PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Daniel Viégas

Criptografia e *backdoors*: uma questão de acesso ao inteligível

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Mestrado Profissional em Direito Civil Contemporâneo e Prática Jurídica da PUC-Rio.

Orientadora: Profª. Thamis Ávila Dalsenter

Rio de Janeiro
Setembro de 2022

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Daniel Viégas

Criptografia e *backdoors*: uma questão de acesso ao inteligível

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Mestrado Profissional em Direito Civil Contemporâneo e Prática Jurídica da PUC-Rio.

Profª. Thamis Ávila Dalsenter
Orientadora
Departamento de Direito – PUC-Rio

Prof. Caitlin Sampaio Mulholland
Departamento de Direito – PUC-Rio

Prof. Adriano Pilatti
Departamento de Direito – PUC-Rio

Profa. Bianca Kremer Nogueira Correa
Dannemann Siemsen

Rio de Janeiro, 1 de setembro de 2022

Daniel Viégas

Graduou-se em Direito pela PUC/RJ em 2011. Atualmente é Procurador do Município de Nova Iguaçu desde janeiro de 2015. Advogado atuante do RJ

Ficha Catalográfica

Viégas, Daniel

Criptografia e backdoors : uma questão de acesso ao inteligível / Daniel Viégas ; orientadora: Thamis Ávila Dalsenter. – 2022.

190 f. : il. color. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Direito, 2022.

Inclui bibliografia

1. Direito – Teses. 2. Criptografia. 3. Backdoors. 4. Infraestrutura. 5. Transnacionalidade. 6. Intermediários. I. Dalsenter, Thamis Ávila. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Direito. III. Título.

CDD: 340

À minha família e, especialmente,

à Mari, com amor.

Agradecimentos

À Professora Thamis Dalsenter, a quem tive a honra de ser orientado. As conversas francas sobre a privacidade mapearam o início desse trajeto.

Agradeço igualmente aos demais professores integrantes do corpo docente desse mestrado e que tive a oportunidade de receber lições, sobretudo pela abertura e paciência ao longo de todas as aulas e seminários: Aline de Miranda Valverde Terra, Carlos Nelson Konder, Marcelo Calixto, Antonio Pele, Pedro Marcos Nunes Barbosa e, especialmente, às Professoras Maria Celina Bodin de Moraes e Caitlin Sampaio Mulholland, em cujas aulas foi se desenhando as ideias sobre esse estudo, além da franqueza necessária da professora Caitlin em minha qualificação, momento em que também estendo esse agradecimento ao professor Adriano Pilatti. Em sua gentileza, todos cederam seus profundos conhecimentos ao engrandecimento dos aprendizes.

Agradeço aos amigos da turma do mestrado de Direito Civil da PUC-Rio do ano de 2020, Ana Luiza Fernandes, Bruna Kamarov, Carolina de Marsillac, Cristiano Schiller, Daniela Domingues, Diego Monteiro Baptista, Isabel Dunshee, Felipe Kadlec, Guilherme Macedo, Leonardo Ribeiro da Luz, Manoela Medeiros Sales, Maria Eduarda Echeverria Magacho, Maria Gentil, Paulo Mostardeiro, Pedro Alberto Schiller de Faria, Pedro Ramalhete, Pedro Sack e, especialmente ao amigo Pedro de Abreu Campos, pelas conversas e auxílios edificantes. Foi um privilégio aprender com vocês.

Agradeço, finalmente, à minha família, pequena, porém sólida, aos pouquíssimos e verdadeiros amigos e, por fim, à Mari, que com seu amor iluminou o final dessa jornada.

Resumo

Viegas, Daniel; Dalsenter, Thamis Ávila Dalsenter. **Criptografia e *Backdoors*: uma questão de acesso ao inteligível.** Rio de Janeiro, 2022. 190p. Dissertação de Mestrado em Direito Civil Contemporâneo e Prática Jurídica, Pontifícia Universidade Católica do Rio de Janeiro.

A presente dissertação tem por objeto o estudo da relação entre a criptografia e os *backdoors* e os seus reflexos sobre diferentes institutos jurídicos: privacidade, segurança, circulação da informação, proteção de dados, entre outros pontos. Considerada a escassa jurisprudência sobre os temas, esse estudo se concentra, majoritariamente, na pesquisa doutrinária e, também considerando a razoável novidade da discussão na doutrina nacional, não serão poucas as fontes estrangeiras. Inicialmente, buscamos investigar como os debates sobre a criptografia se encontram com as discussões sobre *backdoors*, partindo-se de algumas definições básicas sobre os institutos e, sobretudo da família de ideias que orbita a criptografia, tais como a seletividade do inteligível e a filosofia por trás das chaves da decriptação. Subsequentemente, apontamos para os valores em conflito no debate, para o histórico das guerras criptográficas e para os reflexos da criptografia na jurisdição constitucional através da ADPF 403 e da ADI 5.527. Posteriormente, investigamos outras circunstâncias que podem se acoplar ao debate, mas que, aparentemente, não são devidamente enfatizadas. Primeiramente, analisando as fontes dos *backdoors* nas infraestruturas conectadas para, em seguida, apresentar atores e saberes que podem explorar essas fontes com maior facilidade e, assim, acessar informações à revelia da criptografia através de métodos sub-reptícios, sobretudo, se considerado o prisma da transnacionalidade e a opacidade dos acordos informais de colaboração entre intermediários privados e outros governos. Nesse sentido, buscamos sinalizar para outras possíveis funções da criptografia, introduzindo uma tensão entre diferentes jurisdições e assimetrias de acesso a dados que estejam subordinados às infraestruturas interconectadas. Numa última etapa, buscamos apresentar algumas proteções contra os *backdoors* através dos institutos jurídicos ora disponíveis no ordenamento nacional, momento em que traçamos o enquadramento da criptografia como medida de segurança técnica da proteção de dados e das comunicações seguras na internet, atraindo disposições da Lei Geral de Proteção de Dados e do Marco Civil da Internet. Ademais, no afã de confrontar a opacidade e a desconfiança que pode pairar sobre eventuais intermediários colaboradores de outros governos, sinalizamos para ferramentas de transparência na LGPD, mas, desde já, apontamos para as possíveis dificuldades existentes nesse caminho.

Palavras-chave

Criptografia; Backdoors; Vulnerabilidades; Infraestrutura; Informações; Dados; Sub-reptícios; Transnacionalidade; Inteligência; Intermediários; Acordos Informais; Opacidade; Inteligível; Ininteligível; Chaves; Seletividade; Acesso.

Abstract

Viegas, Daniel; Dalsenter, Thamis Ávila Dalsenter. (Advisor). **Cryptography and backdoors: a question of access to the intelligible.** Rio de Janeiro, 2022. 190p. Dissertação de Mestrado em Direito Civil Contemporâneo e Prática Jurídica, Pontifícia Universidade Católica do Rio de Janeiro

This dissertation has as its object the study of the relationship between encryption and backdoors and their reflexes on different legal institutes: privacy, security, information circulation, data protection, among other points. Considered the scarce jurisprudence on the themes, this study is mostly concentrated in doctrinal research and, also considering the reasonable novelty of discussion in national doctrine, there will be no few foreign sources. Initially, we seek to investigate how the debates about encryption are with discussions about backdoors, starting from some basic definitions about the institutes and, especially the family of ideas that orbits encryption, such as the selectivity of the intelligible and philosophy for behind the decryptness keys. Subsequently, we point to conflict values in the debate, the history of cryptographic wars and the reflexes of encryption in constitutional jurisdiction through ADPF 403 and ADI 5.527. Subsequently, we investigate other circumstances that may be coupled to the debate, but apparently are not properly emphasized. First, analyzing the backdoors sources in the infrastructures connected to present actors and knowledge that can explore these sources more easily and thus access information to the default of encryption through surreptitious methods, especially if considered the prism of transnationality and the opacity of informal collaboration agreements between private intermediaries and other governments. In this sense, we seek to signal to other possible functions of encryption, introducing a tension between different jurisdictions and asymmetries of access to data that are subordinate to interconnected infrastructures. At a last stage, we seek to present some protections against backdoors through the legal institutes available now in the national order, when we draw the framing of encryption as a technical security measure of data protection and secure communications on the Internet, attracting the provisions of the General Law of Data Protection and the Civil Marco of the Internet. Moreover, in the eagerness to confront the opacity and distrust that can turn into any intermediaries collaborating from other governments, we signal to LGPD transparency tools, but we point out to the possible difficulties in this path.

Keywords

Cryptography; Backdoors; Vulnerabilities; Infrastructure; Information; Data; Surreptitious; Transnationality; Intelligence; Intermediaries; Informal agreements; Opacity; Intelligible; Unintelligible; Keys; Selectivity; Access.

SUMÁRIO

A perseguição dá origem a uma técnica de escrita peculiar e, com ela, também a um tipo de literatura peculiar, na qual a verdade sobre todas as coisas cruciais é apresentada exclusivamente nas entrelinhas. Essa literatura possui todas as vantagens da comunicação privada sem padecer, porém, de sua grande desvantagem, isto é, do fato de só alcançar os conhecidos do autor. Possui também todas as vantagens da comunicação pública sem ter a maior das desvantagens: a pena de morte imposta ao autor.

Leo Strauss

1. INTRODUÇÃO

Estamos no meio de uma nova redistribuição de poderes. A expansão da internet e a capilarização das mídias digitais no seio da sociedade expandiram, sem precedentes, a capacidade de transmissão e armazenamento de informações das mais diversas naturezas: expressões da intimidade, nossos comportamentos online, nossas relações sociais, mas também, não nos esqueçamos, dinheiro online, propriedades intelectuais, segredos de Estado, bits. Não apenas dados sensíveis, mas as informações sensíveis que regem as grandes infraestruturas do mundo, fazendo do ciberespaço um território de luta sobre os modelos de cibersegurança que lhe serão aplicados.

Historicamente, no intuito de concretizar a segurança, seja ela a segurança pública interna ou a segurança nacional, o Estado se vale da tradicional presença sigilosa em infraestruturas comunicativas, para fins de vigilância e monitoramento de condutas[1]. É nesse sentido, por exemplo, a tradicional prática do "grampo" telefônico, uma prerrogativa de interceptação legal, sigilosa, das comunicações via infraestrutura telefônica tradicional. Essa prática de explorar sigilosamente uma infraestrutura é, com a licença do reducionismo, o que se chama *backdoors*. Em tradução, o acesso aos dados que estão numa infraestrutura, mas através das "portas dos fundos" do sistema comunicativo.

Entretanto com o advento e a massificação das infraestruturas digitais e da comunicação pela internet, sobretudo em substituição às tecnologias comunicativas anteriores, esse paradigma da sigilosa presença estatal nas comunicações acaba por entrar em tensão com os novos modelos de infraestruturas digitais, de modo que muitos governos vêm optando por outras modelagens para fins de conservação, ou mesmo, atualização de suas prerrogativas de vigilância, tanto as legítimas quanto as ilegítimas.

Nessa linha, constata-se como linha de ação governamental o apelo à colaboração do setor privado, sobretudo através de grandes empresas cujas

[1] Não se objetiva discutir, aqui, as contingências dessas práticas, isto é, se são excessivas ou não, conforme o caso concreto. Apenas buscamos demonstrar que há uma tradição da presença do Estado, sigilosa, nas infraestruturas comunicativas, cabendo a cada país regular os freios e contrapesos dessas medidas em equilíbrio com outros direitos.

infraestruturas governam a maioria de nossas interações comunicativas cotidianas – Apple, Google, Microsoft, Facebook, WhatsApp, Yahoo, etc., mas também avançando para ações sobre a própria infraestrutura física da rede: pontos de troca da internet, cabos de fibra ótica submarina, desvio de tráfego de dados, etc.

A concretização dessa aproximação entre governos e algumas empresas é, não raro, cercado por imensa opacidade. Algumas vezes, entretanto, a colaboração se dá através da publicidade da própria legislação ao impor obrigações colaborativas das empresas para com alguns governos, mas outras vezes - o que é mais espinhoso – se dá pela realização de acordos informais em que se franqueia o acesso à infraestrutura privada para um ou outro governo parceiro, mas sem que a esfera pública tome conhecimento da aliança, salvo por eventuais vazamentos de um ou outro *whistleblower*.

Por muitas vezes o objeto da parceria se concretiza pelo próprio *design* das infraestruturas, dos dispositivos que a ela se acoplam e das redes conectadas. Busca-se impor, através da imperatividade do Estado, que o próprio desenvolvimento industrial de tecnologias seja projetado para permitir o acesso sigiloso de um ou outro governo: uma espécie de *insecurity by design.* Outras vezes, o objeto da parceria é materializado por uma relação de colaboração que não se desdobra, necessariamente, através do *design* do produto, mas pelo próprio arranjo jurídico em que se facilita a entrega de dados, o acesso aos servidores empresariais, entre outras especificidades.

Todas essas práticas compõem o paradigma *backdoors*: o conjunto de métodos para viabilizar incursões na infraestrutura comunicativa. São exemplos, a tradicional interceptação legal das linhas telefônicas, as diretrizes para que sejam produzidos algoritmos de fraca segurança no intuito de contorná-los, a captura de chaves de decifração de informações criptografadas, etc. Ao longo do estudo a exposição será mais demorada.

É importantíssimo pontuarmos que esse paradigma é mais antigo do que parece. A relação dos governos com as comunicações privadas é de longa data, tanto quanto são as comunidades de Inteligência e suas pretensões de controle dos suportes comunicativos. Conforme veremos ao longo desse estudo, a aliança entre

supervisão pública e as comunicações inteligentes pela computação estende suas origens na própria Segunda Guerra Mundial.

Entretanto, as revelações de Edward Snowden iluminaram esse paradigma, empurrando-o para deliberação na esfera pública. A história recente, entretanto, revelou que esse paradigma foi conduzido com abuso por algumas comunidades de Inteligência, sobretudo pela Agência de Segurança Nacional dos EUA (*National Security Agency – NSA*) e pelas demais instituições parceiras do mundo anglo-saxônico, sobretudo em razão da compartilhamento de saberes através do *Five Eyes*.

Revelou-se que os excessos cometidos pelo aparato da Inteligência através da vigilância em massa, impulsionados no início desse século pelo 11 de setembro, revelaram não apenas a colaboração das grandes empresas, suscitando, assim, uma legítima desconfiança sobre muitas dessas corporações, mas também revelaram um imenso conjunto de saberes privilegiados sobre como explorar, sorrateiramente, diversas infraestruturas comunicativas, como explorar *backdoors*, como acessar sub-repticiamente dados numa escala transnacional.

Como efeito dos vazamentos, houve uma guinada em prol da privacidade, seja através de novos diplomas jurídicos protetivos, seja pela própria mudança do mundo corporativo, que passou a empregar, em seus dispositivos, fortes ferramentas de cibersegurança, dificultando o acesso governamental a suas infraestruturas comunicativas.

Considerando a dificuldade imposta por esse paradigma *backdoors* e pela impossibilidade de erradicação das comunidades de Inteligências e seus possíveis abusos, o pensamento da época tem apontado para a proteção através de soluções técnicas, como a criptografia, um dos expoentes desses meios de segurança cibernética.

Paralelamente, a segurança das interações digitais vem se consolidando em favor da criptografia, que hoje representa não apenas uma ferramenta de proteção da informação, mas de proteção da própria integridade da infraestrutura comunicativa. Essas exigências por segurança nas interações pela internet com os traumas da vigilância em massa revelados por Snowden se fundem no mercado e a criptografia é abraçada como um elemento de proteção, figurando, atualmente,

como uma técnica em sintonia à privacidade, à proteção dos dados e, conforme expusemos, à integridade das infraestruturas comunicativas.

No entanto, seu estudo não pode ser isolado. É justamente sobre a relação entre a criptografia e os *backdoors*, como temas de cibersegurança, que debruçamos nossa análise. A criptografia deixa de ser um tema reservado aos técnicos para despertar o interesse de juristas, na medida em que introduz um profundo diálogo com valores presentes nos mais diversos ordenamentos jurídicos.

Uma das respostas aos excessos cometidos pelas comunidades de Inteligência, por exemplo, e em favor dos clamores pela privacidade foi a introdução da criptografia ponta a ponta em diversos dispositivos comunicativos presentes massivamente na sociedade, inclusive por muitas das empresas que possuíam algum grau de colaboração com seus governos sedes.

