Brasileira de Inteligência (ABIn), em 2013, chegou a desenvolver novos protocolos criptográficos para uso do alto escalão governamental, o CriptoGOV e o cGOV (Agência Brasileira de Inteligência, 2020), em reação às denúncias de espionagem de Edward Snowden, segundo as quais haveria um amplo programa de vigilância em massa promovida pela *National Security Agency* (NSA), incluindo a espionagem de vários líderes governamentais, como a ex-presidenta Dilma Rousseff (Estadão, 2013). Seria possível dizer que, nesse momento, tem-se origem uma racionalidade governamental que passa a refletir com mais maturidade sobre cibersegurança e de forma mais focada na soberania dos produtos tecnológicos, incluindo os criptográficos.

No ano seguinte, e 2014, como resultado da "CPI da Espionagem", Comissão Parlamentar de Inquérito aberta no Senado (Brasil, 2013) e destinada a investigar as revelações de vigilância empregada pelos Estados Unidos no Brasil, restou patente que o país se encontrava em situação de vulnerabilidade; que necessitava da promoção de uma cultura de segurança entre os brasileiros[121]; e que se tornasse mais enfática a produção de protocolos criptográficos nacionais - raciocínio que está amplamente presente no relatório final da CPI[122].

---

[121] Neste ponto, interessa notar que a "cultura de segurança", destacada no relatório final à CPI da Espionagem, ganha fôlego após as revelações de Snowden, mas já é posta de lado nas rotinas comunicacionais dos integrantes do governo em momento posterior. Em 2016, Dilma Rousseff teve seu telefone novamente grampeado, dessa vez por ordem do ex-Juiz Sérgio Moro. Na ocasião, chegou a ouvir um "eu avisei", por parte de Edward Snowden. No início do mandato, Jair Bolsonaro também foi amplamente criticado, dessa vez pela ABIn, por fazer uso do WhatsApp em aparelho celular sem criptografia. Mais em Junqueira (2016)

[122] Em julho de 2014, a revista do Senado Federal "Em discussão" destinou todo um editorial focado em "espionagem cibernética", detalhando os principais pontos em destaque no relatório final da CPI (Em Discussão, 2014).

Posteriormente, a "Estratégia"[123], proposta pelo Gabinete de Segurança Institucional da Presidência da República, buscou endereçar o planejamento em segurança cibernética para o período 2015-2019 e institucionalizar a gestão pública da área pelo Poder Executivo Federal, incorporando o incentivo à pesquisa e desenvolvimento de modelos criptográficos robustos para a segurança nacional.[124] Porém a iniciativa não resultou de aprovação do Congresso Nacional e tampouco contou com a participação de grupos de trabalho multissetoriais, como com a participação de setores acadêmicos, organizações da sociedade civil ou representações necessárias do setor privado,[125] o que poderia resultar, seria possível dizer, em uma governança insuficiente sobre a cibersegurança no país por não congregar a complexidade de interesses dos atores envolvidos.

No processo de dar forma a uma estratégia nacional de segurança cibernética melhor articulada entre os diversos setores e que sugerisse um modelo regulatório detalhado, em 2018 foi aprovada a Política Nacional de Segurança da Informação - PNSI (Decreto nº 9.637/2018) (Brasil, 2018c). O Decreto cria o Comitê Gestor da Segurança da Informação, assessoria ao Gabinete de Segurança Institucional da Presidência da República - responsável pela execução da política - com composição unicamente governamental, o que terminou por escantear a participação dos demais setores interessados. De toda forma, a importância do uso de criptografia já figurava expressa e reconhecida em seu texto.

A PNSI prepara terreno para a Estratégia Nacional de Segurança Cibernética (E-Ciber), que irá estabelecer algumas diretrizes, como a previsão de ampla participação da sociedade em sua construção e o estabelecimento de módulos que serão objeto de

---

[123] "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal" (Brasil, 2015)

[124] "[S]ão fundamentais a pesquisa e o desenvolvimento de soluções voltadas para a SIC [Segurança da Informação e Comunicações] e a SegCiber [Segurança Cibernética], baseadas em hardware e algoritmos criptográficos proprietários de Estado, com o objetivo de garantir a confidencialidade, integridade e autenticidade das comunicações estratégicas entre órgãos que integrem a APF [Administração Pública Federal]."

[125] Uma crítica feita em publicação patrocinada pela OEA, por exemplo, na "Revisão da Capacidade de cibersegurança no Brasil" (Organização dos Estados Americanos, 2020)

desenvolvimento, entre eles a segurança cibernética, a defesa cibernética e uma postura preventiva contra vazamento de dados. Finalmente, a E-Ciber entra em vigor através do Decreto nº 10.222/2020 (Brasil, 2020), construído com a participação de variados setores da sociedade, incluindo acadêmicos, empresas, pesquisadores e membros do governo, além de ter contado com edital de consulta pública.

Na E-Ciber, ganha ainda mais corpo a importância do uso e desenvolvimento da criptografia pelos mais variados setores governamentais. Dentre as ações destinadas a alcançar o objetivo de seus eixos estratégicos, encontram-se

> [R]ecomendar a adoção de soluções nacionais de criptografia
>
> (...)
>
> [E]stimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis
>
> (...)
> [I]ncentivar o desenvolvimento de competências e de soluções em criptografia
>
> (...)
>
> [U]tilizar criptografia e compartilhar essas práticas com aqueles agentes relacionados no processo da comunicação. Considera-se, ainda, que o uso adequado de recursos criptográficos comprovadamente habilita uma camada de segurança adicional de extrema relevância para atingir os níveis desejados de proteção de dados em repouso ou em trânsito.
>
> (...)
>
> [I]nvestimento na busca de soluções inovadoras em novos tipos de criptografia, de forma a considerar seu potencial variado de aplicabilidade e seu valor estratégico para a segurança da informação e para a segurança cibernética do País

Apesar da E-Ciber ter sido relativamente bem aceita por diferentes setores, incluindo a sociedade civil organizada (Luca, 2020), algumas ressalvas pontuais podem ser feitas em relação à ausência de objetivos concretos e de previsões de investimento governamental para execução das ações planejadas. Ainda que seja possível notar

avanços no estabelecimento de "princípios" e "diretrizes", bem como no amadurecimento da importância da matéria para a segurança da sociedade, das empresas e da própria administração pública, nota-se a burocracia legislativa, de replicação interminável de estratégias, leis, decretos e programas governamentais que delegam a uma política pública posterior o estabelecimento de planos de execução, despesas públicas, cargos, ações consolidadas e demais responsabilidades e prerrogativas administrativas de segurança cibernética para o país[126]. No contrapé, portanto, da aceleração dos processos comunicacionais atuais e das crescentes ameaças à segurança cibernética no país.

Fato é que enquanto todos os setores da sociedade digitalizam, de forma exponencial, multifacetada e interoperável suas atividades, os elementos de segurança passam a agregar complexas peças na composição do espaço informacional nacional e cujo *status* de atualização rapidamente se deteriora. O estabelecimento de políticas que expressam suficiente compreensão dessa realidade constitui uma agenda prioritária para o país, com a criação de corpo institucional que coordene e acompanhe, de forma transparente, dinâmicas domésticas e multissetoriais de segurança da informação, bem como consiga projetar - e se antecipar - à miríade de ameaças tanto por parte de atores maliciosos privados quanto por outros atores públicos. E, como exposto ao longo deste capítulo, a criptografia desempenha função crítica nas engrenagens da cibersegurança.

[126] Até 2019. alguns órgãos se destacavam enquanto responsáveis pela segurança cibernética a nível nacional. Entre eles, a Polícia Federal, a ABIn, e o Centro de Defesa Cibernética (CDCiber), este último vinculado ao Ministério da Defesa e mais atuante na "defesa cibernética". Interessa apontar a diferente conceituação entre "cibersegurança" ou "segurança cibernética" e "defesa cibernética", sendo a primeira associada à meios de prevenção, proteção e garantia de ativos de informação estratégicos, principalmente os relacionados a infraestruturas críticas. Mais sobre essa distinção e sobre o corpo organizacional estatal para esses dois campos, ver Artigo 19 (2016).

7.3 A valorização da criptografia por órgãos multissetoriais consultivos e de recomendações de padrões técnicos.

Do ponto de vista de obrigações legais e limitações técnicas mandatórias, talvez não seja facilmente tecida uma malha regulatória tradicional sobre a criptografia no Brasil - o que levaria, segundo opiniões, a uma escassa eficácia diante da dinâmica e contínua reconstrução tecnológica (Doneda, 2017). Isso por que não há taxatividade restritiva ou propositiva sobre emprego de criptografia tendo em vista um recorte legislativo nacional. No entanto, é possível perceber uma linguagem recomendatória e consultiva, que dialoga melhor com o estabelecimento de boas práticas, a partir de núcleos de governança sobre a criptografia identificados, principalmente, no Comitê Gestor da Internet (CGI.br) e na Infraestrutura de Chaves Públicas (ICP-Brasil).

O CGI.br, criado em paralelo à inserção gradual da Internet comercial no Brasil, em meados de 1995, tem entre, entre outras responsabilidades, a atribuição de "estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil", além de publicar estudos e recomendações procedimentais para a segurança da Internet (Brasil, 2003). É composto de um órgão multissetorial consultivo - um formato resultante de articulações continuamente construídas tendo como ponto de partida as primeiras edições da Cúpula Mundial Sobre a Sociedade da Informação e os Fóruns de Governança da Internet - composto por representantes do poder público, do setor privado, da comunidade técnica ou acadêmica e da sociedade civil, além de uma presidência de notório saber (Comitê Gestor da Internet, 2014).

Durante os mais de vinte anos de atuação do CGI.br, a criptografia foi objeto de discussão e pronunciamentos dados os fatos políticos que tensionaram a resiliência das aplicações de encriptação para o ecossistema de segurança da rede no país, como, por exemplo, as ordens judiciais de bloqueio do WhatsApp, além de figurar como recurso de implementação de rotinas de boas prática em publicações da entidade e em ações pedagógicas de ensino especializado. Por exemplo, a Cartilha de Segurança do CGI.br estabelece a criptografia, incluindo a encriptação de chave pública, enquanto pilar técnico

de recomendações em boas práticas de segurança que incluem a proteção de dados sigilosos, a criptografia de disco, a criação de *backups* e a proteção de comunicações como e-mails, mensagens, transações bancárias ou operações comerciais (Comitê Gestor da Internet, 2017a). Enquanto prática central de ensino do Comitê, as edições da Escola de Governança da Internet incluem transversais temáticas, de bases técnicas e legais, para convergir em temas que vão desde o regime de responsabilidade de intermediários e fundamentos de neutralidade de rede às tecnologias de segurança, privacidade proteção de dados, como a criptografia (Comitê Gestor da Internet, 2017b). Além disso, é possível identificar, ainda que de forma colateral, o estabelecimento de bases éticas, técnicas e legais que se colocam lado a lado com a segurança criptográfica da leitura dos Princípios para a Governança e Uso da Internet no Brasil (Comitê Gestor da Internet, 2009), sobretudo no diz respeito aos padrões de governança democrática e colaborativa; à liberdade, privacidade e direitos humanos; à inovação; à universalidade; à inimputabilidade da rede; à funcionalidade, segurança e estabilidade; à padronização e interoperabilidade; bem como ao ambiente legal e regulatório, o qual deve preservar, mais uma vez, a natureza dinâmica da rede.