A adoção da criptografia ponta a ponta pelos mercadores de infraestruturas comunicativas introduziu, de largada, uma tensão direta com jurisdições locais. Isso porque a criptografia ponta a ponta protege o conteúdo das conversas trocadas entre emissor e destinatário das mensagens. Essa blindagem técnica, agora propagada na sociedade de massas, não foi recebida com bons olhos pelas forças de segurança, que passaram a protestar contra as novas tecnologias, no sentido de que as medidas de segurança a elas aplicadas estariam impedindo as prerrogativas de interceptação de informações para fins de consecução da segurança pública, além de que criminosos usarão a criptografia para esconder os seus métodos.

Como uma nova reação à expansão da criptografia ponta a ponta nos serviços de massa cotidianos, muitos governos retomaram as pautas por fragilização das infraestruturas no sentido de que sejam introduzidos *backdoors* para fins de executar suas prerrogativas de segurança. Por exemplo, busca-se compelir os produtores da infraestrutura digital a adotarem padrões criptográficos de baixa proteção para, assim, poderem contornar a segurança do dispositivo e acessar os dados.

Essa tensão entre a criptografia adotada por empresas com operação transnacional através da internet, aos quais chamamos de intermediários, e as jurisdições locais é o cerne do atual debate entre criptografia e *backdoors*, em sendo desenvolvida nesse estudo, sobretudo no primeiro capítulo, em que são

apresentados os principais institutos, a relação entre eles, os valores em conflito e a importante história do dilema cripto, de modo que possamos começar a mapear o arco histórico da criptografia e o que ele carrega em suas sombras, sobretudo os atores e os saberes privilegiados que orbitam aquela tensão.

Assim sendo, optamos por desenvolver no segundo capítulo um estudo sobre a dinâmica entre os variados atores envolvidos no dilema criptográfico, esboçando como a própria opção política por vivermos conectados e mediados por múltiplas funcionalidades interativas digitais engendra, inevitavelmente, a criação de *backdoors acidentais*, de modo que os sujeitos de conhecimento dessas portas dos fundos se articulam não por uma perspectiva vertical de regulações domésticas, mas numa arena transnacional, produzindo efeitos extraterritoriais e, não raro, valendo-se de meios sub-reptícios de acesso aos dados à revelia da criptografia. Uma dinâmica que pode revelar uma luta de jurisdições pela intensidade do acesso aos dados e que a criptografia, talvez, possa desempenhar outras funções desviantes.

Por fim, no terceiro e último capítulo apresentamos ferramentas protetivas previstas em nosso ordenamento que dialoguem com a criptografia, buscando enquadrar essa técnica às disposições previstas em nosso ordenamento e a relação dos *backdoors* com disposições previstas na Lei Geral de Proteção de Dados. Por fim, considerada a relevância dos intermediários, atores que operam as informações encriptadas numa escala transnacional, e a legítima desconfiança que eles podem despertar à luz do que foi desenvolvido nos capítulos anteriores, apresentamos uma possível ferramenta de transparência, bem como as dificuldades práticas que essa via pode enfrentar.

Uma pequena consideração. Esse estudo possui muitas notas de rodapé, sobretudo com longos comentários. A leitura intercalada entre o corpo do texto e essas notas pode retardar o ritmo da leitura. Por outro lado, falar sobre criptografia é falar em segredo. É falar através dos detalhes e, por vezes, os detalhes não se encerram em hierarquias topográficas.

2. CRIPTOGRAFIA E BACKDOORS: APRESENTAÇÕES

Nesta primeira etapa, buscamos investigar como os debates sobre a criptografia se encontram com as discussões sobre *backdoors*, partindo de uma análise das definições básicas sobre os institutos e, sobretudo da família de ideias que orbita a criptografia, tais como a seletividade do inteligível, a filosofia por trás das chaves da decriptação, entre outras ideias conexas. Subsequentemente, apontamos para o relacionamento entre os dois principais institutos, criptografia e *backdoors*, e o valores supostamente em conflito, o histórico das guerras criptográficas ao longo dos últimos cinquenta anos, de modo a contextualizar o foco do debate para, depois, alargar a discussão para a introdução de outras considerações que possam ser pertinentes ao debate.

2.1 Esclarecimentos Conceituais

Antes de avançarmos, é necessário tecer algumas considerações a respeito de institutos-chave presentes nesse estudo, de modo que a linguagem seja democraticamente acessível. Buscaremos, sempre que possível, abordar os problemas afastando o emprego de uma linguagem demasiadamente tecnocrática. Nem sempre conseguiremos, haja vista alguns pontos pressuporem certas colocações de ordem técnica.

2.1.1 Criptografia: Conceitos e Família de Ideias Associadas

O que é a criptografia? Quais famílias de ideias lhe orbitam? Quais ideias lhe são conexas, ainda que não expressadas claramente?

Primeiro: é possível afirmar que não há um conceito legal geral de criptografia em nosso ordenamento. Existem referências setoriais à criptografia no regulamento[2] do Marco Civil da Internet (MCI[3]), ao recomendar a *encriptação*; no

[2] Decreto n.º 8.771 de 11 de maio de 2016, Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

[3] Lei n.º 12.965 de 23 de abril de 2014 (Marco Civil da Internet – MCI). Para uma leitura mais dinâmica passaremos, de agora em diante, ao simples emprego dos termos: MCI e regulamento do MCI.

setor de telecomunicações, através do Ato Administrativo n.º 77 de 5 de janeiro de 2021 da ANATEL[4], que materializou a Resolução n.º 740 de 21 de dezembro de 2020 – o regulamento de segurança cibernética aplicado ao setor de telecomunicações – nas disposições sobre licitações públicas na modalidade de pregão eletrônico[5], neste último caso, originariamente no Art. 2º, §3º do Decreto Federal n.º 5.450/2005, posteriormente substituído pelo Decreto n.º 10.024/2019, mantida a redação anterior, mas através de seu Art. 5º, §1º, e também no Decreto n.º 7.845/2012[6], que regula algumas disposições específicas da Lei de Acesso à Informação[7], ao prever as expressões *cifração*, *decifração* e *recursos criptográficos,* além de diversas outras previsões voltadas à proteção de informações públicas sigilosas[8].

Segundo: considerando que as previsões normativas dizem muito pouco sobre um conceito estável ou, quando o fazem, endossam uma linguagem estanque, além de se encerrarem aos objetos específicos de cada um daqueles atos normativos, verifiquemos o que a doutrina aponta.

[4] Ato n.º 77/2021 da ANATEL. Algoritmos de criptografia: algoritmos baseados na ciência da criptografia, abrangendo algoritmos de encriptação/decriptação, algoritmos de hash criptográficos, algoritmos de assinatura digital e algoritmos de trocas de chaves.

[5] Revogado Decreto n.º 5.450/2005, Art. 2º O pregão, na forma eletrônica, como modalidade de licitação do tipo menor preço, realizar-se-á quando a disputa pelo fornecimento de bens ou serviços comuns for feita à distância em sessão pública, por meio de sistema que promova a comunicação pela internet. § 3º O sistema referido no caput será dotado de recursos de criptografia e de autenticação que garantam condições de segurança em todas as etapas do certame; Vigente Decreto n.º 10.024/2019, Art. 5º O pregão, na forma eletrônica, será realizado quando a disputa pelo fornecimento de bens ou pela contratação de serviços comuns ocorrer à distância e em sessão pública, por meio do Sistema de Compras do Governo federal, disponível no endereço eletrônico www.comprasgovernamentais.gov.br.

[6] O Decreto n.º 7.845 de 14 de novembro de 2012 regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, tendo por objeto densificar específicas disposições da Lei n.º 12.527 de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), notadamente os Artigos 25, 27, 29, 35, § 5º e 37 desta última. No caso do referido Decreto, são pertinentes as seguintes disposições: Art. 2º Para os efeitos deste Decreto, considera-se: II - cifração - ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem clara por outros ininteligíveis por pessoas não autorizadas a conhecê-la; VIII - decifração - ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original; XVII - recurso criptográfico - sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração; Cabe ressaltar, por fim, que o supracitado Decreto coexiste com o regulamento principal da Lei de Acesso à Informação, nesse caso, o Decreto n.º 7.724, de 16 de maio de 2012.

[7] Lei n.º 12.527 de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI)

[8] Nesse sentido, ver as seguintes disposições no regulamento da LAI no sentido da promoção de adequados recursos criptográficos ao grau de sigilo das informações: Artigos 27; 28; 31; 38, §3º; 39; 40 caput e parágrafo único; 41 caput e incisos I-V; 45, V; 56 caput e parágrafo único.

Carlos Affonso de Souza e Ana Lara Mangeth (2019) conceituam a criptografia como sendo uma “técnica de criação de códigos secretos que permitem enviar e receber mensagens para um destinatário sem que terceiros possam acessar e compreender o seu conteúdo" (Souza e Mangeth, 2019, p.71).

Daqui extraímos, por ora: técnica, comunicação, segredo entre polos. Sendo possível a partir de então, arriscar, um implícito desejo de que terceiros não conheçam o conteúdo trocado, compartilhado, emitido, recebido, ou expressões afins a essas ideias.

Por sua vez, Danilo Doneda e Diego Machado (2019) compartilham do conceito de Christof Paar e Jan Pelzl: “em linhas gerais, entende-se por criptografia ‘a ciência da escrita secreta com o objetivo de esconder o significado de uma mensagem” (2019 apud Paar; Pelzl, 2010, p.139). Daqui extraímos as ideias elementares e conexas de: segredo, camuflagem, mensagem/informação.

Richard Mollin (2007) apresenta uma interessante estrutura, na qual afirma que “a criptografia é o estudo de métodos para enviar mensagens em segredo, a saber, cifradamente ou de forma disfarçada, para que apenas o destinatário pretendido possa remover o disfarce e compreender a mensagem, ou decifrá-la” (2007, p. 79).

Segundo o autor, a mensagem original é chamada de *texto simples*, ao passo que a mensagem disfarçada é chamada de *texto cifrado*. Ele explica que o processo que transforma um *texto simples* em *texto cifrado* é chamado de *encriptação*, por sua vez, o processo reverso de transformação do texto cifrado em texto simples, realizado pelo destinatário e que tem o conhecimento para remover o disfarce é chamado de *decriptação* ou decifragem.

Nesse contexto, o autor também esboça a relação da criptografia com outros conceitos conexos, criptógrafo/criptografista; criptoanálise, criptoanalista; criptologia e criptólogo, explicando-os nos termos abaixo.

Criptógrafo/criptografista: é aquele que estuda e aplica os métodos de encriptação. O objeto de seu trabalho é a criptografia.

Criptoanálise: é o estudo de técnicas para derrotar a segurança dos métodos criptográficos. Complementamos: métodos para superar a criptografia. Em regra,

esses métodos se operam através do ataque aos sistemas encriptados para diagnosticar suas vulnerabilidades.

Criptoanalistas: são aqueles que estudam e aplicam a criptoanálise, explica Mollin (2007).

Ressaltamos, oportunamente, que a *criptoanálise* e os *criptoanalistas* são relevantes nesse estudo. Por essa razão, nos tópicos 3.3, 3.5 e, especialmente no tópico 3.4, dedicaremos algumas linhas sobre como opera essa dinâmica e seus efeitos no debate criptográfico sobre a segurança digital em geral. A título de antecipação, as comunidades de Inteligência[9] possuem extrema expertise na criptoanálise, além de investir massivamente na contratação de criptoanalistas.

Criptologia: é a incorporação dos estudos da criptografia e da criptoanálise, segundo Mollin (Idem). Acrescentamos: um gênero composto por espécies de saberes complementares.

Criptólogos: São aqueles que estudam e aplicam a criptologia, ou seja, tanto a criptografia quanto a criptoanálise, finaliza Mollin.

Podemos perceber, desde esse marco conceitual, uma divisão entre, de um lado, a defesa de sistemas pela criptografia e, de outro, o ataque de sistemas pela criptoanálise, espelhando uma divisão de saberes e de sujeitos de conhecimento desses saberes. No entanto, conforme veremos, os conhecimentos entre os dois campos se entrecruzam e evoluem reciprocamente, tema alargado oportunamente no tópico 3.4. Mas voltemos à criptografia propriamente dita.

A própria etimologia[10] da palavra lança as bases de sua compreensão. Mollin (Idem) explica que ela deriva da palavra grega "*kryptós*"[11], que significa

[9] Nesse trabalho, muitas vezes empregaremos as expressões "comunidades de Inteligência", "establishment da Inteligência", ou simplesmente a expressão "Inteligência" como expressões intercambiáveis. Optamos por empregar esses termos com a vogal "I" em sentido maiúsculo – Inteligência – para enfatizar que estamos nos referindo às instituições de espionagem e segurança nacional, e não ao substantivo abstrato feminino que diz respeito a capacidade de conhecer, raciocinar, etc.

[10] Diego F. Aranha, recorda a etimologia da palavra, "escrita secreta", e a sua tradicional preocupação com a confidencialidade da informação, além de outras propriedades, tais como "integridade, autenticação, não repúdio ou irretratabilidade, e anonimato" (ARANHA, Diego F. O que é a criptografia fim a fim e o que devemos fazer a respeito? *in*: DONEDA, Danilo e MACHADO, Diego. *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 24).

[11] κρυπτός

escondido. Pontuamos alguns sinônimos: cripto, secreto, oculto. E, segundo o autor, da palavra "*gráfein*"[12], que significa: escreva. Decorre da ação de escrever.

No entanto, para os fins aqui propostos, julgamos ser importante que a ideia de esconder uma mensagem não se restrinja à manifestação escrita, mas que também abranja as demais expressões: desenhos, códigos numéricos, códigos-fontes da computação, vozes, até mesmo gestos físicos. Enfim, qualquer expressão que possa ser objetificada e, subsequentemente, cifrada, embaralhada, tornada ininteligível, confidencial, secreta. Uma família de ideias que possui por denominador comum a vontade de excluir, tornar seletivo, restringir o acesso ao inteligível.

Buscamos, portanto, uma definição o mais abrangente possível no que toca aos tipos de expressões, afastando hipóteses que estejam confinadas a restritivas qualidades expressivas do objeto. Isto é, sem adjetivações prévias do objeto. Um conceito aberto o suficiente a contemplar, por exemplo, as futuras expressões, sejam elas humanas ou maquínicas[13].

Nessa linha, arriscamo-nos a definir a criptografia, para os fins aqui propostos, como a técnica empregada para cifrar um objeto, tornando-o ininteligível para aqueles que não tenham acesso às convenções combinadas para decifrá-lo.

Esse objeto, essa linguagem inespecífica, esse conjunto de possíveis símbolos, pode ser qualquer coisa passível de conversão em alguma linguagem inteligível. Desde uma palavra até mesmo um sinal comunicativo capturado enquanto passa pelo ar e posteriormente objetificado em alguma linguagem transmissível.

A definição certamente não é imune de críticas. Trata-se apenas de uma tentativa de esboçar um conceito aberto às múltiplas comunicações e linguagens possíveis, aberto às inúmeras subjetividades. O centro conceitual é a

[12] γράφειν

[13] Ao empregar o termo "maquínicas" não objetivamos ingressar nas profundezas do estudo sobre a subjetividade maquínica discutida por Gilles Deleuze e Félix Guattari no Anti-Édipo. (DELEUZE, Gilles e GUATTARI, Félix – *O anti-Édipo*. Tradução Luiz B. L. Orlandi. 2a ed. Editora 34, 2011).O emprego do termo, aqui, é muito mais modesto. Objetivamos, tão somente, representar a possibilidade de expressões comunicativas de máquinas, por exemplo, através da própria computação e a sua interconexão com outras infraestruturas tecnológicas. O campo da Internet das Coisas, por exemplo, também seria correlato.

ininteligibilidade de um objeto. Nesse sentido, pedimos a condescendência do(a) leitor(a) para analisarmos seu cerne por meio de simples perguntas retóricas.

Faria sentido tornar algum objeto completamente ininteligível? Isto é, faria sentido tornar uma expressão completamente inacessível para todo e qualquer sujeito? Como seria possível a comunicação se o objeto comunicado for absolutamente incompreensível?