No campo da participação na construção de políticas públicas, precedentes judiciais[127] e em pronunciamentos públicos pontuais da entidade, é igualmente possível perceber que a centralidade da manutenção de um ambiente regulatório protetivo à criptografia é com frequência buscado. Já em 2019, o CGI.br contribui para o debate no Brasil que, à época, girava em torno das ações constitucionais no STF, com "Nota Pública sobre o uso de criptografia em sistemas e dispositivos conectados à Internet" (Comitê Gestor da Internet, 2019) para o debate no Brasil que, à época, girava em torno das ações no STF. Na Nota, considera que a criptografia forte é "muito importante para que fluxos de informação se estabeleçam de forma segura e confiável na Internet, não somente para usuários individuais, como também para empresas e órgãos públicos", além do que os fluxos de informação já seriam devidamente regulados em legislação ordinária, passando

[127] Vale notar a participação de Demi Getschko, representante de notório saber do CGI.br, na Audiência Pública convocada no âmbito das ações no STF (Supremo Tribunal Federal, 2017).

pelo Código Civil Brasileiro, pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados Pessoais. Reafirma, conclusivamente, que é necessária a garantia de implementação livre de criptografia ponta-a-ponta, "tanto para a proteção do sigilo de dados e comunicações, como para o exercício de direitos previstos na Constituição Federal e leis infraconstitucionais"; que tais recursos "são fundamentais à integridade e segurança de sistemas digitais, ao sigilo empresarial, bem como à garantia da inimputabilidade da rede e da funcionalidade, segurança e estabilidade da Internet"; para concluir que mecanismos de acesso privilegiado a conteúdos encriptados, além de ineficazes, geram riscos mais amplos ao criar brechas de segurança e contrariam as melhores práticas internacionais de segurança dos usuários e inovação tecnológica.[128]

Por fim, vale mencionar o modelo administrativo de caráter técnico e recomendatório representado pela Infraestrutura de Chaves Públicas, o ICP-Brasil, sistema brasileiro de certificação digital e composto por distintas entidades certificadoras, tendo como "autoridade certificadora raiz" o Instituto Nacional de Tecnologia da Informação (INTI), autarquia federal vinculada à Casa Civil da Presidência da República, além de seguir regulamentações elaboradas por um Comitê Gestor composto por representantes do governo e por representações da sociedade civil (ICP-Brasil, 2017).

O ICP-Brasil, portanto, compõe uma cadeia distribuída de entidades certificadoras que, através de protocolos criptográficos autorizados, proveem métodos de autenticação de identidades, conferindo validade jurídica a serviços e documentos assinados digitalmente. O órgão também regulamenta o estabelecimento de padrões técnicos mínimos no emprego de algoritmos de criptografia, apontando requisitos mínimos como, por exemplo, o tamanho das chaves de encriptação. Essas, por sua vez, levam em consideração o estado da arte no que diz respeito ao poder computacional em seara de criptanálise, especificamente possibilidades de ataques de integridade ou certificação que possam minar a segurança jurídica na certificação de

[128] Além dos documentos acima citados, é válida a busca sobre os inúmeros debates, seminários e mesas redondas promovidos pelo CGI.br em espaços como o Seminário de Privacidade e Proteção de Dados Pessoais, o Internet Governance Forum (IGF) e pelas inúmeras entidades participantes do Fórum da Internet no Brasil, promovido sob os auspícios do CGI. Ver, por exemplo, https://www.youtube.com/user/NICbrvideos.

documentos digitais, como em *smart-contracts*, processos judiciais eletrônicos ou em expedientes cartorários de registro público.

Uma "rede" tecnológica de "confiança administrativa" requer, portanto, que suas informações confiram integridade aos processos burocráticos. E a criptografia é recurso elementar, em termos de recomendações e padronizações de boas práticas para os serviços públicos e privados, para se garantir requisitos mínimos de segurança necessários a essa rede de confiabilidade que envolve estruturas administrativas públicas, agentes privados e sociedade civil.

8 CONSIDERAÇÕES FINAIS: DINAMICIDADE DAS POLÍTICAS DE ENCRIPTAÇÃO E RECURSIVIDADE FUTURA DOS DESVIOS À CRIPTOGRAFIA

Como exposto ao longo deste trabalho, a dinamicidade fractal das disputas regulatórias em torno das políticas de encriptação não permite cristalizar o debate em torno de propostas técnicas - especialmente aquelas provenientes das forças de segurança pública - específicas, localizadas em tempo e espaço determinados. Muito menos os desafios apontam para soluções técnicas estáticas que eventualmente se repetiriam com alguma regularidade, como *backdoors* administrados por provedores de aplicação ou políticas nacionais mandatórias de "depósito" de chaves mediante uma entidade de confiança.

Pelo contrário, há uma recursividade das investidas em favor da flexibilização da encriptação de natureza contextual: motivações sociais e políticas, atores envolvidos, objetos tecnológicos, plataformas de aplicação e diferentes níveis de centralidade de tecnologias na sociedade tornam essas investidas criativamente mutáveis. Isso significa que será necessário, sempre, desenvolver novos - e reafirmar antigos - argumentos se o que se quer é uma interoperabilidade continuamente estável da criptografia forte.

Resgatando elementos da introdução desse trabalho, talvez essa seja uma característica imanente da natureza das políticas informação: uma disputa ontológica sobre as tecnologias que tensionam as relações de poder, como as *privacy enhancing-technologies,* talvez seja inexorável, independente de tempo e espaço em sua recursividade, mas que assume incontáveis identidades. Craig Jarvis (2020), a esse respeito, argumenta que as *cryptowars*, antes de uma disputa localizada na década de 90, como comumente percebido, se caracterizam como um conflito sobre se um cidadão deve ter acesso a técnicas de encriptação, a tecnologias capazes de manter seus segredos além

do alcance do Estado. Abrange, portanto, a noção de guerras criptográficas de forma que *tudo* que diga respeito a conflitos sobre políticas de encriptação se torna uma.

Essa seção, portanto, busca apontar alguns contextos que, a pretexto de desestabilizar o pleno alcance do cidadão à encriptação, se inclinam sobre o presente e, possivelmente, ganharão terreno em um futuro próximo, dando continuidade à recursividade imanente das *cryptowars.* Em certas circunstâncias, essas tendências ainda buscarão endereçar a suspensão do sigilo criptográfico às comunicações; em outras, vão além da qualidade do sigilo, para enfrentar riscos sobre a proteção à integridade dos dados encriptados; e, indo, além, também poderão se deparar com a desestabilização dos algoritmos criptográficos tendo em vista modelos computacionais que, em tese, seriam disruptivos à criptografia moderna.

8.1 Futuro da criptografia para além do sigilo das comunicações

Tudo está se tornando um computador (ou computadores estão se transformando em tudo?). Independente de como a questão é formulada, o presente (e futuro) tecnológico se apresenta através da *datificação* e da computadorização dos ambientes domésticos, urbanos, rurais, públicos, privados, comerciais, sociais e biológicos. A associação tecnológica com o sujeito e meio ambiente circundante, envolvendo objetos e ideias, aprofunda uma relação biopolítica que *sujeita* grupos e indivíduos na *hiperconectividade.*

Não diferente da estrada tecnológica até aqui trilhada, os *jardins bifurcados* que se apresentarão igualmente irão envolver escolhas e estratégias de segurança, onde a encriptação de comunicações - e os recursos criptográficos de modo geral - exercerão função chave para a estabilidade, confiabilidade e resiliência do ecossistema. Aqui, fala-se sobretudo em objetos conectados habilitados por sensores e que destravarão múltiplas camadas de interconectividade, as quais irão gerar novas interações entre

sistemas, padrões e dispositivos que, fundamentalmente, multiplicarão as superfícies de ataque.

Isso significa que o caráter de *virtualidade* classicamente atribuído à Internet vem se aproximando da consequência *material,* pós-moral, através de *chips* e microprocessadores que pisam, gentilmente, nos círculos mais íntimos da experiência do indivíduo com as fabricações técnicas. Logo, a *galáxia da Internet*, como chama Castells (2001), fagocita o particular e gera novos desafios tanto em termos de subjetividades e afetos quanto em termos de segurança da informação e proteção técnica e legal às informações[129]. Isso porque a Internet não foi pensada com a segurança em mente - mas com a interoperabilidade entre redes e praticidade - e essa racionalidade custa, ainda hoje, a "dar o braço a torcer". Por isso, a *cultura* da segurança e da proteção de dados, por exemplo, são desafios estruturais que devem ser enfrentados.

A aproximação da segurança da informação ao corpo, à integridade física e à propriedade - enquanto objetos conectados se multiplicam em nosso campo de visão, entre vestíveis e não vestíveis - vem sendo explorada e ilustrada por uma diversidade de explorações de vulnerabilidades maliciosas (desde televisores, objetos sexuais, geladeiras e uma incontável lista)[130] e por testes de segurança. Schneier (2017) explora as consequências de arquiteturas de segurança mal construídas em três cenários, para lançar um olhar crítico para o futuro dos dispositivos conectados: **(i)** pesquisadores em segurança tomam, a milhas de distância, o controle de um Jeep através de seu sistema de entretenimento, quando o veículo circulação em uma avenida, ligando seu ar-condicionado, trocando a estação de rádio e mesmo as marchas. Nessa esteira, pesquisadores têm declarado poderem fazer o mesmo com aviões domésticos - e o vêm fazendo; **(ii)** hackers vêm detonando armas cibernéticas para desligar subestações de energia, deixando sem abastecimento grandes regiões em diversas localidades do mundo.

---

[129] Acredito ser particularmente interessante essa correlação como forma de *costurar* distintas abordagens críticas, reciprocamente importantes, aos impactos que novas dimensões tecnológicas implicam à sociedade. Sendo assim, redes conectadas são formadas por expressões *tecnossociais* que devem ser abordadas mutidisciplinarmente.

[130] São amplamente documentados os casos de tomada de controle remoto de uma variedade de objetos conectados. Ver, por exemplo, Burgess (2018), Graham (2019); NBC News (2014).

Alguns dos incidentes apontam para origens russas e têm como alvo usinas norte-americanas, o que pode levar à presunção de que a finalidade é política; **(iii)** ataques vêm sendo reportados em impressoras em variadas localidades no mundo - aos milhares de uma só vez inclusive, via distribuição de *worms* - inclusive para imprimir *flyers* com propaganda anti-semita.[131]

Dois fatores, menos discutidos, que dizem respeito à segurança da informação e que passam, transversalmente, pela proteção criptográfica parecem saltar a partir dos cenários ilustrados. Para além do sigilo, claramente violado quando acessível e operáveis os comandos de controle, a *integridade* dos comandos entre usuário e dispositivo merece destaque. O ataque à integridade dos comandos de ar-condicionado ou frequência de rádio poderão perfeitamente ser aplicados aos comandos de retrovisor, "curva", freio ou aceleração, o que geraria um comprometimento crítico da direção e poderia levar à morte do motorista ou de outras pessoas no raio de alcance do veículo. O mesmo, consequentemente, se aplicaria a aviões, metrôs, ônibus, drones e quaisquer outros veículos e meios de transporte conectados. O que presumir de bio-impressoras, produtoras de tecidos nervosos, órgãos humanos, conjuntos celulares complexos cuja aplicação é inerentemente humana?