Certamente não faria sentido algum tornar um objeto absolutamente ininteligível se o objetivo é comunicá-lo ou acessar a sua inteligibilidade. A intenção de tornar algo ininteligível, para fins de comunicação, é sempre relativa. A ininteligibilidade é relativa. Atrai-se a ideia de oponibilidade. A ininteligibilidade não objetiva ser oponível àqueles aos quais se intenciona a compreensão do objeto. Não intenciona ser oponível àqueles aos quais foram concedidas as ferramentas para reverter a ininteligibilidade e, assim, decifrarem o objeto. Essas ferramentas são as convenções compartilhadas entre emissário e receptor: as chaves que eles possuem para a compreensão.

Veja essa frase. Novamente. Veja essa frase. Visualize esse ponto final bem aqui ao lado direito da palavra ao lado. Um pequeno símbolo, “.” , que marca o encerramento de uma frase, o ponto final.

Eu compartilho com você, leitor(a), a convenção da língua portuguesa. Eis uma chave entre nosso entendimento, entre nossa inteligibilidade. Essa frase, esse objeto, nos é inteligível pois possuímos a chave que decifra esse amontoado de letras, símbolos, unidos um ao lado do outro para formar, espaçadamente, palavras. Esta chave foi construída ao longo de todo o nosso processo de alfabetização. Nós a internalizamos. Ela está escondida em nosso sistema cerebral.

Outra chave que possuímos é a convenção, também internalizada, que nos diz para ler da esquerda para direita. Percebe-se que nós dois, emissário e receptor, compartilhamos convenções, chaves, premissas, sem nem mesmo termos nos encontrado? Uma delas é a antiga língua portuguesa, outra é a própria convenção, mais antiga ainda, de se ler da esquerda para direita.

As convenções do entendimento, da inteligibilidade, o compartilhamento de premissas, enfim, as condições do acesso ao inteligível são significantes que alimentam a filosofia por trás do conceito de chaves, um elemento de extrema

importância na criptografia. São as chaves que permitem a *decriptação*, a compreensão justamente daquilo que foi propositadamente embaralhado para que terceiros indesejados não compreendam.

Mas o mais importante, são as chaves que introduzem a seletividade do cognoscível. Elas introduzem o espectro de sujeitos aptos à compreensão e compartilhamento do objeto. Não raro, afirme-se que "esse é o princípio de ordenação da criptografia: todo o poder está com o detentor da chave" (Snowden, 2019, p. 230). E não parece menos importante o fato de que Tim Wu, em sua obra, Impérios da Comunicação, tenha escolhido como epígrafe do seu texto a seguinte frase de Fred Friendly: "Não está em jogo a Primeira Emenda ou a liberdade de expressão, mas a guarda exclusiva da chave geral" (2011, epígrafe). Exclusividade. Exclusão. Excluir. Pertinentes símbolos representativos.

Avancemos e verifiquemos a *encriptação* e a *decriptação* através de um exemplo fornecido por Duane C. Wilson em que são utilizadas aquelas definições anteriores de *texto simples* e *texto cifrado*, mas esboçando a criptografia como uma equação:

"texto cifrado = texto simples + chave de encriptação (1) e

"texto simples = texto cifrado + chave de decriptação (2)" (Wilson, 2021, p. 33).

O autor afirma que na equação (1) o texto simples é convertido em texto cifrado por uma chave de encriptação. Por sua vez, na equação (2), o texto cifrado é traduzido pela chave de decriptação para a sua forma original: de texto simples.

Lembrando que o texto simples pode ser em forma de texto, áudio, vídeo, imagens, enfim, qualquer expressão que possa ser objetificada através de símbolos compartilháveis, transmissíveis para a compreensão daquele(s) que porta(m) as chaves.

Por sua vez, o texto cifrado é justamente o oposto: é um objeto relativamente ininteligível. Ao menos, não compreensível para os terceiros que devem ser seletivamente excluídos da compreensão da informação transmitida ou armazenada.

Para visualizarmos um exemplo, tomemos de empréstimo a seguinte "chave" de encriptação e decriptação demonstrada por Duane C. Wilson:

"texto simples do alfabeto: abcdefghijklmnopqrstuvwxyz

texto cifrado do alfabeto: phqgiumeaynofdxjkrcvstzwb"

Nota-se que, nesse caso, convencionou-se que a letra "p" significa "a"; que a letra "h" significa "b", que a letra "q" significa "c", e assim por diante, nos termos das chaves da compreensão supracitada.

Assim, o autor propõe encriptar o seguinte texto simples/original: "*defend the east wall of the castle*" (2021, p.33). Como seria a sua versão cifrada à luz da chave descrita acima?

Segundo Wilson, sua forma em texto cifrado/encriptado seria: "giuifg cei iprc tpnn du cei qprcni" (Idem, p.33).

Assim, caso o destinatário recebesse a mensagem "giuifg cei iprc tpnn du cei qprcni" e utilizasse a chave/convenção descrita acima, ele chegaria ao entendimento de que é necessário "defender a parte leste do castelo".

Visualize, por sua vez, a seguinte palavra: ROMA

Uma cidade? A capital da Itália?

E se eu lhe dissesse que esta palavra, ROMA, foi encriptada. Que esse não é o significado que eu desejo transmitir. E se eu tivesse convencionado com você, leitor(a), que as chaves de nossa compreensão fosse a seguinte convenção compartilhada, simplíssima: leiamos a palavra "ROMA" da direita para a esquerda. Como você iria passar a ler e interpretar a palavra "ROMA"?

Um sentimento? O maior de todos?

Uma única palavra. Um único objeto. Diferentes significados. Para o auditório, para todos aqueles terceiros indesejados, seria a palavra ROMA, a capital da Itália. Pois eles estão sob a convenção que soma símbolos da esquerda para a direita.

Para nós, emissário e receptor, seria a palavra AMOR, um sentimento. Pois nós estivemos, por um breve momento, sob a convenção que também soma

símbolos, mas da direita para a esquerda. Mudou a inteligibilidade da nossa comunicação? Falar sobre criptografia é, antes de mais nada, falar nas entrelinhas.

Peço, portanto, a indulgência do(a) leitor(a) para que busque essas entrelinhas ao longo da exposição.

Nos exemplos acima, "ROMA-AMOR"[14] e "defenda o lado leste do castelo", tomamos em consideração que as chaves do entendimento das mensagens

[14] Na realidade, o exemplo "ROMA-AMOR" espelha um exemplo simples, muito mais relacionado ao estudo da esteganografia. Trata-se de uma derivação da criptografia, em que também se estuda a transmissão de mensagens de forma secreta, mas com base no próprio design da estrutura visível e através do ocultamento, de modo que não seja apresentado um enunciado cifrado, conforme ocorre com a criptografia, na qual o adversário/terceiro visualiza indícios de que algo está escondido, porém não compreende a sua inteligibilidade. Por sua vez, Ronald L. Rivest define a esteganografia como a "a arte de esconder uma mensagem secreta dentro de uma maior, de tal maneira que o adversário não pode discernir a presença ou conteúdo da mensagem oculta. Por exemplo, uma mensagem pode estar escondida dentro de uma foto, sendo visualizada através da alteração dos Bits de pixel da imagem" (RIVEST, Ronald L. - *Chaffing and Winnowing: Confidentiality without Encryption*. MIT Laboratory for Computer Science – Technology Square Cambridge. Cryptobytes, 1998). No entanto, tanto na criptografia quanto na esteganografia são comuns as ideias de camuflar uma mensagem - torná-la confidencial - e de selecionar quem pode compreendê-la. Apenas o modo de execução do disfarce é que é diferenciado. Para maiores detalhes, ver: (WINSTEIN'S, Keith – *Lexical Steganography Through Adaptive Modulation of the Word Choice Hash*. MIT, 1998). A técnica vem sendo aplicada, em grande parte, no campo das imagens, sobretudo fotografias. Nesse sentido: (ZHANG, K.A., VEERAMACHANENI, K. - *Enhancing Image Steganalysis with Adversarially Generated Examples*. In: DOLEY, S., HENDLER, D., LODHA, S., YUNG, M. (eds) Cyber Security Cryptography and Machine Learning. CSCML, 2019. Lecture Notes in Computer Science, vol 11527, 2019. Para um exemplo do uso da esteganografia expressada em obra cinematográfica, mas sem *spoilers*, ver "O Escritor Fantasma", filme de Roman Polanski, notadamente o desfecho da trama. Digno mencionar, que os estudos contemporâneos da esteganografia, sobretudo a sua aplicação sobre as infraestruturas que integram a internet, ainda é um campo em evolução. Nessa linha, desponta-se, exemplificativamente, os crescentes estudos sobre uma de suas técnicas, a "obfuscation"/ofuscamento/ofuscação. Por curiosidade oportuna, buscamos verificar se a DARPA - instituição mãe da Internet enquanto esta ainda era a ARPANET – possuiria algum braço sobre o tema e encontramos no artigo *Indistinguishability Obfuscation for RAM Programs and Succinct Randomized Encodings*, de 2018, a informação, em rodapé na sua página inicial, sobre o suporte de parte da pesquisa pela DARPA, além de outras instituições envolvidas, como a Microsoft. (BITANSKY, Nir, CANETTI, Ran, GARG, Sanjam, HOLMGREN, Justin, JAIN, Abhishek et al. - *Indistinguishability Obfuscation for RAM Programs and Succinct Randomized Encodings*. Vol. 47, No. 3, pp. 1123–1210, MIT, 2018). Por sua vez, no sítio online da DARPA, à despeito das poucas pesquisas ali publicizadas, encontramos a previsão de investimentos de alguns milhões de dólares para os anos de 2021, 2022 e 2023 no Programa *RACE - Resilient Anonymous Communication for Everyone*, do qual se colhe a seguinte descrição: "The Resilient Anonymous Communication for Everyone (RACE) program is developing cryptographic and communication obfuscation technologies to enable anonymous, attack-resilient, mobile communications within a network environment. RACE is developing a mobile communication application and distributed systems that provide a secure message- passing service by combining advances in distributed system tasking with communication protocol encapsulation methods. The RACE system will maintain confidentiality, integrity, and availability of messaging while preventing large-scale compromise of the system. RACE security is based on rigorous security arguments or statistical arguments based on realistic simulations, and not on ad hoc estimates of security." (DARPA - Department of Defense Fiscal Year (FY) 2023 Budget Estimates April 2022. Defense Advanced Research Projects Agency Defense-Wide Justification Book Vol. 1 of 5 Research, Development, Test & Evaluation, Defense-Wide. (Disponível em: <https://www.darpa.mil/attachments/U_RDTE_MJB_DARPA_PB_2023_APR_2022_FINAL.pdf

foram previamente compartilhadas entre emissor e destinatário. No primeiro caso, supostamente eu teria compartilhado com o leitor(a), tacitamente, a chave "leia da direita para a esquerda", ao passo que no segundo exemplo, eu teria compartilhado a chave em que se deveria ler o alfabeto da seguinte forma: "p = a; h = b; q = c, e assim por diante", conforme alinhado acima.

Esse compartilhamento prévio das convenções da inteligibilidade, das chaves, sempre esteve presente na criptografia. Conforme ensina Diego F. Aranha (2019), "até esse ponto, as técnicas criptográficas conhecidas sempre exigiam o compartilhamento prévio de um segredo (chave criptográfica) para comunicação confidencial, por isso chamadas simétricas" (Aranha, 2019, p. 24).

Entretanto, como funcionariam as nossas diversas comunicações e transações online no mundo contemporâneo se fosse necessário que cada um encontrasse previamente com outro para compartilhar uma chave de entendimento? Seria possível que ao comprarmos algum bem no sítio online de uma empresa tivéssemos que nos encontrar previamente com os donos dessa infraestrutura para convencionar o modo comunicativo seguro? Não. Seria inviável numa sociedade de massas, na medida em que as comunicações trocadas são incessantes, múltiplas e envolvem sujeitos que nem se conhecem, nem nunca se conhecerão.

Para tanto, inventou-se, com escoro na computação, a criptografia assimétrica, ou de chave pública, permitindo, assim, a comunicação confidencial a longas distâncias, explica Aranha. Portanto, entre sujeitos que não se encontraram previamente. Não precisamos entrar em detalhes sobre as diferenças técnicas entre criptografia simétrica e criptografia assimétrica[15]. A diferenciação aqui exposta neste momento teve por objetivo, apenas enfatizar para o(a) leitor(a), que as

---

>. Acesso em 10 jun. 2022. Por fim, para um diferente emprego do termo "*obfuscation*", dissociado do contexto estritamente computacional suscitado acima, e ventilado como um conjunto de técnicas confrontadoras de mecanismos de vigilância, ver a obra: (BRUNTON, Finn e NISSENBAUM, Helen – *Obfuscation: a user's guide for privacy and protest*. 1a ed. - United States: MIT Press paperback edition, 2016).

[15] Para maiores detalhes quanto ao ponto, ver, na doutrina nacional as lições de DIEGO F. ARANHA: (ARANHA, Diego F. *O que é a criptografia fim a fim e o que devemos fazer a respeito? in*: DONEDA, Danilo e MACHADO, Diego. A Criptografia no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. pp. 24-30). Correlatamente, DUANE C. WILSON explica, em breves linhas, que na encriptação simétrica se usa a mesma chave, tanto para encriptar quanto para decriptar e, na assimétrica, diferentes chaves: uma de natureza pública para encriptação (public key/chave pública), e outra, de natureza privada, para decriptação (private key/chave privada), dispondo, ainda sobre os benefícios e as desvantagens de cada um dos modelos. (WILSON, Duane C. – *Cybersecurity*. Cambridge, Massachusets: The MIT Press, 2021, pp. 11-16).

convenções do entendimento, do inteligível, as chaves, persistem como uma ideia cara à criptografia, ainda que hoje não nos encontremos previamente para formar, caso a caso, a nossa ética de encriptação e decriptação.

Avancemos para outras adjetivações da criptografia.

2.1.2 Criptografia Forte e Criptografia Fraca

O exemplo anterior, ROMA-AMOR, espelhou uma criptografia fraca. Bem fraca, por sinal. Fácil de ser decifrada por um terceiro indesejável.

Hoje, por outro lado, já existem meios tecnológicos mais eficientes e que dificultam seriamente o sucesso do processo reverso de decriptação, sobretudo se auxiliados pela computação. Trata-se da criptografia forte: "uma referência genérica a algoritmos de criptografia (e suas implementações) que, em comparação a outros algoritmos, são difíceis de ser comprometidos" (Liguori Filho, 2019, p. 92).

Souza e Mangeth (2019) pontuam que "uma criptografia forte (que usa algoritmos apropriados e é implementada adequadamente) e confiável transformou-se em verdadeira necessidade para as mais diversas operações" (2019, p. 76). Complementarmente, Susan Landau (2017) aponta para uma importante associação. Ela subordina o conceito de criptografia forte ao contexto tecnológico. Para a autora, a mensuração do que é fortemente protegido é relativo ao estado da arte tecnológico disponível para decriptação do objeto: criptografia forte é igual a criptografia difícil de decifrar com a tecnologia atual.

Essa relação entre fraqueza e força de uma proteção à luz do atual[16] estado da arte tecnológico é importantíssima, pois ela introduz a historicidade das

[16] Existem diversos critérios para mensurar o grau de proteção – se forte ou fraco – de um sistema criptográfico. Desde a qualidade do algoritmo até o tamanho das chaves de decriptação, passando pelos fatores de implementação, entre outros pontos. Para maiores detalhes, ver: (GYAWALI, Yashant B. - *ENCRYPTION ALGORITHM Advanced Encryption Standard*. Caldwell University Caldwell, NJ, US. 2020. OLEKSANDR BODRIAGOV e SONJA BUCHEGGER, por sua vez, apresentam critérios para avaliar a qualidade da criptografia ponta a ponta (BODRIAGOV, Oleksandr e BUCHEGGER, Sonja - *Encryption for Peer-to-Peer Social Networks*. School of Computer Science and Communication KTH - The Royal Institute of Technology Stockholm, Sweden. 2011). Considerando, no entanto, que essa verificação está subsumida a uma taxonomia eminentemente técnica, divergindo da abordagem proposta nesse estudo, adotamos a generalização de que a qualidade protetiva está relacionada ao tempo histórico do aparato tecnológico disponível em uma determinada época. À título de exemplo, hoje, os sistemas criptográficos mais fortes não seriam páreo para o advento da computação quântica, a qual, segundo o que se propaga, teria o poder

tecnologias disponíveis, o que pode nos levar a uma pergunta incômoda: atual estado da arte tecnológico disponível para quem? Além do mais, esse grau de proteção funcionalizado ao tempo e às ferramentas tecnológicas é uma premissa que será retomada em breve ao discutirmos o conceito de autofagia no tópico 3.3. Por enquanto, guardemos a ideia.