Da mesma forma, uma falha em recursos de comando também derivariam de ataques à *disponibilidade*, em um cenário em que notificações de *ransomware*, por exemplo, cresceram em cerca de 331% no fechamento de 2020 (Arbulu, 2021). A exploração da expansão de vulnerabilidades em novas superfícies de ataque geradas por dispositivos conectados domésticos, urbanos, vestíveis, industriais, hospitalares, entre outros, poderão tornar indisponíveis, igualmente, os controles sobre um fluxo de medicação intravenosa, procedimentos cirúrgicos operados à distância.

O que esperar de um cenário de mobilidade e planejamento urbano cujas figuras centrais serão os carros autônomos e conectados? A administração municipal irá prever

[131] Dispensa maiores explicações a afirmação de que discursos de ódio violam, não raramente, a integridade física de indivíduos.

padrões e protocolos criptográficos mínimos para o trânsito dos veículos? E, trazendo para o objeto dessa investigação, autoridades de segurança pública e investigação criminal terão a legitimidade de exigir *backdoors* em sistemas de segurança de carros autônomos que porventura sejam usados para o cometimento de crimes? Novas camadas regulatórias deverão ser desenhadas - ou reforçadas - como forma de responder a futuras fricções envolvendo a criptografia.

Por isso à cibersegurança vem sendo adicionada uma valoração legal e política imprescindível: sua proteção no corpo de direitos humanos assegurados internacionalmente. Em Assembleia Geral da ONU, seu então Secretário Geral António Guterres (United Nations, 2017) ressaltou a escalada das ameaças de cibersegurança enquanto contraponto necessário que deve ser feito ao ecossistema de desenvolvimento e inovação tecnológica. Como vem sendo coberto por entidades internacionais como a Human Rights Watch (Brown, 2020) e a Association for Progressive Communications (Esterhuysen, 2019), incidentes de cibersegurança que impliquem em impactos à integridade e à disponibilidade de sistemas, como bloqueios de acesso à Internet - sejam aplicações específicas ou infraestruturas de provimento de acesso - repercutem estruturalmente sobre outros direitos humanos conexos. Some-se ao contexto político atinente à liberdade de expressão a exploração de vulnerabilidades em dispositivos conectados narrada - tanto por parte do Estado, por meio de hacking governamental, como por agentes privados - e se estará diante de uma rede de riscos à proteção integral, interdependente e indivisível dos direitos humanos.

8.2 Desvios (multifacetados) à encriptação

Orin Kerr e Bruce Schneier (2017) catalogam o que chamam de *encryption workarounds* (“desvios à encriptação”, em tradução livre), para propor uma taxonomia das formas através das quais desvios são propostos e operados por entidades policiais e

investigativas ou por agentes maliciosos.[132] É interessante pensar em "desvios" de forma não-rígida, uma vez que as políticas que buscam flexibilizar o acesso à criptografia forte tendem a não se repetir. Por exemplo, as expressões *backdoor* ou *key escrow*, saturadas, assumem novas terminologias que "reiniciam" o debate público a partir de novas bases técnicas, mas que, ao fim do dia, buscam atingir a mesma finalidade: uma acesso dito excepcional ao conteúdo encriptado através de um "desvio". Esta sub-seção procura explorar brevemente algumas das distintas propostas mais notáveis, em políticas públicas contemporâneas, que objetivam esse fim.

- ***Government hacking:*** a exploração de vulnerabilidades, o uso de ataques de força bruta ou malwares como forma de acessar dados e comunicações encriptadas vêm se inscrevendo nas rotinas de autoridades investigativas de forma acelerada. O método é frequentemente acionado quando agências de investigação encontram obstáculos para a produção de provas em dispositivos e serviços que fazem uso de criptografia forte. Algumas empresas frequentemente associadas com o licenciamento de ferramentas de hacking a autoridades policiais são a NSO Group, Cellebrite e Grayshift. Caso notável, por exemplo, é identificado no ínterim na disputa entre FBI e Apple, quando a empresa se resguarda ao direito de não produzir solução técnica que permitiria o desbloqueio do iPhone. A agência busca, então, auxílio da empresa australiana Azymuth Security, logrando acesso ao aparelho (Nakashima; Albergotti, 2021). No Brasil, é possível falar em uma capilaridade bastante disseminada de ferramentas de hacking na cadeia de agências de investigação (Leal, Felix, 2020), recentemente, por exemplo, tendo chamado atenção no desencadeamento do "Caso Henry" (UOL, 2021). O fenômeno, no entanto, parece repousar em um ambiente regulatório pouco delineado, uma vez que não é possível identificar, no panorama legal brasileiro,

[132] Mais precisamente, elencam seis "desvios": **(i)** encontrar a chave **(ii)** descobrir a chave; **(iii) (iii)** obrigar a cessão da chave; **(iv)** explorar uma falha em software de encriptação; **(v)** acessar o purotexto enquanto o dispositivo está em uso; e **(vi)** encontrar uma outra cópia do purotexto.

qualquer regulamentação para o uso de ferramentas de hacking por autoridades brasileiras. Esse cenário é pouco amigável à garantia de direitos fundamentais, uma vez que as precárias balizas para a importação e contratação do serviço, bem como para uso efetivo, abre margem a arbitrariedades que dispensam sua autorização mediante ordens judiciais ou mesmo preveem salvaguardas ao usuário, tendo-se em vista bases do devido processo penal, e às plataformas, que podem sofrer prejuízos econômicos diante de uma erosão de sua reputação em razão de uma possível insegurança em seus serviços. Além do mais, coloca-se diante de dilema ético sobre a exploração de vulnerabilidades, uma vez que a decisão sobre explorá-las ou não pode envolver manter vulnerável determinado sistema para benefício de autoridades policiais,[133] o que, consequentemente, põe em risco a segurança estrutural de sistemas de informação ao mantê-los expostos à exploração maliciosa (Pfefferkorn, 2018).

- ***Client-side scanning:*** dada a resistência política, econômica e tecnológica em se inserir formas de "interceptação" sobre o tráfego de comunicações encriptadas ponta-a-ponta, sobretudo em aplicações de mensageria, chega a ser proposto mecanismo que operaria um *scan* - ou uma filtragem - sobre as mensagens *antes* de serem encriptadas, ou seja, a partir de software adicional que operaria no dispositivo e não através do intermediário (note-se que, normalmente, tecnologia semelhante é utilizada por plataformas que não operam criptografia ponta-a-ponta para averiguar se os dados que estão sendo transmitidos violam direitos autorais ou se figuram como conteúdos de exploração sexual infantil, como o YouTube). Exigem, portanto, que as mensagens recebam um identificador *hash* e, antes de enviadas, sejam conferidas com o auxílio de uma base de dados de conteúdos previamente conhecidos como ilegais. A aplicação, então, suspenderia o envio e,

[133] Seria necessário a construção de mecanismos de regulação específica sobre as práticas de hacking e, de forma geral, sobre a exploração de vulnerabilidades em sistemas informáticos. Os Estados Unidos, por exemplo, contam com o "Vulnerabilities and Equities Process", através do qual realizam um "teste de razoabilidade" sobre a exploração de uma vulnerabilidade nesses sistemas por autoridades estatais, levando em consideração, entre outros fatores, a probabilidade de um ator malicioso ter conhecimento e também explorá-la. Ver Herpig e Schwartz (2019).

adicionalmente, poderia acionar uma autoridade policial. Entidades de defesa de direitos dos usuários apontam para um risco inevitável de que conteúdos "legítimos" sejam rotulados como suspeitos em conjunturas políticas menos democráticas, além de uma possível ineficácia da medida, uma vez que criminosos migrariam para plataformas que não operassem o mecanismo (Internet Society, 2020).

- ***Ghost-user:*** a proposta, originalmente surgida no corpo de agências de investigação britânicas, demandaria que intermediários provessem uma "chave adicional" a autoridades que, a partir de uma atualização do software para um usuário suspeito específico, passaria a estar presente, de forma despercebida, em uma troca de mensagens (Ramiro et al, 2020). Quer dizer, haveria de se interferir nos mecanismos de autenticação para acesso a determinada comunicação através de uma inovação na distribuição de chaves, conferindo autorização a uma parte exterior (*third party*) à comunicação ponta-a-ponta e tornando possível, a grosso modo, um ataque *man-in-the-middle*. Especialistas frisam que o mecanismo não seria, exatamente, distinto de um *backdoor*, uma vez que geraria chave adicional para acesso "excepcional" a conteúdos encriptados, ou seja, apenas "um *backdoor* chamado por outro nome" (Cardozo, 2019).

8.3 Comentários sobre a encriptação forte frente à computação quântica

É desafiador falar sobre o futuro da encriptação e não lançar prognósticos sobre a resiliência dos algoritmos contemporâneos de criptografia diante de um ataque realizado por máquinas de computação quântica.[134] Tendo em vista que esse horizonte de repaginação da criptografia demanda uma bagagem bibliográfica à parte, além de

[134] Um computador convencional processa informação através de operações em *bits*, ou seja, em código binário, *zeros* e *uns.* A grosso modo, um computador quântico opera com base em *qubits*, tipicamente partículas subatômicas, como elétrons e fótons, permitindo um computador processar uma quantidade de informação muito mais elevada se comparadas com a mesma quantidade de *bits*. Ver Giles (2019).

caminhar em uma área científica, em certa medida, especulativa, ainda que premente, trago, portanto, uma revisão muito breve de comentários sobre o tema.

O problema reside, em larga escala, na inédita capacidade que um computador quântico teria de fatorar números primos grandes - algo inviável para que um computador convencional o faça em tempo hábil - o que comprometeria a segurança de algoritmos criptográficos de chave pública, como o RSA e o DSA (Bernstein, 2019). Por essas razões, entidades administradoras de recomendação e padronização de algoritmos criptográficos, a exemplo do National Institute of Standards and Technology (NIST) vêm reunindo grupos de trabalho que proponham novas abordagens matemáticas para algoritmos criptográficos, tornando-os resilientes mesmo diante de um ataque via computador quântico (NIST, 2020). Pela mesma razão, paralelamente, setores de inteligência governamental, como a NSA, também vêm reunindo esforços e conduzindo pesquisas para modernizar sistemas criptográficos que atualmente garantem a segurança de informações sigilosas do Estado (Schneier, 2015).

Portanto, antes de uma "morte da criptografia", como reports alarmistas pretendem fazer parecer, fala-se com segurança em uma "criptografia pós-quântica" (Infante, 2014). Inicialmente, diante de um ataque que opere o "algoritmo de Shor" - o qual oferece maiores chances para que computadores quânticos realizem operações de fatoração de números primos - a solução poderia ser alcançada, com nova resiliência, simplesmente com a adição de novos dígitos ao comprimento da chave, isso quando algoritmos criptográficos pré-existentes, a exemplo de sistemas de assinatura de chave pública baseados em *hash* ou *lattice-based cryptography* - cuja segurança deriva de problemas complexos baseados em aprendizagem de máquina - já não sejam suficientemente eficazes diante de um computador quântico (Bernstein, 2019). Quer dizer, nem todos os modelos criptográficos contemporâneos se tornariam obsoletos de antemão.

Por fim, resta destacar que algoritmos de chave pública ponta-a-ponta, como aqueles percebidos em aplicações de mensagem via Internet, também vem sendo testados

contra eventuais ataques dessa natureza, levando a “encriptação ponta-a-ponta pós quântica” (Tutoveanu, 2021). Resta concluir que, mesmo que haja uma repaginação significativa em padrões criptográficos básicos para a segurança de infraestruturas digitais, a criptografia vem acompanhando as tendências de crescimento exponencial em poder computacional para manter íntegra a confiabilidade dos sistemas conectados.

Para concluir, espera-se que os arcos interpretativos aqui expostos - em que sempre foi buscado a interconexão e diálogo com as disciplinas sociais, políticas e tecnológicas - auxiliem na leitura dos conflitos que desabrocham das engrenagens, das fábricas e laboratórios de novas tecnologias. Entende-se que não são escolhas fáceis - nunca o é -, uma vez que, sim, a encriptação é um fenômeno disruptivo e carrega potências desestabilizadoras, tornando possível tecer sua própria história política. E lança, ao fim e ao cabo, uma luz ofuscante sobre os processos de autonomia informacional e redistribuição de poder que expõe a natureza das políticas da informação típicas de civilizações modernas. Logo, não vai passar despercebida - nunca o foi nem o será - pelas instituições tradicionais e pelos métodos cuja rigidez os impedem de acompanhar a reciprocidade de impactos, a cada minuto revolucionária, entre tecnologia e sociedade.

REFERÊNCIAS

A, Thiago; O, Augusto; S, Allan. **O processo de radicalização e a ameaça terrorista no contexto brasileiro a partir da Operação Hashtag**. Revista Brasileira de Inteligência: Abin, n. 12, dezembro de 2017. Pág. 13. Disponível em https://rbi.enap.gov.br/index.php/RBI/article/view/138/113. Acesso em 23 de março de 2021.

ABELSON et al. **Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications.** Cambridge, 2015. Disponível em https://dspace.mit.edu/handle/1721.1/97690. Acesso em 22 de março de 2021

ABELSON et al. **The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption.** Columbia University Academic Commons, 1997. Págs. 3, 4 e 11. Disponível em https://www.schneier.com/wp-content/uploads/2016/02/paper-key-escrow.pdf. Acesso em 22 de março de 2021.

ABREU, Jacqueline. **Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação.** Revista Brasileira de Políticas Públicas, Vol 7, nº 3, 2017. Págs. 32-35 .

ACCESS NOW. **With shutdowns in major cities to silence protests, India tries to black out democracy.** 2019. Disponível em https://www.accessnow.org/with-shutdowns-in-major-cities-to-silence-protests-india-tries-to-black-out-democracy/. Acesso em 22 de março de 2021.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **CriptoGOV e cGOV.** Agência Brasileira de Inteligência, 2020. Disponível em

https://www.gov.br/abin/pt-br/assuntos/tecnologia/criptogov-e-cgov. Acesso em 22 de março de 2021.

AL-KADIT, Ibrahim A. **Origins of Cryptology: Arab Contributions.** Cryptologia, Taylor & Francis, 2010. Disponível em https://ljk.imag.fr/membres/Bernard.Ycart/mel/hm/AlKadi_cryptology.pdf. Acesso em 22 de março de 2021.

AL-SUWAIYEL, Mohammed I. **Arabic Origins of Cryptography.** King Abdulaziz City for Science and Technology, 2018. Disponível em https://muslimheritage.com/wp-content/uploads/2018/05/cryptology01.pdf. Acesso em 22 de março de 2021.

ALIMONTI. Veridiana. **Criptografia, direitos e a problemática da polarização entre "privacidade individual" e "segurança coletiva".** In: DONEDA, Danilo; Machado, Diego: **A criptografia no direito brasileiro.** Revista dos Tribunais, 2018. Págs 64, 65.

ANDERSON, Tim. **Oppenheimer's Dilemm**a. Stanford University. 2016. Disponível em http://large.stanford.edu/courses/2016/ph241/anderson1/. Acesso em 22 de março de 2021.

AOKI et al. **Law Professors' Letter Opposing Mandatory Key Escrow**. 1997. Disponível em http://osaka.law.miami.edu/~froomkin/lawprof-letter.htm. Acesso em 22 de março de 2021.

ARANHA, Diego et al. **Execução de código arbitrário na urna eletrônica brasileira.** Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais, 2018. Pág 1. Disponível em https://sol.sbc.org.br/index.php/sbseg/article/view/4243. Acesso em 22 de março de 2021.

ARTIGO 19. **Da cibersegurança à ciberguerra: o desenvolvimento de políticas de vigilância no Brasil.** 2016. Disponível em https://artigo19.org/wp-content/blogs.dir/24/files/2016/03/Da-Ciberseguranc%cc%a7a-a%cc%80-Ciberguerra-WEB.pdf. Acesso em 22 de março de 2021.

ARBULU, Rafael. **Ransomware attacks increased 311% in 2020, says Chainalysis.** Olhar Digital, 2021. Disponível em https://olhardigital.com.br/en/2021/02/02/safety/ransomware-attacks-increased-311-in-2020-says-chainalysis/. Acesso em 22 de março de 2021.

AUERBACH, Dan; OPSAHL, Kurt. **Crucial Unanswered Questions about the NSA's BULLRUN Program.** Electronic Frontier Foundation, 2013. Disponível em https://www.eff.org/pt-br/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program. Acesso em 22 de março de 0221.

AUSTRÁLIA. **Five country ministerial 2018.** Home Affairs, 2018. Disponível em https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018. Acesso em 22 de março de 2021.

ÁVILA, Humberto. **Teoria dos Princípios: da definição à aplicação dos princípios jurídicos**. São Paulo: Editora Malheiros, 2019. Págs. 116-125.

BAKER, Stewart; Hintze, Michael. **Government Regulation of Encryption: Domestic & International Developments**. HighTech Industry, 1997. Disponível em http://encryption_policies.tripod.com/us/baker_060100_regulation.htm. Acesso em 22 de março de 2021.

BARROS, Paula Pécora. **ADPF 403 no STF: Bloqueios do WhatsApp são constitucionais?** Bloqueios.info, InternetLab, 2016. Disponível em http://bloqueios.info/pt/adpf-403-no-stf-bloqueios-do-whatsapp-sao-constitucionais/. Acesso em 22 de março de 2021.

BBC NEWS. **Christchurch shooting: Gunman Tarrant wanted to kill 'as many as possible'.** 2020. Disponível em https://www.bbc.com/news/world-asia-53861456. Acesso em 22 de março de 2021.

BENNETT, Colin. **The Privacy Advocates: resisting the spread of surveillance**. The MIT Press, 2008. Pág 27.

BENSON, Lou. **Civil War communications and Cryptology.** National Cryptologic Museum Foundation, 2011. Pág 5. Disponível em https://cryptologicfoundation.org/file_download/inline/8929ca54-6497-48de-a1ea-d78b352b7151. Acesso em 22 de março de 2021.

BERNSTEIN, Daniel J. **Introduction to post-quantum cryptography.** Post-Quantum Cryptography, 2019. Disponível em http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf. Acesso em 22 de março de 2021.

BLAZE, Matt et al. **Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists.** 1996. Págs 1-10. Disponível em https://www.schneier.com/wp-content/uploads/2016/02/paper-keylength.pdf . Acesso em 22 de março de 2021.

BLOQUEIOS.INFO. **Caso WhatsApp IV: descumprimento de ordem judicial de entrega de dados.** InternetLab, 2016. Disponível em http://bloqueios.info/pt/casos/bloqueio-por-descumprimento-de-ordem-judicial-de-entrega-de-dados-2/. Acesso em 22 de março de 2021.

BLUEKRYPT. **NIST Report on Cryptographic Key Lenght Recommendation.** BlueKrypt, 2021. Disponível em https://www.keylength.com/en/4/. Acesso em 22 de março de 2021.

BONEH, Dan; SHOUP; Victor. **Graduate Course in Applied Cryptography**. Trabalho em desenvolvimento, 2020. Pág 413. Disponível em http://toc.cryptobook.us/book.pdf. Acesso em 22 de março de 2021.

BOK, Sissela. **Secrets: on the ethics of concealment and revelation**. Vintage Books. 1983. Pág. 14.

BORGES, Laryssa. **STF anula grampo entre Lula e Dilma e envia para Sergio Moro investigações contra ex-presidente.** Revista Veja, 2016. Disponível em https://veja.abril.com.br/politica/stf-anula-grampo-entre-lula-e-dilma-e-envia-para-sergio-moroinvestigacoes-contra-ex-presidente/. Acesso em 22 de março de 2021.

BORN, Max et al. **The Russell-Einstein Manifesto.** Student Pugwash Michigan, 1955. Disponível em http://umich.edu/~pugwash/Manifesto.html. Acesso em 22 de março de 2021.

BRASIL. **Decreto nº 1.0222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética.** Brasília, 2020. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em 22 de março de 2021.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008.** Brasília, 2008. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em 22 de março de 2021.

BRASIL. **Decreto Nº 4.829, de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências.** Brasília, 2003. Disponível em https://cgi.br/pagina/decretos/108/. Acesso em 22 de março de 2021.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação.** Brasília, 2018c. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em 22 de março de 2021.

BRASIL. **Estratégia Brasileira para Transformação Digital (E-Digital).** Ministério de Ciência, Tecnologia, Inovação e Comunicações, 2018b.

BRASIL. **Estratégia Nacional de Ciência, Tecnologia e Inovação.** Ministério de Ciência, Tecnologia, Inovação e Comunicações, 2016c. Pág 106. Disponível em http://www.finep.gov.br/images/a-finep/Politica/16_03_2018_Estrategia_Nacional_de_Ciencia_Tecnologia_e_Inovacao_2016_2022.pdf. Acesso em 22 de março de 2021.

BRASIL. **Portaria nº 14 de 11 de maio de 2015. Homologa a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal.** Presidência da República, 2015. Disponível em https://www.gov.br/gsi/pt-br/assuntos/noticias/2015/estrategia-de-seguranca-da-informacao-e-comunicacoes-sic-e-de-seguranca-cibernetica-da-administracao-publica-federal-apf. Acesso em 22 de março de 2021.

BRASIL. **Projeto de Lei nº 2.418/2019. Acrescenta os parágrafos 5° e 6º ao art. 10 da Lei nº 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de internet para fins de persecução criminal, nos casos que especifica.** Câmara dos Deputados, 2019a. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=480F6FBE4DCDBAA2C5B4467427A384DA.proposicoesWebExterno1?codteor=1649230&filename=Tramitacao-PL+6960/2017. Acesso em 22 de março de 2021.

BRASIL. **Projeto de Lei nº 9.808/2018. Acrescenta os parágrafos 5° e 6º ao art. 10 da Lei nº 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de internet para fins de persecução criminal, nos casos que especifica.** Câmara dos Deputados, 2018a. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=480F6FBE4DCDBAA2C5B4467427A384DA.proposicoesWebExterno1?codteor=1649230&filename=Tramitacao-PL+6960/2017. Acesso em 22 de março de 2021.

BRASIL. **Senado Federal. CPI da Espionagem. Relatório Final.** 2013. Disponível em https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferrac o. Acesso em 22 de março de 2021.

BRASIL. **Supremo Tribunal Federal. Ação de Descumprimento de Preceitos Fundamentais (ADPF) nº 403, Min. Rel. Edson Fachin, julgamento 27 de maio de 2020.** 2016a. Disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=591026689. Acesso em 22 de março de 2021.

BRASIL. **Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 5527, Min. Rel. Rosa Weber, julgamento 27 de maio de 2020.** 2016b. Disponível em

http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4983282. Acesso em 22 de março de 2021.