Mas, afinal, para fins práticos e atuais, o que a criptografia protege hoje em dia? Sobre o que ela incide em nosso cotidiano?

2.1.3. Alcance Protetivo da Criptografia

Segundo Landau (2017), a criptografia protege a informação em trânsito – comunicações – e a informação armazenada – particularmente, informação armazenada em *smartphones*, *laptops* e outros dispositivos digitais.

Doneda e Machado (2019) pontuam que a criptografia em repouso – *encryption at rest* – remete-se a dados protegidos enquanto são persistentemente armazenados em um terminal, por exemplo, num *laptop*, num dispositivo móvel ou até mesmo no servidor de um provedor de serviços.

Dessa forma, Doneda e Machado afirmam que seria possível encriptar um arquivo digital, uma pasta, uma parcela do disco rígido e até mesmo um dispositivo inteiramente, de modo que "sem a chave de decriptação o conteúdo do arquivo encriptado ou de todos os dados armazenados no dispositivo ou terminal são ininteligíveis a terceiros não autorizados" (Idem, p. 153-154).

---

de desencriptar praticamente todos os segredos tutelados pelos variados padrões de criptografia forte praticados atualmente. Nesse sentido, ver: ADITYA, J., SHANKAR RAO, P. - *Quantum Cryptography*. Computer Science Engineering at Andhra University. Disponível em: <https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf>. Acesso em 22 dez. 2021. JAKE TIBBETTS, por sua vez, apresenta um contexto de rivalidade entre EUA e China na corrida pela computação quântica (TIBBETTS, Jake. - *Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers.* Center for Global Security Research LAWRENCE LIVERMORE NATIONAL LABORATORY. September 20, 2019). Na mesma linha, para verificação da recente fabricação de um semicondutor capaz de materializar a mais rápida produção de números aleatórios já vista, bem como as suas potenciais ressonâncias para a criptografia e para a computação quântica, ver: CASTELVECCHI, Davide – *This Is the Fastest Random-Number Generator Ever Built: A laser generates quantum randomness at a rate of 250 trillion bits per second and could lead to devices small enough to fit on a single chip*. Scientific American – Nature magazine. On March 3, 2021. Disponível em: <https://www.scientificamerican.com/article/this-is-the-fastest-random-number-generator-ever-built/>. Acesso em 10 dez. 2021.

Por sua vez, para os autores a criptografia em trânsito/movimento/em fluxo – *encryption in transit* – "se opera quando a informação comunicada trafega de um computador a outro" (Doneda e Machado apud. Gill; Israel; Parsons, 2019, p. 153).

Pensamos ser mais inclusiva a noção de trânsito entre um terminal e outro terminal. Isso porque o MCI adota como conceito de terminal o que se segue: Art. 5º, II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

Nesse sentido, o computador seria uma espécie do gênero "terminal". Subsequentemente, a encriptação em trânsito/em fluxo poderia ser aquela que se opera enquanto a informação trafega entre terminais.

Em acréscimo, Doneda e Machado (Idem) chamam a atenção para um importantíssimo risco relativo a essa divisão: o fato de que a encriptação em trânsito, se não for acompanhada pela cifragem de dados em repouso, submeterá as informações comunicadas a vulnerabilidades suscetíveis de exploração por terceiros.

Mas a criptografia é aplicável somente à tutela da informação propriamente dita ou ela também pode ser estendida para outras situações?

Doneda e Machado apontam para novas possibilidades de aplicação da criptografia. Apesar de ressaltarem a importância do antigo prisma de discussão calcado na informação, também chamam a atenção para a necessidade de uma atualização do tema, alargando-se o escopo do estudo e das discussões sobre as repercussões da criptografia. Eis as palavras dos autores:

> com a multiplicação das infraestruturas de informação e comunicação, a criação de ambiente interconectados e o exponencial aumento de tecnologias baseadas no intensivo processamento de dados e automatização, o destaque da segurança nas operações de tratamento de dados segue ritmo idêntico. Há quem sustente que no contexto atual não se deve falar apenas em segurança da informação, mas deve-se utilizar o termo cibersegurança (cibersecurity), de significado mais alargado. Enquanto na primeira noção objetiva-se proteger a informação como ativo tratado via tecnologias da informação e da comunicação (TICs), nesta última parte-se do entendimento de que tanto a informação como a infraestrutura formada pelas TICs são a razão subjacente das vulnerabilidades existentes que, exploradas, podem causar danos a pessoas, seja a interesses privados ou coletivos (2019, pp. 8-9)

Os autores chamam a atenção para um importante marco jurídico nessa discussão, a decisão do Tribunal Constitucional Federal alemão de 27 de fevereiro de 2008 (*BVerfG, NJW 2008, 822*), em que se entendeu que o rol de direitos

fundamentais então vigentes, privacidade, sigilo das comunicações e autodeterminação informativa, não seriam suficientes à proteção dos cidadãos em face do monitoramento e busca remotos que computadores podem ensejar.

A decisão, segundo os autores, teria criado um direito fundamental: um direito à confidencialidade e à integridade não da informação, mas, diferentemente, um direito à confidencialidade e à integridade dos próprios sistemas de tecnologia da informação.

É interessante a aplicação da criptografia como um ativo das tecnologias de informação. No tópico 2.1.5, adiante, teceremos algumas palavras, por exemplo, sobre as tecnologias de informação e comunicação, as TICs.

Por ora, podemos afirmar que essa abordagem, extensiva da criptografia à tutela das próprias infraestruturas comunicativas, é propícia ao endereçamento da relação entre criptografia e *backdoors* para o seu ramo comum: a cibersegurança[17].

No entanto, afora essas novas considerações sobre a aplicação da criptografia, em quais situações envolvendo a informação propriamente dita a criptografia não estende sua proteção? Quais tipos de informações não são protegidos, em regra, pela criptografia? Os metadados.

2.1.4 O "Fora Complementar": Metadados

O que são metadados?

Segundo Jenn Riley (2017), em linhas gerais, a própria etimologia da palavra revela seu significado: metadados são dados sobre dados. Ela afirma serem as informações que criamos, armazenamos e compartilhamos para descrever um

[17] Duane C. Wilson afirma que o objetivo geral da cibersegurança é proteger os ativos digitais de serem comprometidos, desdobrando-se em seis objetivos específicos de proteção: i) Confidencialidade: manutenção das informações em segredo; ii) Integridade: verificação da confiabilidade dos dados e sistemas; iii) Disponibilidade: garante que as informações estejam disponíveis para as pessoas certas na hora certa; iv) Autenticação: verificação de identidades; v) Autorização: verificação do acesso a recursos e; vi) Não repúdio: validação da fonte de informação. Diante desses 06 principais objetivos, o autor explica que três deles possuem a criptografia como um meio de proteção inerente e necessário, confidencialidade, integridade e não repúdio, ao passo que os demais podem se valer da criptografia como um elemento contingente a depender das espécies/formas de disponibilidade, de autenticação e de autorização escolhidas casualmente. (WILSON, Duane C. – *Cybersecurity*. Cambridge, Massachusets: The MIT Press, 2021, pp.10-46).

objeto. Elas não se confundem com o objeto em si. São as descrições sobre esse objeto.

Por exemplo, em um livro físico o conteúdo seria o texto impresso nas páginas. E os metadados sobre o livro seriam: a capa dura, o tamanho da brochura, o número de páginas, as dimensões das páginas, a coloração da capa, etc.

Conforme Riley (Idem) aponta, essa definição ampla – dados sobre dados – pode despertar a suspeita de que os metadados estão em todos os lugares, em sendo precisamente correta essa suspeição. A autora explica que os metadados estão difundidos em sistemas de informação sob diferentes formas, de modo que a maioria dos softwares que utilizamos é orientada por metadados.

De acordo com a autora, "as pessoas ouvem música através do *Spotify*, postam fotos no *Instagram*, buscam vídeos no *YouTube*, conectam-se umas às outras por *email*, texto e mídia social, armazenam longas listas de contatos em seus dispositivos móveis. Todo esse conteúdo está imbuído de metadados: informações sobre a criação do item, nome, tópico, recursos utilizados e similares" (2017, p. 02).

Para os fins aqui propostos, os metadados se referem a dados além do conteúdo da comunicação eletrônica. Assim, em um aplicativo de troca de mensagens dotado de criptografia ponta a ponta, por exemplo, o conteúdo seria o que foi conversado entre os polos, isto é, o teor das mensagens trocadas entre os participantes da conversa. Segundo consta em relatório publicado pela UNESCO (2016), esse conteúdo estaria protegido pela criptografia.

Por outro lado, os metadados seriam as informações que os provedores de serviços podem observar na prestação de serviços: quando; com que frequência; por quanto tempo; e com quem os usuários estão se comunicando (Idem). É dizer: o IP/localização, a hora do envio da mensagem, para quem e por quem a mensagem foi enviada, a duração da comunicação, o eventual número discado, a lista de contatos, entre outras inúmeras informações descritivas da comunicação trocada. Essas informações descritivas, em regra, não estão encriptadas (Idem).

Ainda de acordo com o relatório publicado pela UNESCO, o poder dos metadados reside no fato de que uma vez reunidos, eles podem compor um conjunto extremamente detalhado das comunicações de uma pessoa, contribuindo para a formação de padrões comportamentais. Por sua vez, conforme ressalta a *Electronic*

Frontier Foundation (EFF), em regra, os sistemas jurídicos protegem o conteúdo mais do que os metadados.[18]

Portanto, há de se pontuar que a criptografia não abrange os metadados. Ela tutela o conteúdo em trânsito e o conteúdo armazenado, mas não alcança os metadados. Nessa linha, os metadados representam um "fora complementar" da criptografia, na medida em que compõem um conjunto de possíveis identificadores de uma pessoa humana e de seu comportamento.

Acima, mencionamos que a criptografia ponta a ponta protege o conteúdo da informação transmitida de um polo a outro. Mas o que é a criptografia ponta a ponta?

2.1.5 Criptografia Ponta a Ponta

A criptografia ponta a ponta, *peer-to-peer*, ou P2P, é considerada, hoje, à luz do atual estado da arte tecnológico disponível, um exemplo concreto de criptografia forte. Mas, antes, o que é a comunicação ponta-a-ponta (P2P ou *peer-to-peer*)?

Ponta a ponta é a troca de informações entre dispositivos ou sistemas em que ambos são capazes de operar tanto como provedores/servidores de informação como clientes/consumidores da informação.[19]

Felipe Jung Vilanova (2006) afirma que a maior parte dos serviços de Internet são distribuídos utilizando o modelo tradicional "cliente/servidor". Ele explica essa lógica comunicativa através da seguinte ilustração:

[18] Eletronic Frontier Foundation (EFF) – Surveillance Self-defense. Metadata. disponível em: <https://ssd.eff.org/pt-br/glossary/metadados>. Acesso em: 02 jul. 2022

[19] Disponível em: <http://www.wirelessdictionary.com/aw_dictionary_widget_wireless.asp>. Acesso em: 01 jul. 2022. Tradução livre do autor.

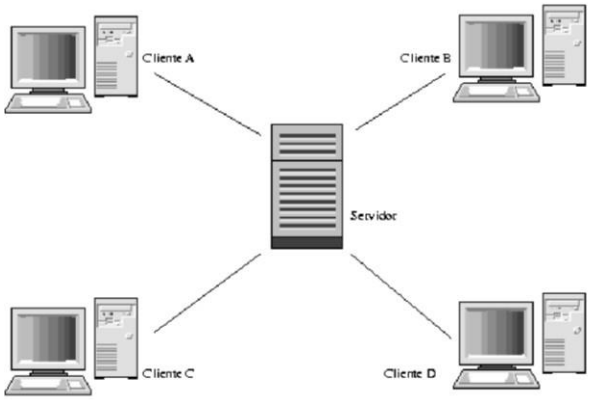


Figura 1.1: Modelo Cliente/Sevidor

Nesse modelo, "os clientes utilizam um protocolo de comunicação específico para acessar um recurso específico e grande parte do processamento envolvido no serviço ocorre no servidor" (Vilanova, 2006, p. 12).

Para Vilanova, a desvantagem desse modelo seria: i) a centralização, isto é, o processamento de informações num servidor central, o que introduziria um ponto central de falhas e; ii) a característica passiva do cliente, que, segundo o autor, "poderia efetuar pedidos a serviços, mas não poderia disponibilizar serviços a outros clientes" (Idem).

Ele explica que, diferentemente, o modelo ponta a ponta - *peer-to-peer* (P2P) expande a capacidade de os dispositivos individuais fornecerem serviços uns aos outros. Eis a ilustração utilizada pelo autor (Vilanova, 2006, p. 13):

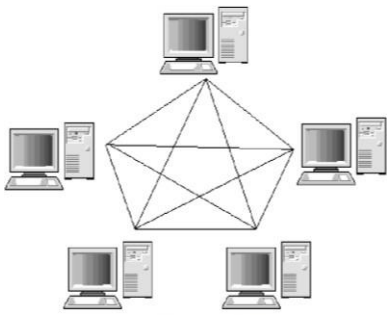


Figura 1.2: Modelo P2P

Conforme Vilanova explica, diferentemente do modelo anterior – cliente/servidor – as redes P2P não dependem de servidores centrais, disponibilizando uma rede plana e interconectada, de modo que as máquinas atuem como clientes e servidores, reciprocamente. Portanto, entende-se que esse modelo possui uma natureza descentralizada e distribuída de sistemas.

No caso, as redes P2P não estão ancoradas no armazenamento centralizado dos dados tal como no modelo tradicional. No modelo P2P, conforme ensinam Oleksandr Bodriagov e Sonja Buchegger, os "dados podem ser armazenados não apenas em um computador específico de um determinado proprietário, mas quase em qualquer lugar, por exemplo: computadores de amigos, pontos aleatórios da rede social, armazenamento externo de terceiros, etc" (2011, p. 01).

Essa amplificação na capacidade de armazenamento e transmissão de dados se dá porque os dispositivos da rede estão interconectados descentralizadamente e com reciprocidade de funções, independentemente de um servidor centralizado. O novo modelo introduz uma nova hierarquia comunicativa e de armazenamento entre os múltiplos pontos integrantes de uma rede.

Conforme explicam Dang et al. (2021), os nódulos passam a ser considerados iguais em sua potência de compartilhamento de dados. Portanto, pontos, agora, não mais sujeitos à distinção entre passividade e atividade. Pontos que concentram essas múltiplas funções, engendrando uma nova eficiência comunicativa maquínica.

Os pontos "conversam" entre si[20]. As máquinas retroalimentam-se. Redistribuem-se. Tornam-se aptas à produção de novas interações.

Mas onde entra a criptografia?