BRASIL. **Lei nº 9.296 (Lei de Interceptações) de 24 de julho de 1996.** Brasília, 1996. Disponível em http://www.planalto.gov.br/ccivil_03/leis/l9296.htm#:~:text=seu%20representante%20legal.-,Art.,objetivos%20n%C3%A3o%20autorizados%20em%20lei. Acesso em 22 de março de 2021.

BRASIL. **Simpósio Going Dark termina com declaração de 13 países.** Ministério da Justiça, 2019b. Disponível em https://www.justica.gov.br/news/collective-nitf-content-1550010028.2. Acesso em 22 de março de 2019.

BRITANNICA. **History of Cryptology.** Britannica, 2021. Disponível em https://www.britannica.com/topic/cryptology/Developments-during-World-Wars-I-and-II. Acesso em 22 de março de 2021.

BROEMELING, Lyle. **An Account of Early Statistical Inference in Arab Cryptology.** The American Statistician, Vol 65, 2011. Disponível em https://www.tandfonline.com/doi/abs/10.1198/tas.2011.10191. Acesso em 22 de março de 2021.

BROWN, Deborah. **It's Time to Treat Cybersecurity as a Human Rights Issue.** Human Rights Watch, 2020. Disponível em https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue. Acesso em 22 de março de 2021.

BRUNO, Fernanda. **Máquinas de ser, modos de ver: vigilância, tecnologia e sociedade.** Editora Sulina, 2013.

BURGESS, Matt. **Smart dildos and vibrators keep getting hacked – but Tor could be the answer to safer connected sex.** Wired, 2018. Disponível em https://www.wired.co.uk/article/sex-toy-bluetooth-hacks-security-fix. Acesso em 22 de março de 2021.

CANTO, Mariana; RAMIRO, André; REAL, Paula Corte. **Criptografia no STF: o que dizem os votos de Rosa Weber e Edson Fachin.** Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). 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 22 de março de 2021.

CAPUTO, Victor. **Bloqueio no Brasil tira WhatsApp do ar na Argentina e Chile.** Revista Exame, 2015. Disponível em https://exame.com/tecnologia/bloqueio-no-brasil-tira-whatsapp-do-ar-na-argentina-e-chile/. Acesso em 22 de março de 2021.

CARDOZO, Nate. **A Goden Age of Surveillance.** KCRW, 2018. Disponível em https://www.kcrw.com/culture/shows/scheer-intelligence/nate-cardozo-a-golden-age-of-surveillance. Acesso em 22 de março de 2021.

CADROZO, Nate. **Give up the ghost key: a backdoor by another name.** Just Security, 2019. Disponível em https://www.justsecurity.org/62114/give-ghost-backdoor/. Acesso em 22 de março de 2021.

CARNEIRO, Lucianne et al. **WhatsApp recorre de bloqueio judicial que afeta 100 milhões de usuários.** O Globo, 2016. Disponível em

https://oglobo.globo.com/economia/whatsapp-recorre-de-bloqueio-judicial-que-afeta-100-milhoes-de-usuarios-19211225. Acesso em 22 de março de 2021.

CASTELLS, Manuel. **Galáxia da Internet.** Oxford University Press, 2001.

CHAUM, David. **Security without identification: transaction systems to make big brother obsolete.** Communications of the ACM, 1985. Disponível em https://dl.acm.org/doi/10.1145/4372.4373. Acesso em 22 de março de 2021.

CHATTOPADHYAY, Anupam; LAM, Kwok-Yan. **Autonomous Vehicle: Security by Design.** School of Computer Science and Engineering, Nanyang Technological University, Singapore, 2018. Disponível em https://arxiv.org/pdf/1810.00545.pdf. Acesso em 22 de março de 2021.

COHEN, Julie. **What Privacy is for.** Harvard Law Review, Vol. 126, 2013. In: BRASIL. **Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 5527, Min. Rel. Rosa Weber, julgamento 27 de maio de 2020.** 2016b. Disponível em http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4983282. Acesso em 22 de março de 2021

COHN, Cindy. **Nine epic failures of regulating cryptography.** Electronic Frontier Foundation, 2014. Disponível em https://www.eff.org/pt-br/deeplinks/2014/09/nine-epic-failures-regulating-cryptography. Acesso em 22 de março de 2021.

COMEY, James. **Addressing the Cyber Security Threat.** Federal Beaureau of Investigation. International Conference on Cyber Security, Fordham University, 2015. Disponível em https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat. Acesso em 22 de março de 2021

COMEY, James; **Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?** Brookings Institution, 2014. Disponível em https://www.fbi.gov/news/speeches/going-dark-aretechnology-privacy-and-public-safety-on-a-collision-course. Acesso em 23 de março de 2021.

COMEY, James. **Privacy, Public Safety, and Security: How We Can Confront the Cyber Threat Together.** Federal Bureau of Investigation. International Conference on Cyber Engagement, Georgetown University, 2016a. Disponível em https://www.fbi.gov/news/speeches/privacy-publicsafety-and-security-how-we-can-confront-the-cyber-threat-together. Acesso em 22 de março de 2021

COMEY, James. **Expectations of Privacy: Balancing Liberty, Security, and Public Safety.** Federal Bureau of Investigation. Center for the Study of American Democracy Biennial Conference, Kenyon College, 2016b. Disponível em https://www.fbi.gov/news/speeches/expectations-of-privacybalancing-liberty-security-and-public-safety.Acesso em 22 de março de 2021

COMEY, James. **The FBI and Cyber Crime: New Perspectives, New Partnerships, and New Ways of Doing Business**. Federal Bureau of Investigation. Intelligence and National Security Alliance (INSA) Leadership Dinner, 2017. Disponível em https://www.fbi.gov/news/speeches/the-fbi-andcyber-crime-new-perspectives-new-partnerships-and-new-ways-of-doing-business-. Acesso em 22 de março de 2021.

COMITÊ GESTOR DA INTERNET. **Cartilha de Segurança: criptografia.** 2017a. Disponível em https://cartilha.cert.br/criptografia/. Acesso em 22 de março de 2021.

COMITÊ GESTOR DA INTERNET. **Brasília recebe curso da Escola de Governança da Internet voltado aos profissionais da área jurídica**. 2017b. Disponível em

https://www.cgi.br/noticia/releases/brasilia-recebe-curso-da-escola-de-governanca-da-internet-voltado-aos-profissionais-da-area-juridica/. Acesso em 22 de março de 2021.

COMITÊ GESTOR DA INTERNET. **Governança multissetorial e pluriparticipativa da Internet no Brasil.** 2014. Disponível em https://cgi.br/noticia/cgi-br-governanca-multissetorial-e-pluriparticipativa-da-internet-no-brasil/10062. Acesso em 22 de março de 2021.

COMITÊ GESTOR DA INTERNET. **Nota Pública sobre o uso de criptografia em sistemas e dispositivos conectados à Internet.** 2009. Disponível em https://www.cgi.br/esclarecimentos/ver/nota-publica-sobre-o-uso-de-criptografia-em-sistemas-e-dispositivos-conectados-a-internet.pdf. Acesso em 22 de março de 2021.

COMITÊ GESTOR DA INTERNET. **Resolução CGI.br/RES/2009/003/P. Princípios para a Governança e Uso da Internet no Brasil.** 2009. Disponível em https://www.cgi.br/resolucoes/documento/2009/003/. Acesso em 22 de março de 2021.

COMITÊ GESTOR DA INTERNET. **TIC Kids Online 2019.** Centros Regional de Estudos para o Desenvolvimento da Sociedade da Informação - CETIC.br. Pág 82. Disponível em https://cetic.br/media/docs/publicacoes/2/20201123093344/tic_kids_online_2019_livro_eletronico.pdf. Acesso em 22 de março de 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Caso Escher e outros vs. Brasil.** Corte Interamericana de Direitos Humanos, 2009. Disponível em https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em 22 de março de 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Revisão da capacidade de Cibersegurança no Brasil.** 2020. Pág 13. Disponível em https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf. Acesso em 22 de março de 2021.

CRYPTO MUSEUM. **History of the Enigma: the rotor-based cipher machines.** Crypto Museum, 2021. Disponível em https://www.cryptomuseum.com/crypto/enigma/hist.htm. Acesso em 22 de março de 2021.

DAM, Kenneth W.; LIN, Herbert S. **Cryptography's Role in Securing the Information Society.** National Research Council, National Academy Press, 1996. Pág 215, 300.

DANBLON, Emmanuelle. **Crises in Rhetoric, Crises in Democracy.** Questions de Communication nº 12. Press Universitaires de Lorraine, 2007. Págs 2-10.

DATA PRIVACY BRASIL. **Rastreabilidade, metadados e direitos fundamentais.** 2020. Pág 20. Disponível em https://www.dataprivacybr.org/wp-content/uploads/2020/07/Data-Privacy-Brasil.-Rastreabilidade-e-Direitos-Fundamentais.-PL-2630.2020.pdf. Acesso em 22 de março de 2021.

DIFFIE, Whitfeld; HELMAN, Martin. **New directions on Cryptography.** IEEE Transactions on Information Theory, 1976. Disponível em https://ee.stanford.edu/~hellman/publications/24.pdf. Acesso em 22 de março de 2021.

DIFFIE, Whitfield; LANDAU, Susan, **The export of cryptography in the 20th century and the 21st.** Sun Microsystems, 2001. Págs, 9,

DENARDIS, Laura. **The Global War for Internet Governance**. Yale University Press, 2014. Pág 23

DOCTOROW, Cory. **NERD HARDER! FBI Director reiterates faith-based belief in working crypto that he can break.** Boing Boing, 2018. Disponível em https://boingboing.net/2018/01/12/imaginary-numbers.html. Acesso em 15 de dezembro de 2019.

DONEDA, Danilo. **A regulação da criptografia e o bloqueio do WhatsApp.** Conjur, 2017. Disponível em https://www.conjur.com.br/2017-mai-30/danilo-doneda-regulacao-criptografia-bloqueio-whatsapp. Acesso em 22 de março de 2021.

DONEDA, Danilo. **O direito fundamental à proteção de dados pessoais.** In: MARTINS, Guilherme (coord.). **Direito privado e Internet.** Atlas, 2014. Pág 77-78.

ELECTRONIC FRONTIER FOUNDATION. **Bernstein vs. US Department of Justice.** 2021. Disponível em https://www.eff.org/pt-br/cases/bernstein-v-us-dept-justice?page=1. Acesso em 22 de março de 2021.

ELECTRONIC FRONTIER FOUNDATION. **EFF Analysis of Vice-President Gore's Letter on Cryptography Policy.** EFFector, 1994. Disponível em https://www.eff.org/effector/7/12. Acesso em 22 de março de 2021.

ELMER-DEWITT, Philip. **Who Sould Keep the Keys?** TIMES Magazine, 2001. Disponível em http://content.time.com/time/magazine/article/0,9171,164002,00.html. Acesso em 22 de março de 2021.

EM DISCUSSÂO. **Espionagem Cibernética: rede vulnerável.** Senado Federal, 2014. Disponível em https://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/@@images/arquivo_pdf/. Acesso em 22 de março de 2021.

ESTADÃO. **Abin cria sistemas de criptografia para proteger dados do governo.** 2013. Disponível em https://outline.com/e46R3U. Acesso em 22 de março de 2021.

ESTADOS UNIDOS. **Five Country Ministerial 2017: Joint Communiqué.** Homeland Security, 2017. Disponível em https://www.dhs.gov/news/2017/06/28/five-country-ministerial-2017-joint-communiqu. Acesso em 22 de março de 2021.

ESTERHUYSEN. Anriette. **Why cybersecurity is a human rights issue, and it is time to start treating it like one.** 2019. Disponível em https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one. Acesso em 22 de março de 2021.

EUROPEAN COMMISSION. **Technical solutions to detect child sexual abuse in end-to-end encrypted communications.** 2020. Disponível em https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf. Acesso em 22 de março de 2021.

EUROPEAN COMMISSION. **What does data protection 'by design' and 'by default' mean?** European Commission, 2021. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. Acesso em 22 de março de 2021.

EVANGELISTA, Rafael. **Para além das máquinas de adorável graça: cultura hacker, cibernética e democracia.** Edições SESC, 2018. Págs 59-71

FEBRABAN. **Pesquisa FEBRABAN de tecnologias bancárias 2020.** Federação Brasileira de Bancos, 2020. Disponível em https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%202020%20VF.pdf. Acesso em 22 de março de 2021. Pág 5.

FERRAZ JR. Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Revista da Faculdade de Direito, USP, Vol. 88. Págs. 447-448. Disponível em https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em 22 de março de 2012.

G1. **Dupla ataca escola em Suzano, mata oito pessoas e se suicida.** 2019. Disponível em https://g1.globo.com/sp/mogi-das-cruzes-suzano/noticia/2019/03/13/tiros-deixam-feridos-em-escola-de-suzano.ghtml. Acesso em 22 de março de 2021.

G7**. Combating the use of the Internet for terrorists and violent extremist purposes**. G7 France, 2019. Disponível em http://www.g7.utoronto.ca/justice/2019-internet.pdf. Acesso em 22 de março de 2021.

GETSCHKO, Demi. **VII Seminário de Privacidade e Proteção de Dados Pessoais.** Comitê Gestor da Internet no Brasil. Disponível em https://www.youtube.com/watch?v=iqkTwt55HPs&t=4376s&ab_channel=NICbrvideos. Acesso em 22 de março de 2021.

FGV DIREITO SP. **CryptoMap.** Faculdade Getúlio Vargas - Direito. São Paulo, 2021. Disponível em http://www.fgv.br/direitosp/cryptomap/#home. Acesso em 22 de março de 2021.

GILES, Martin. **Explainer: what is a quantum computer?** MIT Technology Review, 2019. Disponível em https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/. Acesso em 22 de março de 2021.

GILL, Lex. **Law, Metaphor, and the Encrypted Machine**. Osgoode Hall Law Journal, 2018. Pág 446. Disponível em https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=3290&context=ohlj. Acesso em 22 de março de 2021.

GAGLIARDUCCI, Stefano et al. **War of the Waves: Radio and Resistance During World War II**. American Economic Journal, Vol 12, 2020. Págs 1-38. Disponível em https://www.aeaweb.org/articles?id=10.1257/app.20190410. Acesso em 22 de março de 2021.

GARFINKEL, Simon. **NSA allows encryption.** Simson.net, 1992. Disponível em https://simson.net/ref/NeXT/nextworld/NextWorld_Extra/92.09.Sept.NWE/92.09.Sept.NWExtra11.html. Acesso em 22 de março de 2021.

GLOBAL PARTNERS DIGITAL. **Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders.** Global Partners Digital, 2017. Pág 38. Disponível em https://www.gp-digital.org/wp-content/uploads/2017/09/TRAVELGUIDETOENCRYPTIONPOLICY.pdf. Acesso em 22 de março de 2021.

GLOBAL PARTNERS DIGITAL. **World map of encryption laws and policies.** Global Partners Digital, 2021. Disponível em https://www.gp-digital.org/world-map-of-encryption/. Acesso em 22 de março de 2021.

GOFFMAN, Ervin. **Framing analysis: an essay on the organization of experience.** Northeastern University Press, 1986.

GRAHAM, Jefferson. **FBI Agrees: your smart TV could be hacked.** USA Today, 2019. Disponível em https://www.usatoday.com/story/tech/2019/12/04/fbi-agrees-your-smart-tv-could-hacked-update-password-now/2610134001/. Acesso em 22 de março de 2021.

GREENBERG, Andy. **This machine kills secrets: how WikiLeakers, cypherpunks, and hacktivists aim to free the world's information.** Dutton, 2012. Pág. 80.

GREENWALD, Glenn. **No Place to Hide**. Metropolitan Books, 2014.

GRIMMET, Jeanne J. **Encryption Export Controls.** Congressional Research Services, 2001. Pág 8. Disponível em https://fas.org/irp/crs/RL30273.pdf. Acesso em 22 de março de 2021.

HAGEMANN, Ryan; HAMPSON, Josh. **Encryption, Trust, and the Online Economy.** Niskanen Center, 2015, Pág 3.

HART, C. W. **J. Robert Oppenheimer: A Faith Development Portrait. Springer,** Blanton-Peale Institute, 2007. Pág. 124.

HERPIG, Sven; SCHWARTZ, Ari. **The Future of Vulnerabilities Equities Processes Around the World.** Lawfare, 2019. Disponível em

https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world. Acesso em 22 de março de 2021.

HIJYIA, James. **The Gita of J. Robert Oppenheimer.** PROCEEDINGS OF THE AMERICAN PHILOSOPHICAL SOCIETY, Vol. 144, Nº. 2. Pág 128.

HOLLER, Manfred. **The Zimmermann Telegram: How to Make Use of Secrets?** Homo Oeconomicus, nº 26, 2009. Págs 23-39. Disponível em https://www.researchgate.net/publication/303083858_The_Zimmermann_Telegram_How_to_Make_Use_of_Secrets. Acesso em 22 de março de 2021.

HOMELAND SECURITY TODAY. **U.S. Government to Spend Over $18 Billion on Cybersecurity.** 2020. Disponível em https://www.hstoday.us/subject-matter-areas/cybersecurity/u-s-government-to-spend-over-18-billion-on-cybersecurity/#:~:text=According%20to%20an%20Atlas%20VPN,for%20cybersecurity%20spending%20in%202021. Acesso em 22 de março de 2021.

HUGHES, Eric. **A Cypherpunk's Manifesto.** 1993. Disponível em: https://www.activism.net/cypherpunk/manifesto.html. Acesso em 22 de março de 2019.

ICP-BRASIL. **Padrões e Algoritmos Criptográficos da ICP-Brasil.** Infraestrutura de Chaves Públicas, 2019. Págs 7-11. Disponível em https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-01-01-v-4-2-padroes-e-algoritmos-criptograficos-da-icp-brasil-copy-pdf. Acesso de 22 de março de 2021.

ICP-BRASIL. **Sobre.** Infraestrutura da Chaves Públicas, 2017. Disponível em https://www.gov.br/iti/pt-br/assuntos/icp-brasil. Acesso em 22 de março de 2021.

IDEC. **Idec defende banda larga como serviço essencial e outras mudanças nos serviços de telecomunicações.** Instituto Brasileiro de Defesa do Consumidor, 2016. Disponível em https://idec.org.br/em-acao/em-foco/idec-defende-banda-larga-como-servico-essencial-e-outras-mudancas-nos-servicos-de-telecomunicaces. Acesso de 22 de março de 2021.

ÍNDIA. **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules.** Ministry of Electronics and Information Technology, 2021. Págs. 19 e seguintes. Disponível em http://egazette.nic.in/WriteReadData/2021/225464.pdf. Acesso em 22 de março de 2021.

INÊS, Isabela. **Criptografia é segurança para crianças e adolescentes, não está claro?** Onservatório da Criptografia, 2021. Disponível em https://obcrypto.org.br/#/post/criptografia-e-seguranca-para-criancas-e-adolescentes-nao-esta-claro. Acesso em 22 de março de 2021.

INFANTE, Andre. **Quantum Computers: The End of Cryptography?** Make use Of, 2014. https://www.makeuseof.com/tag/quantum-computers-end-cryptography/. Acesso em 22 de março de 2021.

INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE - IP.rec. **Democracia, disputa de narrativas e conflitos de segurança: entrevista com Riana Pfefferkorn.** Outubro de 2020. Pág 2. Disponível em https://ip.rec.br/wp-content/uploads/2020/10/Democracia-disputa-de-narrativas-e-conflitos-de-seguranca-nas-politicas-de-criptogarfia-Entrevista-com-Riana-Pfefferkorn-IP.rec_-1.pdf. Acesso em 13 de março de 2021.

INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE; CODING RIGHTS. **Nota Técnica sobre o artigo 10 do Projeto de Lei n. 2630/2020 -**

Rastreabilidade de Aplicativos de Mensageria Privada. 2020. Disponível em https://ip.rec.br/2020/05/14/nota-tecnica-sobre-pl-1429-2020-e-pls-1358-2020-que-institu em-a-lei-brasileira-de-liberdade-responsabilidade-e-transparencia-na-internet/. Acesso em 22 de março de 2021.

INTERNET SOCIETY. **Paths to our Digital Future.** 2017. Pág 38. Disponível em https://future.internetsociety.org/2017/wp-content/uploads/sites/3/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf. Acesso em 22 de março de 2021.

INTERNET SOCIETY. **A policy framework for an open and trusted Internet.** Internet Society, 2016. Pág 6. Disponível em https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/. Acesso em 23 de março de 2021.

INTERNET SOCIETY. **Client-side scanning: What it is and why it threatens trustworthy, private communications.** 2020. Disponível em https://www.internetsociety.org/wp-content/uploads/2020/04/Client-side-Scanning-Fact-Sheet-EN.pdf. Acesso em 22 de março de 2021.

INTENETLAB. **Rastrear o Viral? Riscos à privacidade no Projeto de Lei de "Combate às Fake News".** 2020. Pág 6-8. Disponível em https://www.internetlab.org.br/wp-content/uploads/2020/08/rastrear-o-viral_internetlab.pdf. Acesso em 22 de março de 2021.

IORDANOU, Ioanna. **The Professionalization of Cryptology in Sixteenth-Century Venice.** Enterprise and Society, Vol 19. Pág 1-35. Disponível em https://www.researchgate.net/publication/327847251_The_Professionalization_of_Cryptology_in_Sixteenth-Century_Venice. Acesso em 22 de março de 2021.

JARVIS. Craig. **Cryptowars: the fight for privacy in the digital age: a Political History of Digital Encryption.** CRC Press, 2020.

JASANOFF, Sheila. **Future Imperfect: Science, Technology, and the Imagination of Modernity. In Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power**. University of Chicago Press, 2015.

JUNQUEIRA, Daniel. **Dilma devia saber que era para usar criptografia em comunicações, lembra Snowden.** Gizmodo, 2016. Disponível em https://gizmodo.uol.com.br/dilma-devia-saber-que-era-para-usar-criptografia-em-comunicacoes-lembra-snowden/. Acesso em 22 de março de 2021.

KAHN, David. **The Codebreakers: the comprehensive history of secret communications from Ancient Times to the Internet.** Scribner Book Company, 1973. Págs,

KEHL, Danielle; WILSON, Andi; BANKSTON, Kevin. **Doomed to Repeat History? Lessons from the Crypto Wars of the 1990**. Open Technology Institute, New America Foundation, 2015. Pág 10.

KERR, Orin; SCHNEIER, Bruce. **Encryption Workarouds.** 106 Georgetown Law Journal 989, 2017. Pág. 3.