Bodriagov e Buchegger apõem um considerando a respeito da descentralização do armazenamento e da nova hierarquia comunicativa: "como o armazenamento externo geralmente não é confiável ou apenas semi-confiável, a

[20] Pertinente ao tema, ademais, sobretudo para o(a) leitor(a) curioso(a), seria a Análise nº 178/2020/VA, da ANATEL, contida no Processo Administrativo Processo nº 53500.060032/2017-46, que tem por objeto a Reavaliação da regulamentação visando diminuir barreiras regulatórias à expansão das comunicações Máquina-a-Máquina (M2M) e da Internet das Coisas (IoT). (BRASIL. ANATEL. *Análise nº 178/2020/VA. Processo Administrativo Processo nº 53500.060032/2017-46*. Reavaliação da regulamentação visando diminuir barreiras regulatórias à expansão das comunicações Máquina-a-Máquina e da Internet das Coisas. Conselheiro: Vicente Bandeira de Aquino Neto. Boletim de Serviço Eletrônico em 03/11/2020. Disponível em: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO6yRUAVOQVFdXLPeDggveAxcE4-tlqW-MeX1k1TbwBPtMONOL6_rN0i1fibBRqmPQdArtM-hTvIvm0w5MrjUv00>. Acesso em: 20 jun. 2022. Igualmente interessante seria refletir o desdobramento dessas novas modelagens comunicativas à luz da Teoria do Ator-Rede (TAR), em LATOUR, Bruno – *Reagregando o social: uma introdução à Teoria do Ator-Rede*. Tradução Gilson César Cardoso de Sousa. Salvador: EDUFBA – EDUSC, 2012. Para uma crítica da teoria, entretanto, ver GROSSETTI, Michel – *Les limites de la symétrie. À propos de l'ouvrage de Bruno Latour Changer de société. Refaire de la Sociologie*, Paris, La Découverte, 2006. Sociologies, Journal Open Edition, 2007.

criptografia desempenha um papel fundamental na segurança das redes sociais P2P" (2011, p. 01).

Dentro dessa perspectiva sobre "conversa" entre máquinas e, sobretudo, para a segurança dessa troca de "confidências", eis uma importante passagem colhida de um artigo escrito há dezessete anos, antes da criptografia ganhar fortíssimos impulsos como elemento protetivo da privacidade após os vazamentos de Snowden em 2013. No caso, ao comentarem as tecnologias de dupla utilização[21], Whitfield Diffie e Susan Landau tocam num interessante e sensível ponto de interseção entre o controle humano e o maquínico:

> À medida que a revolução da informação avançava – particularmente à medida que computadores começaram a "falar" cada vez mais para outros computadores – o argumento para o status do uso duplo melhorou lentamente. Telecomunicações entre humanos podem ser autenticadas por combinações de mecanismos mais ou menos informais: reconhecimento de voz, discagem dial-back, solicitação para saber a última checagem em uma conta, etc. Para alcançar grande segurança na comunicação entre computadores sem intervenção humana, a criptografia é indispensável (2005, p. 06).

Exclusões. Comunicações entre polos. Temporalidades: 24/7. 24/7. 24/7...7/24. 7/24....

É pertinente que a criptografia seja tão relevante para as tecnologias de comunicação e informação (TICs). Aparentemente, ela figura como um elemento da ordem da necessidade para com essas infraestruturas. Do necessário, do indispensável, justamente o oposto do contingente.

Nesse momento, peço novamente a paciência do(a) leitor(a) para um pequeno parênteses a respeito do conceito legal das *Tecnologias de Comunicação e Informação (TICs)* em nosso ordenamento, já que a criptografia é um ativo protetivo dessa infraestrutura. Talvez possamos espelhar uma pequena

[21] "Bens de dupla utilização são produtos e tecnologias normalmente usadas para fins civis, mas que também podem ter aplicações militares. De forma geral, dupla utilização pode referir-se a qualquer tecnologia que satisfaça mais de uma proposta a qualquer momento. Assim, tecnologias caras que em determinadas circunstâncias serviriam apenas para fins militares pode também ser usadas para beneficiar interesses civis, como é o caso do GPS." (TECNOLOGIA DE DUPLA UTILIZAÇÃO. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2022). Disponível em: <https://pt.wikipedia.org/w/index.php?title=Tecnologia_de_dupla_utiliza%C3%A7%C3%A3o&oldid=63671246>. Acesso em: 27 mai. 2022.

historicidade dessas tecnologias e vislumbrar outros direitos, criptos, que com elas possivelmente também "conversam".

Abre-se um ponto. Abre-se um parênteses.

Em 23 de outubro de 1991 foi publicada a Lei n.º 8.248, tendo por objeto dispor sobre a capacitação e competitividade do setor de informática e automação nacional. Em sua redação originária, o seu Art. 16 dispunha que, *verbis*: a introdução de novas tecnologias que digam respeito à automação de processos produtivos deverá ser apreciada por comissão paritária, de caráter consultivo, constituída de empregados e empregadores ou, na falta desta, pelos respectivos sindicatos.

Essa disposição foi vetada pelo então presidente Fernando Collor. Fundamento do veto: contrariedade ao interesse público. Eis as razões[22]:

> Apesar do caráter consultivo da comissão, prevista neste artigo, o dispositivo impõe novo obstáculo ao desenvolvimento tecnológico e à incorporação de novas tecnologias produtivas, num momento em que o País vem buscando, com empenho, eliminar tais barreiras.
> O exame prévio pela comissão poderá inibir a introdução de novas tecnologias poupadoras de mão-de-obra, dificultando a adoção de processos produtivos que venham contribuir para o aumento da competitividade do produto brasileiro. É importante salientar que, na ausência da citada comissão, conforme prevê o artigo em apreço, a introdução de novas tecnologias deverá ser apreciada pelos sindicatos, não estando claro se o papel dos mesmos seria também apenas consultivo. A inexistência da comissão, por outro lado, pode decorrer da mera recusa de uma das partes de nela participar.
> A proteção em face da automação, prevista no art. 7º, inciso XXVII, da Constituição Federal, deve ser conferida através de formas positivas, tais como o retreinamento para novas funções e a criação de novos empregos, e não por esquemas que possam redundar em perda de produtividade e competitividade para a economia nacional. Contrário ao interesse público.

Apenas quase uma década depois da revogação do originário Art. 16 é que foi acrescido à Lei n.º 8.248/91 um novo dispositivo. Na oportunidade, introduziu-se a expressão "*bens e serviços de informática e automação*", muito na linha da materialidade do originário Art. 16, vetado dez anos antes. Nessa nova ocasião, tratava-se do Art. 16-A, introduzido pela Lei n.º 10.176/2001 durante o governo FHC:

[22] BRASIL. Mensagem n.º 574, de 23 de outubro de 1991. Veto presidencial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/Mensagem_Veto/anterior_98/VEP-LEI-8248-1991.pdf>. Acesso em: 20 abr. 2022

> Art. 16-A. Para os efeitos desta Lei, consideram-se bens e serviços de informática e automação:
> I – componentes eletrônicos a semicondutor, optoeletrônicos, bem como os respectivos insumos de natureza eletrônica;
> II – máquinas, equipamentos e dispositivos baseados em técnica digital, com funções de coleta, tratamento, estruturação, armazenamento, comutação, transmissão, recuperação ou apresentação da informação, seus respectivos insumos eletrônicos, partes, peças e suporte físico para operação;
> III – programas para computadores, máquinas, equipamentos e dispositivos de tratamento da informação e respectiva documentação técnica associada (software);
> IV – serviços técnicos associados aos bens e serviços descritos nos incisos I, II e III.

No entanto, em 08 de dezembro de 2017, o governo Temer altera a redação do Art. 16-A através da Medida Provisória n.º 810, passando a empregar, em seu *caput*, não mais a expressão *bens e serviços de informática e automação*, mas a expressão *bens e serviços de tecnologias da informação e comunicação*, as famosas TICs, sob as quais articula-se fortemente a incidência da criptografia contemporânea, muito embora o conteúdo dessas tecnologias tenha permanecido o mesmo. Esse conteúdo ainda não foi encriptado, leitor(a). Já o seu referencial normativo desperta um grande talvez.

Isso porque a alteração foi a apenas do *caput*. Ou seja, o conteúdo material do que antes eram *bens e serviços de informática e automação* para, depois, passar a ser apresentado formalmente como *bens e serviços de tecnologias da informação e comunicação*, foi mantido integralmente (incisos I, II, III e IV do Art. 16-A). Apenas as formas jurídicas é que foram "historicizadas" conforme os novos tempos.

Por fim, a referida Medida Provisória foi convertida na Lei n.º 13.674 de 11 de junho de 2018, que manteve o texto do ato presidencial, restando vigente até o presente momento a definição tal como *bens e serviços de tecnologias da informação e comunicação (TICs).*

Fecha-se aquele ponto. Fechem-se os parênteses.

Voltemos à grafia cripta. Entre ~~pontos:~~ linha[23].

Alinhamentos comunicativos.

[23] "1. Ponto é aquilo de que nada é parte. 2. E linha é comprimento sem largura. 3. E extremidades de uma linha são pontos." (EUCLIDES – Os Elementos. Editora Unesp; 1ª edição. 2009, p. 97).

Souza e Mangeth comentam a criptografia ponta a ponta afirmando tratar-se de um tipo de técnica "na qual o conteúdo fica protegido desde o dispositivo que o envia até o que o recebe, de forma a impossibilitar que um servidor intermediário tenha acesso à comunicação" (2019, p. 76).

Com base no modelo tradicional de comunicação em trânsito da internet, a informação sai do polo remetente de forma cifrada, passa por um servidor externo aos participantes, momento em que os dados são decriptados ao chegarem e novamente encriptados ao saírem do servidor em direção ao destinatário, chegando, no ponto final, de forma inteligível. Nesse modelo, tanto os participantes como o servidor externo, usualmente da empresa intermediária, possuem as chaves da inteligibilidade. Trata-se de um modelo de encriptação parcial, de modo que em uma etapa do trânsito é passível de se verificar a inteligibilidade do fluxo informativo.

Diversamente, o modelo ponta a ponta de encriptação armazena as chaves exclusivamente nos polos participantes da comunicação, remetente e destinatário, conferindo maior segurança, pois não haveria o armazenamento das chaves também num terceiro ponto intermediário.

Essa modelagem comunicativa introduz uma tensão direta com as práticas jurídicas do Estado[24] calcadas na interceptação da comunicação em trânsito, na

[24] Por que adotamos, nesse estudo, a expressão "Estado"? No estudo sobre a criptografia e os *backdoors*, é comum afirmar, sobretudo nas fontes de estudo estadunidenses e europeias, que aquela técnica introduz uma tensão com órgãos públicos representativos da expressão "Law Enforcement". Essa expressão é ruim. Não há uma tradução adequada para tanto. Sua tradução literal seria "aplicadores da Lei". Ora, o que são aplicadores da Lei? Por exemplo, os particulares, no dia a dia, também aplicam a Lei. Nesse sentido, seria uma expressão muito vasta e, sinceramente, esquisita. Parece-nos que a expressão "Law Enforcement" busca designar, numa segunda interpretação, os órgãos públicos associados à segurança pública, o que poderia derivar nas polícias judiciárias, e também nos demais órgãos com competências persecutórias/requisitórias, atraindo, por exemplo, os Ministérios Públicos e também o próprio Poder Judiciário. Nesse sentido, seriam razoáveis as expressões "forças de segurança" e até mesmo "aparato persecutório-judicial". Muitas vezes utilizaremos essas duas expressões. O sentido que buscamos derivar delas é a representação de órgãos que tenham o poder de requisitar informações privadas (obviamente observados os ritos adequados) para formar alguma verdade jurídica. No entanto, também sabemos que diversos órgãos que não estão de algum modo relacionados à segurança, à persecução ou ao Judiciário, também podem entrar em tensão com o acesso às informações privadas. Vide, por exemplo, a Receita Federal, entre outros órgãos da Administração Pública. O que está em jogo no presente estudo são as prerrogativas jurídicas de qualquer órgão ou entidade estatal no que toca o acesso às informações privadas, agora blindadas tecnicamente pela criptografia. Não podemos impor amarras reducionistas. Isso porque cabe ao constituinte decidir, internamente, a quem caberá o acesso ao reino do privado. Cada unidade política no globo decide, conforme a sua soberania, qual é a organização interna do Estado e a distribuição dos poderes de acesso às informações tuteladas pela privacidade e/ou pelo sigilo. Se um ou outro Estado adota o desenho institucional "A" ou "B", sendo

medida em que blinda o acesso ao teor do conteúdo. Foi justamente a adoção desse modelo de criptografia pelos aplicativos mais populares de troca de mensagens que reacendeu o debate sobre a criptografia nos últimos anos, conforme veremos adiante.

Todavia, antes de ingressarmos nos termos do debate propriamente dito, passemos ao exame de outro instituto essencial ao escopo do presente trabalho: os *backdoors*.

2.1.6 O PARADIGMA *BACKDOORS* E O ACESSO EXCEPCIONAL

Assim como na criptografia, não há um conceito jurídico geral sobre *backdoors*. A previsão normativa desse instituto é setorial e decorrente do mesmo Ato n.º 77/2021 da ANATEL, mencionado no início do tópico 2.1:

> *Backdoor:* mecanismo não documentado contido no software/firmware do produto que possibilita acesso não autorizado ao equipamento. A presença de *backdoors* no produto final pode ser intencional ou acidental.

Apesar de a referida definição ser setorial e estar aquém da amplitude do debate em que os *backdoors* se inserem, ao menos ela possui uma importante divisão: a de que a presença de um *backdoor* pode ser intencional ou acidental. Essa diferença será mais bem explorada no tópico 3.3. No entanto, por ora, nos é necessária uma definição mais abrangente. Consultemos a doutrina.

Para Veridiana Alimonti, *backdoor* "se refere em geral a um mecanismo oculto, em *software*, em *hardware* ou via código malicioso, por meio do qual se acessa dispositivo de comunicação" (2019, p. 52). Enquanto Souza e Mangeth afirmam que *backdoor*s seriam "métodos integrados de contornar a segurança de um sistema" (2019, p. 74).

Ronald Deibert, ao comentar o instituto, afirma o seguinte: "estritamente falando, *backdoors* referem-se a métodos especiais de ignorar procedimentos de autenticação para acessar secretamente os sistemas de computação" (2013, p. 04).

A com freios e contrapesos mais intensos, e B, menos intensos, isso é outro problema a ser particularizado caso a caso. Considerando que o debate reside na tensão da criptografia com as diversas jurisdições existentes no globo, ainda é útil a boa velha generalização: Estado. Trata-se de uma premissa amplamente compartilhável.

Essas são definições mais estritas sobre *backdoors*. O elemento central nelas é a propriedade de superar/contornar um sistema de defesa de determinada infraestrutura para explorá-lo secretamente.

Essas concepções se alimentam da ideia de exploração da vulnerabilidade de uma infraestrutura. É justamente nesse sentido que Duane C. Wilson (2021) esclarece que *vulnerabilidade* é um termo de cibersegurança referente a uma falha num sistema que pode deixá-lo exposto ao ataque.

Digno acrescentar que Deibert (2013) também apresenta um conceito mais elástico, que ele enuncia como sendo o "*paradigma backdoors*", do qual compartilhamos, no sentido de que não seriam apenas as vulnerabilidades propriamente ditas contidas nas infraestruturas comunicativas e passíveis de exploração, ou ataque. Segundo Deibert, o paradigma também representaria o conjunto de políticas e práticas pelas quais os governos buscariam compelir, ou de outra forma, obter a cooperação de empresas do setor privado para fornecer o acesso aos dados que controlam. Para o autor, considerando que os governos procuraram monitorar as comunicações digitais para fins de segurança, o paradigma *backdoor* tornou-se a abordagem predominante.

No presente trabalho, também utilizaremos as palavras *backdoors* e *vulnerabilidades* como signos intercambiáveis, representativos de falhas[25] na segurança de um sistema para fins de exploração secreta.

Importante, ressaltar, ademais, uma breve taxonomia.

Os *backdoors*, como vimos, são vulnerabilidades na infraestrutura e passíveis de exploração. Essa exploração pode ser lícita ou ilícita. Lícita porque,

[25] Reconhecemos que a expressão "falhas na segurança", aqui representativa do conceito de *backdoors*, pode ser dogmaticamente e formalmente questionável dentro dos rigores da segurança cibernética. Isto porque existem outras considerações sobre o conceito, dentro das quais associam-se os *backdoors* muito mais a uma condição própria do sistema de segurança, não necessariamente uma falha, mas um risco que ao não ser devidamente remediado pode ensejar uma exploração indevida. Nesse sentido, ver, por exemplo, o conceito delineado pelo NIST, em tradução livre: "*Backdoor* - Uma maneira não documentada de obter acesso ao sistema de computador. Um *backdoor* é um risco potencial de segurança." <https://csrc.nist.gov/glossary/term/backdoor>. Acesso em: 7 set. 2022). Sob esta ótica, a palavra "risco" também poderia ser adequada para expressar um *backdoor*, pois estaria associada muito mais uma condição de possível exposição de um sistema de segurança a um eventual ataque ou acesso não autorizado.
Ademais, o instituto dos *backdoors* possui profundo diálogo com as disposições no MCI e na LGPD sobre segurança, tais como as medidas técnicas de segurança, o incidente de segurança, entre outros pontos a serem explorados nos tópicos 4.1, 4.2 e 4.3.

eventualmente, o próprio Estado objetiva explorar essas vulnerabilidades no intuito de cumprir suas prerrogativas constitucionais, por exemplo, interceptando a comunicação em fluxo para efetivar a segurança pública. O tradicional grampo telefônico, por exemplo, é um tradicional *backdoor* concedido ao Estado para que ele escute as conversas telefônicas.

Nesses casos franqueados ou em que se objetiva o franqueio ao Estado, muitas vezes iremos empregar as expressões acesso autorizado ou acesso excepcional. Isso se passa quando as vulnerabilidades são exploradas por atores autorizados constitucionalmente a tanto.

De outra sorte, veremos que essas mesmas vulnerabilidades franqueadas ao Estado também atraem a exploração por parte de terceiros mal intencionados, que não possuem, justamente, o acesso autorizado. Esse risco dificulta eventuais defesas pela criação de *backdoors* voluntários, propositais, funcionalizados ao Estado, pois eles poderão ser capturados por terceiros, desviados de sua função pública, conforme será exposto no curso desse estudo.

Antecipe-se que no tópico 3.3, iremos apresentar, ainda, como se formam as vulnerabilidades na infraestrutura, independentemente de elas serem ou não serem criadas para e em razão do Estado. Discutiremos as suas fontes, e quais atores possuem amplo conhecimento sobre essa dinâmica. Nessa linha, voltaremos àquela classificação empregada pela ANATEL sobre *backdoors intencionais* e *backdoors acidentais*, apontada mais acima, no início desse tópico.

Mas qual é a relação entre criptografia e *backdoors*?

2.2 A Relação entre Criptografia e *Backdoors*

Já pudemos apontar, em linhas muito breves, que criptografia e *backdoors* convergem como um tema de cibersegurança.

Em regra, *softwares*, *hardwares*, infraestruturas comunicacionais em geral, ao interagirem entre si, engendram vulnerabilidades. Riscos convidativos à exploração por terceiros mal intencionados. Nesse sentido, se convém afirmar que uma determinada infraestrutura possui uma *superfície de ataque* mais ou menos exposta à ação de terceiros, conforme o caso.

Sobre isso, Diego F. Aranha afirma que “a superfície de ataque de um sistema é composta dos pontos passíveis de intervenção pelo atacante, incluindo protocolos de comunicação, mecanismos de autorização, processos humanos, algoritmos criptográficos e suas implementações em softwares ou hardware” (2019, p. 27).

Muitas dessas vulnerabilidades sujeitas ao ataque, ou exploração secreta, podem ter a sua superfície de ataque minorada e, por vezes, suprimida, se adotadas uma série de medidas de segurança, tanto de ordem administrativa quanto de ordem técnica. No caso, uma relevantíssima medida técnica para proteger uma vulnerabilidade, reduzindo-se sua superfície de ataque, é a criptografia. Antagonicamente, no entanto, os métodos de enfraquecer a proteção de um sistema, seja pelo enfraquecimento dos padrões da criptografia, ou por outros meios de contorno para poder acessar um sistema, sub-repticiamente, também compõem o referido paradigma *backdoors*, representativo do conjunto de práticas para enfraquecimento da cibersegurança de um sistema.

São institutos inter-relacionáveis. À medida que a criptografia se popularizou, sendo aplicada massivamente nas interações do cotidiano, o acesso direto ao conteúdo das informações pelo Estado sofreu sérias dificuldades, pois as práticas jurídicas tradicionais de acessar uma informação privada deixaram de ser antagonizadas apenas pela blindagem jurídica fornecida pelos institutos do sigilo e da privacidade, os quais, como direitos, podem ser balanceados com outros interesses. Agora, no entanto, essas práticas também passam a ser antagonizadas por uma nova camada, uma blindagem de ordem técnica oferecida pela criptografia, menos flexível do que aquele balanceamento.

É diante da presença dessa técnica nas comunicações privadas em fluxo e/ou armazenadas que, não raro, se busca acessar os dados através de outros meios de contorno à criptografia: seja enfraquecendo-a, seja introduzindo *backdoors* nas infraestruturas que não sejam superados pela criptografia, seja até mesmo através da criação de outros métodos sub-reptícios de acesso aos dados, independentemente da criptografia, conforme veremos no tópico 3.4.

No entanto, antes de avançarmos e compreendermos os valores que realmente estão em jogo no debate, é necessário mapearmos as sutilezas históricas

do dilema criptográfico para que possamos visualizar o conjunto de atores e saberem que integram o debate e a dinâmica entre os envolvidos ao longo da História. Eis o próximo tópico.

2.3 O Desenvolvimento Histórico do Dilema Cripto

Conforme Landau (2017) recorda, a gênese da aliança entre computação e segurança nacional decorre da Segunda Guerra Mundial, momento em que a quebra de códigos pelos computadores se provou crítica à conclusão do conflito. Esse marco histórico, revelador de um importante subsídio computacional ao militarismo, diz respeito, segundo A. Ray Miller (2019), à quebra das comunicações do Terceiro Reich, que eram cifradas pela máquina Enigma[26], um antigo aparato de encriptação ao qual as forças alemães depositaram a sua segurança comunicativa.

Naquele momento, a decifração da comunicação nazista pelo trabalho da criptoanálise[27] marcou uma grande aliança entre a supervisão pública e as bases da computação na formação e consolidação das comunicações do século XX.

A capacidade de superar um sistema criptográfico não é de hoje. Thomas L. Burns (2011) explica que a criptologia integra o conceito de Inteligência de Comunicações (*Communications Intelligence* – COMINT) desde o período anterior à Segunda Guerra e, desde essa época, há uma intensa luta pela centralização de seu controle, antes disperso entre diferentes órgãos militares e agências civis para, depois, culminar com a fundação da própria *National Security Agency* (NSA)[28] em 1952.

[26] Diferentemente do que se pode imaginar, a máquina Enigma não era originariamente nazista, tendo sido inventada décadas antes pelo engenheiro elétrico Arthur Scherbius. (KRUH, Louis; DEAVOURS, Cipher – *The Commercial Enigma: Beginnings of machine cryptography*. Vol. XXVI, no 1 – Cryptologia, 2022, p. 1). Para maiores detalhes sobre a máquina, ver as Patentes US 1556964 A; US 1584660 A e US 1657411 A, em <https://ppubs.uspto.gov/pubwebapp/static/pages/landing.html>. Acesso em 15 nov. 2021. Para acesso às históricas publicações do caso nos jornais da época e com ilustrações do aparato, ver: i) <https://patentimages.storage.googleapis.com/41/1e/93/ea39ef52bf95db/US1556964.pdf>; ii) <https://patentimages.storage.googleapis.com/e2/82/35/6e8429192f63ae/US1584660.pdf>; iii) <https://patentimages.storage.googleapis.com/cb/ca/ff/d4d2e2e9adc7db/US1657411.pdf>. Acesso em: 15 nov. 2021.

[27] Para maiores detalhes técnicos sobre a criptoanálise da máquina Enigma, ver (BOROWSKA, Anna; RZESZUTKO, Elżbieta – *The cryptanalysis of the enigma cipher. The plugboard and the cryptologic bomb*. Computer Science. Vol. 15, no 4, 2014, p. 366).

[28] Agência de Segurança Nacional dos EUA. Nesse estudo adotaremos o acrônimo original: NSA.

A luta entre diversas instituições pela criptografia nos leva às origens do dilema cripto, mas para compreendermos a profundidade desse conflito devemos investigar o embrião das guerras criptográficas, o qual possui, segundo Landau (2017) quarenta anos de formação, bem como a sua evolução até os dias atuais.

Pois bem. Segundo o artigo *Keys Under Doormats* (Abelson et al., 2015) as guerras criptográficas tiveram início na década de 1970, nos Estados Unidos da América, tendo por objeto dois pontos centrais: i) se o setor de computação poderia exportar *hardwares* e *softwares* com encriptação forte e; ii) se a academia poderia publicar livremente pesquisas envolvendo áreas sensíveis da criptografia.

A mentalidade de que a ampla liberdade nas invenções e na pesquisa pudesse comprometer a segurança nacional sempre permeou o pós-guerra, sobretudo quando o objeto pesquisado e a sua família de ideias, tais como a computação e a criptologia, foram essenciais ao triunfo do conflito bélico que redesenhou a geopolítica global do último século.

Percebe-se o desenvolvimento de uma segunda etapa do dilema cripto, segundo o artigo supracitado, mas dessa vez durante a década de 1980, momento em que o embate envolvendo a criptografia evoluiu para um conflito de competências a respeito de quem controlaria o desenvolvimento da normatização dos padrões técnicos criptográficos a serem adotados pelas agências civis do governo: instituições públicas não militares e/ou não ligadas à Inteligência.

Caberia à NSA ou ao NIST[29] definir as normas técnicas relativas à criptografia para os setores do governo não subordinados à segurança nacional? No caso, segundo aponta o artigo *Keys Under Doormats* (Idem), foi o NIST quem recebera formalmente essa autoridade por meio da Lei de Segurança dos Computadores de 1987[30].

[29] Sobre o *National Institute of Standads and Technology* – NIST (Instituto Nacional de Padrões e Tecnologia), eis o que consta do seu próprio sítio eletrônico: *"The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time — a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany and other economic rivals."* (National Insitute of Standards and Technology, U.S. Department of Commerce, About NIST. January 11, 2022). Disponível em: <https://www.nist.gov/about-nist>. Acesso em: 08 mar. 2022. Uma instituição equivalente ao NIST em solo nacional seria a Associação Brasileira de Normas Técnicas – ABNT.

[30] Trata-se do *Computer Security Act* de 1987, mas publicado em 08 de janeiro de 1988, época em que o NIST era chamado de *National Bureau of Standards*. Para maiores detalhes sobre o referido

Ato contínuo, os anos noventa se iniciam com a Guerra do Golfo, com o início da internet comercial e, segundo Landau (2017), com as exigências do comércio por mais segurança nas comunicações para realização de seus negócios. Nessa linha, a autora afirma que um cenário de facilitação do acesso à criptografia por todos ao redor do mundo, indistintamente, não era atraente para a NSA. É que, nessa época, a criptografia ainda era uma técnica de domínio eminentemente militar.

No entanto, qual seria a solução a ser concedida ao mercado e às suas expectativas expansionistas num mundo pós-guerra fria? Por ora, construir-se-iam diferentes matizes de mercantilização dos produtos e sistemas com recursos criptográficos. E como isso seria realizado? Através da supervisão pública direcionada ao controle das exportações[31].

Riana Pfefferkorn afirma (2017) que se desenhou uma modelagem segundo a qual os equipamentos de uso militar permaneceriam controlados. Segundo a autora, os EUA enquadraram a criptografia, no plano internacional, como armamento de uso restrito, no intuito de exercer um rigoroso controle da exportação para outros países[32].

A motivação por trás do ato normativo era claramente geopolítica e calcada nos imperativos de Defesa. Conforme Pfefferkorn explica, grande parte do poderio estadunidense funciona por meio do complexo industrial militar-Inteligência, então, se outros Estados possuíssem a criptografia tão forte quanto a norte-americana, o serviço de Inteligência estadunidense passaria a encontrar grandes obstáculos.

ato normativo, ver: Public Law 100-235. *Computer Security Act of 1987*. Disponível em: <https://www.congress.gov/100/statute/STATUTE-101/STATUTE-101-Pg1724.pdf>. Acesso em: 20 abr. 2022.

[31] Interessante pensar que do ponto de vista de outros países, compradores de tecnologia, a supervisão pública deveria - se não o foi - ter sido realizada no eixo diametralmente oposto: o das importações.

[32] Para maiores detalhes do ato normativo, ver: FEDERAL REGISTER. *Presidencial documents. Administration of Export Controls on Encryption Products*. Vol. 61, No. 224. Disponível em: <https://www.federalregister.gov/documents/1996/11/19/96-29692/administration-of-export-controls-on-encryption-products>. Acesso em: 8 jul. 2021.

Landau (2017) explica que os controles de exportação[33] também se estenderam às chamadas tecnologias de uso duplo[34], aquelas com aplicações militares e civis, de modo que computadores ou sistemas comunicativos com propriedades criptográficas dependeriam de licença governamental para serem exportados, causando, assim entraves burocráticos aos potenciais mercadológicos da internet, o que não agradou a indústria.

A supracitada autora prossegue explicando que nos anos noventa, contudo, foi ofertada uma saída aos fabricantes: a exportação seria facilitada apenas para produtos e sistemas dotados de criptografia fraca. Pfefferkorn (2017), por sua vez, informa que algumas companhias americanas responderam a esse sinal através do oferecimento de duas versões de produtos no mercado: *i)* para usuários americanos/venda doméstica: padrões criptográficos fortes; *ii)* para outros usuários estrangeiros/exportações: padrões fracos.

Esse embate sobre a qualidade protetiva dos padrões criptográficos embutidos nos mais diversos dispositivos e a sua consequente proliferação transnacional através do filtro das exportações, nos anos noventa, ficou conhecido como a primeira guerra criptográfica[35], muito embora a NSA travasse as origens dessa guerra desde os anos setenta e a própria criptoanálise também fosse marcada, historicamente, pela proximidade ao militarismo e à Inteligência desde as sementes da Segunda Guerra Mundial.

Um primeiro elemento diferencial em relação ao passado do conflito criptográfico é que, nesse momento, anos noventa, não apenas os imperativos da Defesa[36] presidem o debate, mas também os fortes interesses mercantis, então animados pela abertura geopolítica, pós-guerra fria, contemporânea à promissora expansão da internet comercial.

---

[33] No caso, a criptografia foi enquadrada como tecnologia de uso duplo, nos termos do Acordo de Wassenaar, se submentendo a algumas matizes de controle de exportação por parte dos países signatários do acordo. Em linhas gerais, trata-se de um acordo multilateral para o controle das exportação de armamentos e tecnologias de uso dual. O Brasil não integra o pacto. Para maiores detalhes, ver o próprio website do Acordo em: <https://www.wassenaar.org/>. Acesso em: 20 abr. 2022.

[34] No tópico 2.1.5, já explicamos o que são tecnologias de uso duplo, nota n.º 20.

[35] Um embate, pensamos, que um investigador mais cético poderia sintetizar na seguinte pergunta: criptografia de quem e para quem?

[36] Emprego Defesa com "D" maiúsculo apenas para ressaltar o sentido de segurança nacional, militar, territorial, geopolítica e afins.

Um segundo elemento diferencial importante é que, em paralelo, o FBI adere ao debate. Pfefferkorn (2017) recorda que é nesse mesmo período dos anos 90 que se iniciam os clamores das forças de segurança internas de que o crime organizado blindar-se-ia através da criptografia. Conforme a autora ressalta, os segmentos de segurança pública do Estado nomearam essa ameaça de *going dark*.

Segundo relatório publicado pela UNESCO (2016), o argumento que associa as tecnologias criptográficas à supressão da efetividade das atividades de investigação podem ser sintetizadas na expressão *going dark*. Em rigor, a expressão *going dark*, que em tradução livre seria "ir às escuras", tornou-se a alegoria representativa de um embate entre, sobretudo, os órgãos públicos com competências investigativas e persecutórias representados pela expressão *Law Enforcement*[37] e os fabricantes e prestadores de serviço de TICs aptas a dificultarem, ou até mesmo suprimirem tradicionais práticas investigativas, em razão de certas medidas técnicas empregadas em seus bens e serviços, como a criptografia.

Contudo, o principal exemplo que tem capitaneado o debate representado pelo *going dark* tem sido os efeitos que a criptografia ponta a ponta produz sobre a prática estatal da interceptação legal das comunicações em fluxo, notadamente a blindagem técnica conferida pela encriptação sobre o acesso ao conteúdo informativo. A blindagem tecnocrática que a criptografia aporia sobre a infraestrutura comunicativa dificultando e/ou vedando o acesso do Estado ao teor das informações inseridas nessas infraestruturas.