KLEINWÄCHTER, Wolfgang; ALMEIDA, Virgílio. **The Internet Governance Ecossystem.** IEEE Internet Computing, v. 19, n. 2, 2015. Págs. 64-67.

KURBALIJA, Jovan. U**ma Introdução à Governança da Internet.** Comitê Gestor da Internet, 6ª ed., 2015, pág 203

LAKOFF, George; JOHSEN, Mark. Metaphors we live by. The University of Chicago Press, 2003. Disponível em http://shu.bg/tadmin/upload/storage/161.pdf. Acesso em 22 de março de 2021. Págs 156-157.

LANDAU, Susan. **The Five Eyes Statement Encryption: things are seldom what they seem.** Lawfare, 2018. Disponível em: https://www.lawfareblog.com/five-eyes-statement-encryption-things-areseldom-what-they-seem. Acesso em 15 de dezembro de 2019

LEAL, Davi; FELIX, Yuri. **O mercado de dados: o caso cellebrite e a investigação digital no Brasil.** Instituto Brasileiro de Ciências Criminais (IBCCRIM), 2020. Disponível em https://www.ibccrim.org.br/noticias/exibir/160. Acesso em 22 de março de 2021.

LEAL, Felipe Alcântara de Barros (Polícia Federal do Brasil). In: SUPREMO TRIBUNAL FEDERAL. **Audiência Pública sobre as Ação Direta de Inconstitucionalidade nº 5.527 e Ação de Descumprimento de Preceito Fundamental nº 403.** Supremo Tribunal Federal. Brasília, 2018. Disponível em http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 15 de dezembro de 2019.

LEFEVRE, Flávia. **O STF, a Internet a as Telecomunicações.** Flávia Lefevre: direito e telecomunicações no Brasil (Blog), 2017. Disponível em https://flavialefevre.com.br/pt/blog/o-stf-a-internet-a-as-telecomunicacoes. Acesso em 22 de março de 2021.

LEMOS, Ronaldo; Souza, Carlos Affonso. **Marco Civil: construção e aplicação.** Editar, 2016. Pág 6, 7 e 17.

LÉVY, Pierre (1999). **Cibercultura**. Editora 34, 2010.

LEVY, Steven. **Crypto: how the code rebels beat the Government, saving privacy in the digital age**. Penguin Books, 2002. Pág 10, 246 e 263

LEVY, Steven. **The Cypherpunks vs. Uncle Sam.** In: HOFFMAN, Lance. **Building in Big Brother: The Cryptographic Policy Debate.** Institute for Computer and Telecommunications Systems Policy and Department of Electrical Engineering and Computer Science, 1995. Págs 266-283.

LOUIS, James A; ZHENG, Denise E; CARTER, William A. **The effect of encryption on lawful access to communications and data.** Center for Strategic and International Studies, 2017. Pág 14-15. Disponível em https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data. Acesso em 22 de março de 2021.

LUCA, Cristina de. **Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética.** Porta 23, UOL, 2020. Disponível em https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/. Acesso em 22 de março de 2021.

MAASS, Peter. **The Philosopher of Surveillance.** The Intercept, 2015. Disponível em https://theintercept.com/2015/08/11/surveillance-philosopher-nsa/. Acesso em 22 de março de 2021.

MAFEI, Rafael. **Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de troca de mensagem.** In: DONEDA, Danilo; Machado,

Diego: **A criptografia no direito brasileiro.** Revista dos Tribunais, 2018. Págs 35-47

.

MAFEI, Rafael; PONCE, Paula. **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.** Revista Internet e Sociedade, InternetLab, 2020. Págs. 65-90

MARÉS, Chico; BECKER, Clara. **O (in)acreditável mundo do WhatsApp.** Revista Piauí, 2018. Disponível em https://piaui.folha.uol.com.br/lupa/2018/10/17/whatsapp-lupa-usp-ufmg-imagens/. Disponível em 22 de março de 2021.

MAY, Timothy. **The CYPHERNOMICON.** 1994. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ. Acesso em 22 de março de 2021.

MAY, Timothy. **The Coming Police State.** The Cypherpunk's Mailing List, 1994. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-police-state.txt. Disponível em 22 de março de 2021.

MAY, Timothy. **The Crypto Anarchist Manifesto.** 1988. Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html. Acesso em 22 de março de 2012.

MCCONNELL, Mike; CHERTOFF, Michael; LYNN, William. **Why the fear over ubiquitous data encryption is overblown.** Washington Post, 2015. Disponível em https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-dataencryption/2015/

07/28/3d145952-324e-11e5-8353-1215475949f4_story.html. Acesso em 22 de março de 2021.

MONSEES, Linda. **Crypto-Politics: Encryption and Democratic Practices in the Digital Era.** Routledge, 2020. Pág 18.

MOODY, Glym. **Paris terrorists used burner phones, not encryption, to evade detection.** ArsTechnica, 2016. Disponível em https://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/. Acesso em 22 de março de 2021.

MORAES, Alexandre. **Curso de Direito Constitucional.** Editora Atlas, 2003, Pág 65 e 68. Disponível em https://jornalistaslivres.org/wp-content/uploads/2017/02/DIREITO_CONSTITUCIONAL-1.pdf. Acesso em 22 de março de 2021.

NAKASHIMA, Ellen; ALBERGOTTI, Reed. **The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm.** The Washington Post, 2021. Disponível em https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/. Acesso em 06 de junho de 2021.

NARAYANAN, Arvind. **What Happened to the Crypto Dream?, Part 1.** IEEE Computer and Reliability Societies, 2013. Pág 1-2. Disponível em https://www.cs.princeton.edu/~arvindn/publications/crypto-dream-part1.pdf. Acesso em 22 de março de 2021.

NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN. **End-to-end encryption: ignoring abuse won't stop it.** 2019. Disponível em

https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption. Acesso em 22 de março de 2021.

NBC News. **Smart Refrigerators Hacked to Send out Spam: Report.** 2014. Disponível em https://www.nbcnews.com/tech/internet/smart-refrigerators-hacked-send-out-spam-report-n11946. Acesso em 22 de março de 2021.

NIST. **NIST's Post-Quantum Cryptography Program Enters 'Selection Round'.** National Institute of Standard and Technology, 2020. Disponível em https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round. Acesso em 22 de março de 2021.

OLIVEIRA, Marcos. **Nasce a Internet.** Revista FAPESP, 2011. Disponível em https://nic.br/noticia/nasce-a-internet/4397. Acesso em 22 de março de 2021.

O'BRIAN, Danny. **Orders from the Top: The EU's Timetable for Dismantling End-to-End Encryption.** Electronic Frontier Foundation, 2020. Disponível em https://www.eff.org/pt-br/deeplinks/2020/10/orders-top-eus-timetable-dismantling-end-end-encryption. Acesso em 22 de março de 2021.

OCDE. **Consumer Data Rights and Competition - Background note.** Organização para Cooperação e Desenvolvimento Econômico, 2020. Disponível em https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf. Acesso em 22 de março de 2021.

OCDE. **Guidelines for Cryptography Policy.** Organização para Cooperação e Desenvolvimento Econômico, 1997. Disponível em

http://www.oecd.org/digital/ieconomy/guidelinesforcryptographypolicy.htm. Acesso em 22 de março de 2021.

OXFORD ENGLISH DICTIONARY. **“Cypherpunk”.** 2021. Dispoível em https://www.lexico.com/definition/cypherpunk. Acesso em 22 de março de 2021.

PAILLOLE, Paul. **The Spy in Hitler’s Inner Circle: Hans-Thilo Schmidt and the Intelligence That Decoded Enigma.** Casemate Publishers, 2016.

PALFREY, John. **Security and the Basics of Encryption in E-Commerce.** Cyber Harvard, 2021. Disponível em https://cyber.harvard.edu/ecommerce/encrypt.html. Acesso em 22 de março de 2021.

PASSARINHO, Nathalia. **Governo elabora projeto para regular acesso a informações do WhatsApp.** G1, 2016. Disponível em http://g1.globo.com/politica/noticia/2016/07/governo-elabora-projeto-para-regular-acesso-informacoes-do-whatsapp.html. Acesso em 22 de março de 2021.

PATEL, Priti et al. **International Statement: End-To-End Encryption and Public Safety.** Department of Justice, 2020. Disponível em https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety. Acesso em 23 de março de 2021.

PENNEY, Jon. **Chilling Effects: Online Surveillance and Wikipedia Use.** Berkeley Technology Law Journal, Vol 31, n. 1, Pág 125. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645. Acesso em 22 de março de 2021.

PFEFFERKORN, Riana. **New intermediary rules jeopardize the security of Indian internet users.** TechStream, Brookings Institution, 2021. Disponível em https://www.brookings.edu/techstream/new-intermediary-rules-jeopardize-the-security-of-indian-internet-users/. Acesso em 22 de março de 2021.

PFEFFERKORN, Riana. **Security Risks of Government Hacking.** Stanford University, 2018. Disponível em http://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf. Acesso em 22 de março de 2021.

PFEFFERKORN, Riana. **The Rheroric of Responsible Encryption**. Just Security, 2017. Disponível em https://www.justsecurity.org/46102/rhetoric-responsible-encryption/. Acesso em 22 de março de 2021.

POLK, Ryan; FRONEK, April. **Your day with encryption.** Internet Society, 2019. Disponível em https://www.internetsociety.org/blog/2019/10/your-day-with-encryption/. Acesso em 22 de março de 2021.

PORESKY et al. **Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies.** Center for Long-Term Cibersecurity, Universidade da Califórnia - Berkley, 2017. Disponível em https://www.researchgate.net/publication/321443750_Cyber_Security_in_Nuclear_Power_Plants_Insights_for_Advanced_Nuclear_Technologies. Acesso em 22 de março de 2021.

RAMIRO, André. **A construção de imaginários nas narrativas governamentais sobre criptografia.** Derechos Digitales, 2019. Disponível em https://www.derechosdigitales.org/wp-content/uploads/A-Construcao-de-Imaginarios-nas-Narrativas-Governamentais-sobre-Criptografia-final.pdf. Acesso de 22 de março de 2021.

RAMIRO, André; CANTO; Mariana. **Cartilha: a importância social e econômica da criptografia".** Coalizão Direitos na Rede, 2020. Disponível em http://cartilhacriptografia.direitosnarede.org.br/. Acesso em 22 de março de 2021.

RAMIRO, André et al. **O mosaico legislativo da criptografia no Brasil: uma análise de projetos de lei.** Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2020. Pág 39. Disponível em https://obcrypto.org.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 22 de março de 2021.

RIBEIRO, Gabriel. **O Infocalipse vem aí.** UOL Notícias. 2018. Disponível em https://www.uol/noticias/especiais/ele-previu-o-apocalipse-das-noticias-falsas.htm#o-infocalipse-vem-ai. Acesso em 22 de março de 2021.

ROGAWAY, Phillip. **Ethics of Academic Cryptographers.** University of California - San Diego, 2014. Disponível em https://www.youtube.com/watch?v=HGEEJ44tkKs&ab_channel=KristovAtlas. Acesso em 22 de março de 2021.

ROGAWAY, Phillip. **The Moral Character of Cryptographic Work.** University of California- Davis, 2015. Págs 1-3, 10, 17, 46. Disponível em http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf. Acesso em 22 de março de 2021.