Voltando. Pfefferkorn (2017) explica que nesse momento, meados dos anos noventa, o FBI direciona sua agenda ao Legislativo, conseguindo aprovar, em 1994, a CALEA[38], uma Lei que prevê a introdução de falhas propositais em diversos dispositivos comunicativos para fins de interceptação e monitoramento de comunicações privadas[39]. Um *backdoor* como norma de ordem pública.

[37] No tópico 2.1.6, especialmente da nota 23, explicamos os motivos pelos quais convertemos a expressão *Law Enforcement* na expressão Estado.

[38] Para maiores detalhes sobre o ato normativo, ver: (H.R.4922 - Communications Assistance for Law Enforcement Act). Disponível em: <https://www.congress.gov/bill/103rd-congress/house-bill/4922/text>. Acesso em: 18 dez. 2020.

[39] Em rigor, sobre a abrangência da CALEA, a autora explica que o ato, originariamente proposto para atingir todos os serviços de mensagens eletrônicas, recebera alguns limites, não abrangendo, por ora, todos os serviços da internet, tampouco os produtos com criptografia, embora tenha se expandido, após sua promulgação, para incluir dentro dos poderes de interceptação os provedores

Em paralelo, segundo Landau (2017), a NSA apresenta a proposta do *Clipper Chip* em 1993, uma proposta de contorno da encriptação para telefones, consistente no armazenamento das chaves de decriptação sob a guarda de agências governamentais, no entanto, o projeto recebera uma forte contestação da comunidade técnica[40] e fora abandonado.

Sucede que, no final dos anos noventa, o *e-commerce* havia decolado e o forte controle da exportação da criptografia não estava funcionando para os interesses empresariais, tal como apontado por Landau (2017). Os imperativos econômicos e concorrenciais acabaram por governar as necessidades.

Comentando sobre o referido momento histórico, a autora faz uma constatação de ordem prática: a de que a encriptação, além de ser central aos produtos informáticos, também a maior parte do mercado para esses produtos estava fora dos EUA. Afirmando, nesse sentido, que se as empresas estadunidenses não pudessem vender bens e serviços com recursos criptográficos, então outros países o fariam.

Diante dessa pressão econômica, Landau afirma que a primeira guerra criptográfica teria terminado em 2000 por meio do arrefecimento do controle das exportações para satisfazer a indústria e, interessantemente, avaliamos, também para a satisfação de uma parte do próprio do Departamento de Defesa estadunidense.

A modelagem resultante dessa abertura transnacional, segundo Landau, foi a de que as vendas para outros governos[41] e serviços de comunicações, assim como

---

de internet banda larga e alguns provedores VOIP. Nesse sentido, a referida Lei, no presente momento, ainda não prevalece sobre a criptografia, apesar de abranger outros serviços de comunicações ainda bastante presentes em nossa sociedade atual.

[40] Para uma crítica daquela época em relação ao projeto do Clipper Chip, ver <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>. Acesso em: 05 nov. 2020. Diversamente, no entanto, uma especialista que divergiu do consenso técnico do momento e sinalizou positivamente, já naquele momento, para o projeto foi Dorothy E. Denning. Para maiores detalhes, ver sua entrevista em (DENNING, Dorothy E. – *Interview, Oral History 424* - Conducted by Jeffrey R. Yost on 11 April 2013. Computer Security History Project Naval Postgraduate School, Monterey, CA. 2013, pp. 50-55). Disponível em: <https://conservancy.umn.edu/bitstream/handle/11299/156519/oh424ded.pdf?sequence=1&isAllowed=y>. Acesso em 10 nov. 2020.

[41] Correlatamente no Brasil, sobre aquisições pelo Poder Público, recentemente foram introduzidas disposições sobre dispensa de licitação para a aquisição de bens e serviços que possam afetar a segurança nacional envolvendo as áreas de: a) inteligência; b) segurança da informação; c) segurança cibernética; d) segurança das comunicações; e e) defesa cibernética. Trata-se da alteração do Decreto n.º 2.295/1997 pelo Decreto n.º 10.631/2021, que incluiu aquelas cinco hipóteses temáticas.

as vendas de sistemas customizados, permaneceriam sob estrita regulação, ao passo que as demais vendas não estariam mais subsumidas ao processo de licenciamento governamental.

Quanto a esse aspecto histórico do dilema cripto, é importantíssimo ressaltarmos um ponto que muitas vezes não é enfatizado: o de que o movimento para a revogação dos atos de controle viera do próprio Departamento de Defesa estadunidense, o qual "dependia cada vez mais do Vale do Silício para novas tecnologias" (Landau, 2017, p. 11). Sobre as razões que determinaram o fim da primeira guerra criptográfica, eis a opinião da autora:

> Em parte, essa decisão foi tomada em razão de custos: os sistemas de prateleira custavam consideravelmente menos do que os modelos customizados sob medida. De outra parte, também por razões de celeridade: empreendedores inovam para o mercado privado muitas vezes mais rápido do que inovariam para o Pentágono. Mas até certo ponto, a parceria militar com o vale do Silício emergiu das mudanças entre as alianças dos Estados Unidos. O compartilhamento de tecnologias criptográficas com aliados de longos tempos é uma coisa, mas fazer o mesmo com parceiros de coalizações ad hoc, tais como os da primeira guerra do golfo, é bem diferente. A coalizão deste ano pode muito bem conter os oponentes do ano seguinte. Um sistema comercial de prateleira seguro oferece todos os benefícios de comunicações seguras sem o risco que os sistemas sigilosos e projetados sob medida produzem" (Landau, 2017, p. 11).[42]-[43]-[44]-[45]

Não pensamos ser irrazoável a constatação de que a solução empregada no ano de 2000 costurou um jogo de ganhos recíprocos – *win-win*[46] – entre mercado e a comunidade da Inteligência. Isso porque, de um lado, os bens que a indústria estava interessada em exportar não mais seriam submetidos a algumas fortes

[42] Sobre essa passagem, recortamos e fazemos algumas considerações: "a parceria militar com o vale do Silício." Treze anos mais tarde o mundo conheceria o tamanho dessa parceria através de Edward Snowden.
[43] Novamente um recorte e considerações: "aliados de longos tempos". Seria a OTAN?
[44] Ainda sobre a passagem "parceiros de coalizões ad hocs, tais como os da primeira guerra do golfo". A coalizão da guerra do golfo diz respeito a uma aliança entre trinta e cinco países lideradas pelos EUA sob a Resolução 678 do Conselho de Segurança das Nações Unidas. Para maiores detalhes, ver: (Coalition of the Gulf War. In: WIKIPÉDIA, a enciclopédia livre. Under United Nations Security Council Resolution 678, a coalition of 35 countries, led by the United States, fought Iraq in the Gulf War from 1990–1991). Disponível em: <https://en.wikipedia.org/w/index.php?title=Coalition_of_the_Gulf_War&oldid=1100511272>. Acesso em: 09 jun. 2022.
[45] E, por fim: "A coalizão deste ano pode muito bem conter os oponentes do ano seguinte". A instabilidade geopolítica como condicionante à regulação da criptografia é um ponto que encontrará ressonâncias com a discussão travada no tópico 3.5.
[46] Segundo o Dicionário Cambridge, a expressão *win-win* representa uma situação ou resultado em que todos os envolvidos saem ganhando. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/win-win>. Acesso em 15 jun. 2022.

amarras do licenciamento governamental e, de outro lado, os bens e sistemas que interessavam à agência de Inteligência de sinais[47] – NSA – permaneceriam sob a supervisão pública da agência, tal como afirmado por Landau (2017). Entretanto, a autora recorda que a solução não agradou ao FBI, que contra-atacou novamente através da CALEA.

Um ponto digno de nota a respeito desse momento histórico – ano 2000 e o suposto fim da primeira guerra criptográfica com o arrefecimento das exportações – é que, apesar de a solução do primeiro dilema cripto ter desagrado ao FBI, a decisão fora avalizada pela comunidade de Inteligência, pensamos, um segmento muito mais opaco às prestações de contas democráticas.

Nesse momento, apesar de o FBI e as forças de segurança comuns domésticas continuarem a argumentar que estavam sendo blindadas pela tecnologia através da inacessibilidade do conteúdo comunicativo, isto é, indo às escuras – *going dark* – por outro lado, conforme observa Landau (2017), muito pouco foi dito sobre a Inteligência ter "ido às surdas" ou *going deaf*[48]. O futuro próximo diria os porquês.

Por essas razões, parece-nos bastante sóbria e realista as observações de Castro et. al, já em 2013, ao contestar o suposto fim da primeira guerra criptográfica e o suposto apoio do governo estadunidense à criptografia forte, tendo em vista que os vazamentos de Snowden apontaram para a introdução, deliberada, de *backdoors* em produtos comerciais e para o enfraquecimento de padrões de segurança por parte da NSA.

Comentando a referida presença de *backdoors* em diversos bens e serviços disponibilizados comercialmente por diversas empresas estadunidenses em escala

[47] A expressão Inteligência de sinais é a tradução da expressão "*signals intelligence*", frequentemente representada pelo acrônimo SIGINT. Eis a definição do objeto pela própria NSA em tradução livre: *"SIGINT é a inteligência derivada de sinais eletrônicos e sistemas usados por alvos estrangeiros, como sistemas de comunicação, radares e sistemas de armas que fornecem uma janela vital para nossa nação para as capacidades, ações e intenções dos adversários estrangeiros"* (NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE – Signals Intelligence (SIGINT) Overview). Disponível em: <https://www.nsa.gov/Signals-Intelligence/Overview/>. Acesso em: 01 jun. 2022.

[48] Ressalte-se que em 2005, antes dos vazamento de Edward Snowden, já se pôde conferir o reconhecimento entre quadros internos da NSA no sentido de não existir a possibilidade de a instituição ter "ido às surdas". No entanto, a publicação somente se deu em 2018. (THE INTERCEPT – *Is NSA Going Deaf? What is 'Golf Cart Reporting'?* - An Interview With REDACTED, on Oct. 19, 2055, in: The Intercept, Mar. 1, 2018).

transnacional, Castro et. al (2013) acendem uma legítima desconfiança sobre a retórica do mercado, de um lado, e o que possivelmente se passa nos bastidores, de outro.

Não custa recordar, ainda, que aqueles bens e serviços de prateleira - *comercial off the shelf* (COTS) –, liberados para exportação e para operacionalização transnacional, e supostamente dotados de fortes padrões criptográficos, foram destacados, lá em 2002, logo após a abertura para seu comércio exterior, como sendo estratégicos à NSA, encorajando-se as suas utilizações, conforme colhe-se do artigo *Keys Under Doormats* (Abelson et al., 2015).

Voltando à cronologia de eventos. Com o suposto encerramento da primeira guerra criptográfica, em 2000, através do arrefecimento do controle de exportações, como se desenvolveu a privacidade e as comunicações no período subsequente, no caso, a primeira década do Século XXI até 2013 quando o mundo conheceu os vazamentos de Edward Snowden?

Primeiramente, em 11 de setembro de 2001, os ataques terroristas ao World Trade Center inauguram um período em que, de um lado, proliferam-se atos normativos de exceção[49] para combate ao terrorismo e, de outro, exsurge um desenvolvimento tecnológico revolucionário: a chegada dos *smartphones* e a expansão da comunicação por dispositivos móveis, momento em que, segundo Landau (2017), a linha divisória entre trabalho e casa se embotam. A autora aponta para esse período como sendo a primeira etapa da revolução digital, demarcada pela crescente disponibilidade de redes rápidas.

Nessa primeira década, 2000-2010, entretanto, se operavam através da opacidade uma série de acordos informais[50] entre a NSA e empresas de TICS nos bastidores, enquanto, na esfera pública, por sua vez, os *smartphones* ainda não

[49] Quanto às legislações de exceção, o sentimento de medo e vingança suscitados pelos ataques do 09//11 facilitaram a passagem de uma série de medidas restritivas de direitos que fortaleceram demasiadamente o braço Executivo do Estado estadunidense, despontando como principal emblema jurídico-político o "*USA Patrioct ACT*", de 2001, tido como uma resposta emergencial ao terrorismo, mas que produziu nefastos efeitos extraterritoriais. Para detalhes sobre o ato normativo: (Public Law 107-56. US Patriot Act). Disponível em: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acesso em: 18 dez. 2020.

[50] A questão sobre os acordos informais será desdobrada e problematizada no tópico 3.4.

providos de fortes padrões criptográficos concediam uma mobilidade de captura e armazenamento de informações aos comuns, todos nós, sem precedentes.

Landau (2017) recorda que em 2010, por sua vez, o FBI intensifica suas demandas diante do novo cenário tecnológico, clamando novamente que as forças de segurança estavam indo às escuras - *going dark* - em razão das complexidades introduzidas pelas novas comunicações, incluindo a criptografia e a constante introdução de novos aplicativos no mercado. Nessa linha, a autora afirma que o órgão pressionava no sentido de que qualquer forma de criptografia possuísse algum meio de acesso excepcional, *backdoor*, de sorte que pudesse interceptar as comunicações quando munido de uma adequada ordem judicial.

E assim chega-se a 2013 e um novo marco histórico é traçado através dos vazamentos de Edward Snowden. Nesse momento, há uma guinada para a privacidade e, sobretudo, a criptografia passa a ser alocada como um importante ativo publicitário por parte das grandes empresas de tecnologia. Posteriormente, através de relatório publicado pela UNESCO pôde-se colher apontamentos reconhecendo a criptografia como um benefício empresarial: "um grande incentivo para as empresas usarem criptografia, imediatamente após o cumprimento dos regulamentos, é proteger a marca ou evitar danos à reputação por violação de dados" (Schulz e Hoboken, 2016, pp. 44-45).

É nesse contexto de clamor público pela privacidade que também podemos observar, por meio de análise de Landau (2017) sobre o período que se inicia em 2013, que o padrão *by default*[51] se estende para além das comunicações em fluxo (dados em trânsito), alcançando também a informação armazenada (dados armazenados), sobretudo em *smartphones*.

A partir desse momento, pós-Snowden, observa-se, em prol da privacidade, um forte alinhamento entre opinião pública e mercado, fortalecendo-se a legitimação de uma grande aposta do mercado: a criptografia *by default*. Um

[51] Segundo a European Data Protection Supervisor (EDPS), a proteção *by default* consiste, em breves linhas, no princípio segundo o qual uma organização (o controlador de dados) garante que apenas os dados estritamente necessários para cada finalidade específica do processamento sejam processados por padrão sem a intervenção do usuário. (EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) – *Privacy by Default*). Disponível em: <https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en>. Acesso em: 10 jun. 2022. É dizer: aplica-se uma proteção de ofício - pelo próprio prestador do serviço -, sem que o titular beneficiário necessite adotar uma postura ativa para efetivar a proteção fornecida pelo produto.

período em que as demandas do FBI vão perdendo força haja vista o pêndulo estar se afastando da segurança e pairando em favor da privacidade.

Conforme acrescenta Pfefferkorn (2017), o argumento das forças de segurança pública era no sentido de que suas campanhas seriam apenas um esforço de *preservação* do seu poder persecutório, e não uma pauta de *expansão* desse poder. A autora afirma que o tom era o de manutenção das prerrogativas constitucionais que as forças de segurança já possuiriam, de modo que elas estariam diante, apenas, de uma tradicional e constitucional prática, mas, agora, a ser aplicada em novas tecnologias de comunicação, contudo, estas se encontrariam num estado bastante refratário à presença do Estado em suas infraestruturas.

Essa era a linha de pensamento que o *establishment* da segurança pública possuía até setembro de 2014, quando o dilema criptográfico passou a ter como referência o conflito entre o FBI e uma mudança de postura tecnológica da *Apple*, em que esta tornar-se-ia o novo paradigma comunicativo dos últimos anos. E isso ocorreu quando a empresa anunciou o iOS-8 para o *iPhone*, segundo Pfefferkorn (2017). Ela afirma que a partir desse novo *software* a *Apple* forneceria criptografia forte, ponta a ponta e por padrão (*by default*) para *iPhones*, de modo que nem mesmo a empresa poderia contornar seu sistema de segurança. Em rigor, mesmo que as forças de segurança conseguissem um mandado para acessar o conteúdo de um *iPhone*, a *Apple* não conseguiria "destrancar" o dispositivo.