ROSEN, Jeffrey A. **Deputy Attorney General Jeffrey A. Rosen Delivers Remarks at Justice Department's Lawful Access Summit.** Department of Justice, 2019. Disponível em

https://www.justice.gov/opa/speech/deputy-attorney-general-jeffrey-rosen-delivers-remarks-justice-departments-lawfulaccess. Acesso em 22 de março de 2021..

ROSENSTEIN, Rod. **Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy.** Department of Justice, 2017. Disponível em https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarksencryption-united-states-naval. Acesso em 15 de dezembro de 2019.

SANGER, David; CLAUSING, Jeri. **U.S. Removes more Limits on Encryption.** The New York Times, 2000. Disponível em https://www.nytimes.com/2000/01/13/business/us-removes-more-limits-on-encryption.html. Acesso em 22 de março de 2021.

SCHNEIER, Bruce. **Applied Cryptography.** John Willey & Sons, 1996. Pág 21-22 e 58. Disponível em https://mrajacse.files.wordpress.com/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf. Acesso em 22 de março de 2021.

SCHNEIER, Bruce. **Click here to kill everybody: security and survival in a hiperconnected world.** W. W. Norton & Company, 2017. Págs. 8-10, 84-86.

SCHNEIER, Bruce. **Mujahid Secrets 2.** Schneier on Security, 2008. Disponível em https://www.schneier.com/blog/archives/2008/02/mujahideen_secr_1.html. Acesso em 22 de março de 2021.

SCHNEIER, Bruce. **Newsmaker Interview: Bruce Schneier on "Going Dark" and the Crypto Arms Race.** Schneier on Security, 2018. Disponível em

https://www.schneier.com/news/archives/2018/07/newsmaker_interview_.html. Acesso em 22 de março de 2021.

SCHNEIER, Bruce. **NSA Plans for a Post-Quantum World.** Lawfare, 2015. Disponível em https://www.lawfareblog.com/nsa-plans-post-quantum-world. Acesso em 22 de março de 2021.

SCHNEIER, Bruce. **Scaring people into supporting backdoors.** Schneier on Security, 2019. Disponível em https://www.schneier.com/blog/archives/2019/12/scaring_people_.html. Acesso em 22 de março de 2021.

SÉCULO DIÁRIO. **Grampo foi a maior violação aos direitos humanos já revelados no ES, diz subsecretário.** 2012. Disponível em https://www.seculodiario.com.br/justica/grampo-foi-a-maior-violacao-aos-direitos-humanos-ja-revelados-no-es-diz-subsecretario. Acesso em 22 de março de 2021.

SHORTELL, David. **FBI director claims encryption plan would make Facebook a 'dream come true' for child pornographers.** CNN Politics, 2019. Disponível em https://edition.cnn.com/2019/10/04/politics/fbi-facebook-child-encryption/index.html. Acesso em 22 de março de 2019.

SINGH, Simon. **The code book: how to make it, break it, hack it, crack it.** Delacorte Press, 2001. Págs. 96.

SINGH, Karan. **Twitter Blocks Accounts in India as Modi Pressures Social Media.** The New York Times, 2021. Disponível em https://www.nytimes.com/2021/02/10/technology/india-twitter.html. Acesso em 22 de março de 2021.

SITE INTELLIGENCE GROUP. **Al-Fajr Media Center Releasese New Encryption Program, "Amn Al-Mujahid".** 2013. Disponível em https://ent.siteintelgroup.com/Software-and-Technical-Materials/al-fajr-media-center-releases-new-encryption-program-amn-al-mujahid.html. Acesso em 22 de março de 2021.

SNOWDEN, Edward. **Eterna vigilância: como montei e desvendei o maior sistema de espionagem do mundo.** Editora Planeta, 2019, Pág 10.

SOLOVE, Daniel. **Nothing to Hide: the false tradeoff between privacy and security.** Yale University Press, 2011. Pág 25-26.

SPAGNUOLO, Sérgio. **Telegram: o novo refúgio da extrema direita no Brasil.** El País, 20201. Disponível em https://brasil.elpais.com/brasil/2021-02-21/telegram-o-novo-refugio-da-extrema-direita.html. Acesso em 22 de março de 2021.

STATISTA. **E-commerce in Brazil - Statistics & Facts.** 2021. Disponível em https://www.statista.com/topics/4697/e-commerce-in-brazil/. Acesso em 22 de março de 2021.

STATISTA. **Global Retail e-commerce sales worldwide from 2014 to 2023.** 2020. Disponível em https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/. Acesso em 22 de março de 2021.

STRASSER, Gerhard. **The long and winding history of Encryption.** The Atlantic, 2016. Disponível em

https://www.theatlantic.com/technology/archive/2016/01/the-long-and-winding-history-of-encryption/423726/. Acesso em 22 de março de 2021.

SUPREMO TRIBUNAL FEDERAL. **Audiência Pública sobre as Ação Direta de Inconstitucionalidade nº 5.527 e Ação de Descumprimento de Preceito Fundamental nº 403. Supremo Tribunal Federal.** 2017. Pág 53, 54 Disponível em http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 15 de dezembro de 2019.

SWIRE, Peter; AHMAD, Kenesa. **"Going Dark" versus a "Golden Age of Surveillance. Center for Democracy and Technology.** 2012 Disponível em https://fpf.org/wp-content/uploads/Going-DarkVersus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf. Acesso em 22 de março de 2021.

TECMUNDO. **Alexandre de Moraes, novo ministro do STF, favorece bloqueio do WhatsApp.** 2017. Disponível em https://www.tecmundo.com.br/whatsapp/114480-alexandre-moraes-novo-ministro-stf-favorece-bloqueio-do-whatsapp.htm. Acesso em 22 de março de 2021.

THE NATIONAL ARCHIVES. **Fighting talks: First World War Telecommunications.** The National Archives, 2021. Disponível em https://www.nationalarchives.gov.uk/first-world-war/telecommunications-in-war/. Acesso em 22 de março de 2021.

TRINTA, Fernando; MACÊDO, Rodrigo. **Um Estudo sobre Criptografia e Assinatura Digital.** Universidade Federal de Pernambuco, 1998. Disponível em https://www.cin.ufpe.br/~flash/ais98/cripto/criptografia.htm. Acesso em 22 de março de 2021.

TUCHMAN, Barbara. **The Zimmerman Telegraph.** Penguin Random House, 2016.

TUTOVEANU, Anton. **Active Implementation of End-to-End Post-Quantum Encryption.** University of Wollongong, 2021. Disponível em https://www.researchgate.net/publication/350134684_Active_Implementation_of_End-to-End_Post-Quantum_Encryption. Acesso de 22 de março de 2021.

UIT. **Global Cybersecurity Index 2018.** União Internacional de Telecomunicações, 2018. Pág 58. Disponível em https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. Acesso em 22 de março de 2021.

UNICEF. **Children's Online Privacy and Freedom of Expression.** 2018. Pág 4, 19-20. Disponível em https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf. Acesso em 22 de março de 2019.

UNICEF. **Encryption, Privacy and Children's Rights to Protection from Harm.** 2020, Pág. 10-11. Disponível em https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf. Acesso em 22 de março de 2021.

UNITED NATIONS. **Secretary-General of the United Nations. H.E. Mr. António Guterres, Secretary-General.** 2017. Disponível em https://gadebate.un.org/en/72/secretary-general-united-nations. Acesso em 22 de março de 2021.

UNITED NATIONS. **Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.** United Nations Office on Drugs and Crimes (UNODC), 2015. Pág 21-23. Disponível em https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf. Disponível em 22 de março de 2021.

UNIVERSITY OF EDINBURGH. **The Wassenar Arrangement.** The University of Edinburgh, 2021. Disponível em https://www.ed.ac.uk/infosec/information-protection-policies/procedures-guidance/travelling-working/secure-international-travel/where-are-you-going/countries-permitting-encryption/wassenar Acesso em 22 de março de 2021.

UOL. **Caso Henry: como software israelense achou dados apagados em celulares.** 2021. Disponível em https://www.uol.com.br/tilt/noticias/redacao/2021/04/09/caso-henry-como-funciona-o-software-que-achou-dados-apagados-em-celulares.htm. Acesso em 22 de março de 2021.

VENTURA, Felipe. **WhatsApp passa a usar criptografia ponta a ponta em todas as mensagens e plataformas.** Gizmodo, 2016. Disponível em https://gizmodo.uol.com.br/whatsapp-criptografia-ponta-a-ponta/. Acesso em 22 de março de 2012.

WILHEM, Pierre. **The Telegraph: strategic means of communications during the American Civil War.** Revista de História Americana, nº 124, 1999. Disponível em https://www.jstor.org/stable/23800946?seq=1. Acesso em 22 de março de 2021.

WEISER, Mark. **The Computer for 21st Century.** Scientific American, 1991. Disponível em https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf. Acesso em 22 de março de 2021.

WHITE HOUSE. **Administration Updates Encryption Export Policy.** Press Secretary, 2000. Disponível em https://cryptome.org/us-crypto-up.htm. Acesso em 22 de março de 2021.

WHITE HOUSE. **Statement by the Press Secretary.** Press Secretary, 1993. Disponível em https://epic.org/crypto/clipper/white_house_statement_4_93.html. Acesso em 22 de março de 2021.

WHITE HOUSE. **Statement by the Press Secretary.** Press Secretary, 1994. Disponível em https://epic.org/crypto/clipper/white_house_statement_2_94.html. Acesso em 22 de março de 2021.

WINNER, Langdon. **Do artifacts have politics?** University of Chicago Press, 1986. Disponível em https://nissenbaum.tech.cornell.edu/papers/Winner.pdf. Acesso em 22 de março de 2021.

WILLIAM, Robin; EDGE, David. **The social shaping of technology.** Research Policy Vol. 25. 1996. Pág. 2.

WINTERBOTHAM, F. W. **The Ultra Secret.** Harpercollins, 1974. Apud KAHN, David. **The Ultra Secret.** New York Times, 1974. Disponível em https://www.nytimes.com/1974/12/29/the-ultra-secret.html. Acesso em 22 de março de 2021.

WORLD ECONOMIC FORUM. **Cyber Resilience: Playbook for Public-Private Collaboration.** 2018. Pág 40. Disponível em http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf. Acesso em 22 de março de 2021.

WORLD ECONOMIC FORUM. **The Global Risks Report 2020.** 2020. Disponível em http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Acesso em 22 de março de 2021.

WRAY, Christopher. **Finding a Way Forward on Lawful Access: Bringing Child Predators out of the Shadows.** Federal Beureau of Investigation. Lawful Access Summit, 2019. Disponível em https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access. Acesso em 22 de março de 2021.

WYSOPAL, Chris; ENG, Chris. **Static Detection of Application Backdoors.** Veracode Inc, 2010. Pág. 1. Disponível em https://www.veracode.com/sites/default/files/Resources/Whitepapers/static-detection-of-backdoors-1.0.pdf. Acesso em 22 de março de 2021.

XINHUANET. **China to lead global cybersecurity market growth in next 5 years.** 2019. Disponível em http://www.xinhuanet.com/english/2019-09/09/c_138377152.htm#:~:text=China%27s%20cybersecurity%20spending%20in%202019,percent%20of%20the%20total%2C%20respectively. Acesso em 22 de março de 2021.

ZIMMERMAN, Phil. **Why I Wrote PGP**. 1999. Disponível em: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html. Acesso em 22 de março de 2021

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.** PublicAffairs, 2018.