Digno recordar que, segundo Pfefferkon, antes dessa mudança na política interna da empresa, a própria *Apple* franqueava sua tecnologia à NSA, através de acordos informais denunciados por Snowden e, em relação ao FBI, colaborava tecnicamente com o órgão para que este pudesse acessar *smartphones* anteriores ao modelo iOS-8, entretanto, posteriormente, resolveu modificar as facilidades das parcerias com o FBI, introduzindo a criptografia ponta a ponta, *by default*, massivamente.

Pfefferkorn acrescenta uma importante consideração contextual: a de que a criptografia nunca fora comumente utilizada pelos consumidores em seu cotidiano. Segundo a autora, o interessado deveria ter a árdua tarefa de encontrar alguma ferramenta que se adequasse às configurações de seu dispositivo e então aprender um passo a passo de como instalá-la, configurá-la e usá-la corretamente, de modo

que o ato de encriptar dados sempre foi um procedimento desestimulante, não raro a maioria não se preocupar com isso.

Eis, então, que a *Apple*, de forma extremamente simples, funde a criptografia ao seu já popular *iPhone*, bastando ao usuário habilitar uma simples senha, ressalta Pfefferkorn. Assim, a autora afirma que milhões de pessoas estariam blindadas: deixava de ser necessária a tarefa de pesquisar uma tecnologia, baixar, instalar e aprender a usar a técnica. Agora não, a própria Apple fez todo o caminho para seus usuários através da *criptografia ponta a ponta by default*. E isso obviamente não agradou alguns segmentos do Estado, sentencia Pfefferkorn.

Então, o que as forças de segurança fariam?

O FBI e outros oficiais demandavam que a legislação impusesse às fabricantes de tecnologia a construção de *backdoors* na infraestrutura de seus produtos. Pfefferkorn afirma que a mentalidade era a do acesso de mão única, ou seja, a ideia de que apenas as autoridades públicas pudessem explorar as vulnerabilidades propositadamente inseridas nas infraestruturas, mas que essas mesmas vulnerabilidades, por sua vez, não pudessem ser acessadas por terceiros, criminosos.

No curso dessa segunda guerra criptográfica, a qual, segundo Landau (2017), seria uma guerra travada pelo FBI, e não pela NSA, é publicado em julho de 2015 um paradigmático estudo de especialistas técnicos. Seu objeto é justamente a análise da viabilidade técnica das pretensões das forças de segurança por acesso excepcional/backdoors nas infraestruturas comunicativas como meio de coletar informações privadas exclusivamente em favor do Estado: o artigo *Keys Under Doormats*[52].

Nesse estudo dos especialistas técnicos (Abelson et al., 2015), entre outros pontos a serem explorados adiante (tópicos 2.4 e 2.5) , informa-se que a introdução de vulnerabilidades propositais nos dispositivos e sistemas de comunicação em favor do Estado produziria uma insegurança apta a atrair terceiros atores, mal

[52] ABELSON, Harold et al. *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*. MIT Press. Cambridge, 2015. Disponível em: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>. Acesso em: 16 out. 2020.

intencionados, potenciais exploradores destas falhas de segurança, comprometendo, assim, a segurança digital de todos.

Alguns meses após a publicação do referido estudo, em 02 de dezembro de 2015, ocorre o ataque terrorista de São Bernardino/Califórnia e, diante do calor do momento, Pfefferkorn (2017) explica que um novo fôlego é conferido a pauta do FBI para enfraquecimento das medidas de segurança nas comunicações privadas no intuito de franquear o acesso excepcional às autoridades públicas.

A partir dessa tragédia surge o caso judicial *Apple* x FBI, envolvendo o trancamento do *iPhone* de um dos terroristas. Sobre o caso, Landau (2017) explica que após os terroristas matarem algumas pessoas, eles foram mortos num tiroteio, mas o FBI além de ter recolhido outras evidências, também coletou o *iPhone* de um dos criminosos. No entanto, o referido dispositivo estava bloqueado e a única pessoa que supostamente sabia a senha, o terrorista, estava morto.

Segundo Landau (2017), o FBI tentou forçar a *Apple* a desenhar um novo *software* que permitisse destrancar as proteções de segurança do dispositivo, mas a empresa se recusou. Por sua vez, conforme explica Pfefferkorn (2017), o argumento da empresa era o da impossibilidade técnica de acesso à informação em razão da criptografia forte presente no dispositivo: nem a própria fabricante teria as chaves da decriptação. Pfefferkorn acrescenta que o FBI interpretou a objeção da empresa, calcada na impossibilidade técnica de acesso ao conteúdo, como uma postura prejudicial à segurança pública, levando o caso ao Judiciário.

Contudo, diferentemente das dezenas de casos de desbloqueio de *iPhones* solicitados anteriormente ao Judiciário de modo sigiloso, dessa vez a agência não registrou esse específico caso sob o manto do sigilo processual, explica Pfefferkorn. A autora ressalta que o registro público do caso foi uma aposta, por parte do FBI, de que a opinião pública ratificaria seu pleito em razão da animosidade social suscitada pelo ataque terrorista.

No entanto, em 16 de fevereiro de 2016, a *Apple* publica uma carta aberta[53] aos seus consumidores, formulando um chamado à criptografia com argumentos muito próximos aos dos especialistas técnicos de que o enfraquecimento da

[53] COOK, Tim – A Message to Our Customers. The Need for Encryption – Apple. February 16, 2016. Disponível em: <https://www.apple.com/customer-letter/>. Acesso em: 20 abr. 2020.

criptografia introduziria uma insegurança digital e, consequentemente a disseminação de possíveis danos a todos os seus usuários[54].

Em razão da opção pela publicidade do processo feita pelo próprio FBI, a situação tomou grande repercussão, atingindo a opinião pública, mas esta ficou ao lado da *Apple*. Contudo, o mais interessante sobre o aparente fim desse conflito, ressalta Pfefferkorn, foi o fato de que o próprio FBI desistiu do processo, alegando que conseguira acessar o telefone através do auxílio de um terceiro[55] por meio da compra sigilosa de uma ferramenta forense alternativa.

Pfefferkorn acrescenta que apesar de a desistência do caso, por um lado, ter afastado a discussão sobre um possível constrangimento de que a *Apple* produzisse um *backdoor* em seus produtos, outras questões, por outro lado, ficaram sem respostas: i) ainda não há clareza de como o governo acessou o telefone; ii) não foi informado, à época, qual era a ferramenta, ou quem a fabricara, ou até mesmo qual vulnerabilidade/*backdoor* no sistema no iOS teria sido explorada. Nesse sentido, Pfefferkorn provoca: se existe um ponto fraco num sistema dito tão forte, quem conhece esse ponto frágil?

Importante contextualizar que a luta pelo acesso aos dados armazenados e às informações em fluxo não se operou apenas por tentativas no Legislativo. Pfefferkorn recorda que a luta pelo acesso aos dados também era direcionada ao Judiciário, de modo que meados de 2008 e até o final de 2015, o FBI solicitou e recebeu inúmeros mandados judiciais determinando à própria *Apple* o contorno da senha em *iPhones* pré-iOS 8. Recordando que esse contorno ainda era possível pela *Apple*, pois anterior ao modelo 8.

---

[54] No mesmo sentido, Susan Landau: "Por sua vez, o conselho geral da Apple e eu apresentamos uma narrativa diferente: num mundo de crescentes ciberataques, as comunicações e a informação requerem proteções mais fortes. Enfraquece-las é a última coisa que deveríamos fazer" (LANDAU, Susan – *Listening In: Cybersecurity in an Insecure Age*. Michigan: Grand Rapids, 2017, prefácio, x).

[55] Susan Landau, por sua vez, afirma que esse desfecho iluminou um mercado clandestino de ferramentas de dados forenses. (LANDAU, Susan – *Listening In: Cybersecurity in an Insecure Age*. Michigan: Grand Rapids, 2017, p. 143). Posteriormente, verificar-se-ia que a empresa israelense *Cellebrite*, uma gigante no fornecimento de ferramentas de extração de dados para forças de segurança ao redor do mundo, teria auxiliado no destrancamento do celular. (JAFFE, Adam - *The CEO of Cellebrite, the firm famous for helping the FBI crack into locked iPhones, says 'there is a race' to beat Apple from patching vulnerabilities it exploits*. Cellebrite. June 16, 2021). Disponível em: <https://cellebrite.com/en/the-ceo-of-cellebrite-the-firm-famous-for-helping-the-fbi/>. Acesso em: 16 jun. 2022.

Pfefferkorn afirma que o surpreendente nesse histórico é que todos esses provimentos judiciais ocorreram sob sigilo, secretamente, assim como reuniões privadas com empresas, ela endossa que ir aos tribunais sigilosamente teria levado o governo e as empresas a operarem fora da luz do debate público. A autora acrescenta que em razão dos processos não possuírem a devida publicidade, é possível que o governo dos EUA possua ordens de assistência técnica, sob sigilo, que forcem a *Apple* ou qualquer outra empresa a colaborar, advertindo, ainda, que pode existir todo um corpo técnico e jurídico secreto obrigando fabricantes de *smartphones* ou provedores de serviços a contornar a criptografia.

A opacidade adere ao debate como um inconveniente de difícil superação. Por sua vez, a questão da opacidade e da transnacionalidade e suas relações com a criptografia e os *backdoors* serão desenvolvidas no próximo capítulo, sobretudo nos tópicos 3.4 e 3.5. Por ora, passemos à síntese dos aparentes valores em conflito.

2.4 Os Valores em Conflito

Podemos colher do histórico do dilema cripto, sobretudo nos últimos anos, a constatação de que o emprego de fortes padrões criptográficos em bens e serviços utilizados massivamente na sociedade atual, notadamente o uso da criptografia ponta a ponta, opôs, conforme leciona Rafael Queiroz, "um desafio óbvio a possibilidade de interceptação ou à entrega do conteúdo de mensagens trocadas mediante ordem judicial." Isso porque "a característica constitutiva da criptografia ponta a ponta reside justamente na inacessibilidade do conteúdo" (Queiroz, 2019, p. 36).

Na perspectiva das forças de segurança, o debate é representativo de um embate - *trade-off* - entre, de um lado, privacidade[56] e, de outro lado, a segurança

[56] A privacidade é reconhecida como um Direito Humano. Na declaração da ONU de 1948, em seu Art. 12 consta: *"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."* Por sua vez, a Constituição da República de 1988 não menciona explicitamente a palavra "privacidade", adotando, entretanto, as expressões "intimidade" e "vida privada" em seu Art. 5ª, 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;* No mesmo sentido o Código Civil de 2002, que em seu Art. 21 prevê: *"A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."* Constam, ainda, como desdobramentos específicos da privacidade, em sede constitucional, as disposições sobre a tutela do domicílio (Art. 5º, XI) e sobre o sigilo das comunicações privadas em

pública[57]. O ex-diretor do FBI, James Comey (Landau apud. James Comey, 2017, pp. 164-165), por exemplo, endossa a narrativa em que a criptografia ponta a ponta e os dispositivos trancados representam grandes entraves para a investigação de condutas reprováveis, sobretudo terrorismo, tráfico de drogas e pedofilia. Nesse sentido, o lado da segurança vem defendendo que estaríamos diante de um dilema demarcado pelo *going dark*. Eles teriam "ido às escuras" por força da criptografia.

Como efeito desse suposto antagonismo de valores – privacidade vs. segurança - proliferam-se pedidos de autoridades para a construção de *backdoors*/vulnerabilidade que garantam o acesso excepcional aos dispositivos para fins de interceptação, ou outros meios de enfraquecer e/ou contornar o espectro protetivo conferido pela criptografia.

Entretanto, os especialistas em cibersegurança (Abelson et al., 2015) apresentam outro tipo de argumento ao analisarem as pretensões estatais de construção de *backdoors* nas infraestruturas para assegurar o acesso autorizado do Estado. No caso, eles advertem que as vulnerabilidades criadas para o acesso excepcional em favor do Poder Público trariam o risco de igualmente franquear

face da intromissão governamental (Art. 5º, XII), respectivamente: *XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; 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;* A "vida privada" também é prevista nos Artigos 14 e 17 do Pacto Internacional sobre Direitos Civis e Políticos - PIDCP, do qual o Brasil é signatário e foi internalizado no ordenamento nacional por meio do Decreto n.º 592, de 6 de julho de 1992, bem como no Art. 11 da Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), internalizada pelo Decreto n.º 678, de 6 de novembro de 1992.

[57] Como disposições relevantes ao exercício das prerrogativas estatais de acesso às informações tuteladas pela privacidade e pelo sigilo, despontam as previsões: i) do Art. 5º, XII, da CF/88, sobre interceptação, bem como a sua regulamentação pelo parágrafo único do Art. 1º da Lei n.º 9.296/96, que alcançou as infraestruturas informática e telemática, *verbis*: Art. 1º *A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática."*; ii) e do Art. 10, caput e §2º conjugados com os incisos II e III do Art. 7º, todos do MCI: 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.* § 2º *O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º ;* MCI, Art. 7º *O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;*

essas falhas à exploração por terceiros mal-intencionados. Assim sendo, para a comunidade técnica, não haveria um *trade-off* entre privacidade e segurança, mas um sopesamento entre segurança, de um lado, e segurança também do outro lado.

O estudo da comunidade técnica se concentra em três problemas principais que o acesso excepcional por meio de *backdoors* engendraria: i) a quebra das melhores práticas – *best practices* - instauradas nos últimos anos na internet; ii) um aumento na complexidade dos sistemas e isto seria ruim, pois conforme veremos no tópico 3.3, a complexificação dificulta a segurança do todo; iii) o acesso excepcional introduziria vulnerabilidades nas infraestruturas, muito convidativas à captura das chaves da decriptação por terceiros mal intencionados.

Para além do relatório estadunidense *Keys Under Doormats*, paradigma do argumento técnico, Souza e Mangeth (2019) também recordam a existência de outro marco de extrema relevância para a compreensão dessa tensão entre a criptografia e as demandas Estatais por acesso excepcional: a declaração do Grupo de Trabalho do Artigo 29, em que são reunidas as manifestações de diversas autoridades europeias de proteção de dados no sentido da indispensabilidade da criptografia para a confidencialidade e integridade dos dados, além de cominar uma valoração negativa à qualquer obrigação que vise reduzir a sua efetividade.

Nesse sentido, há um alinhamento entre o relatório *Keys Under Doormats*, de 2015, e a Declaração do Grupo de Trabalho do Artigo 29[58], de 2018, sob o argumento de que a fragilização intencional produzida pelos *backdoors* nas infraestruturas introduziria um estado de insegurança generalizado prejudicial à privacidade dos indivíduos.

Atualmente, há um forte alinhamento entre as advertências da comunidade técnica, a postura do mercado, sobretudo após os vazamentos de Snowden, e a doutrina da privacidade.

A forma como o dilema cripto é apresentado, bem como a sua relação com os *backdoors* para fins Estatais, associa a criptografia como um instrumento protetivo de Direitos Humanos, especialmente a privacidade e a liberdade de

[58] Para maiores detalhes, ver: ARTICLE 29 DATA PROTECTION WORKING PARTY. *Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU*. Bruxelas, 2018. Disponível em: <https://www.aepd.es/sites/default/files/2019-09/art29-statement.pdf>. Acesso em: 21 mar. 2022.

expressão, conforme enquadramento contido em relatório publicado pela UNESCO (2016).

No entanto, essa aliança entre valores humanos e uma técnica que tem por função tornar um objeto relativamente ininteligível, seja ele uma expressão humana ou diversa, também vem sendo desdobrada para novos domínios ao se resgatar a ideia de comunicações irrestritas como uma extensão da liberdade de expressão e comunicação. Uma premissa outrora reconhecida, conforme colhido em relatório publicado pela UNESCO (2016), pela Suprema Corte dos EUA, pelo *Bundesverfassungsgericht* alemão, bem como pelo Tribunal Europeu de Direitos Humanos.[59]

Eis uma passagem oportuna contida no supracitado relatório:

> Uma vez que as medidas estatais que restringem o uso e a implantação de encriptação tendem a ter o efeito de limitar as comunicações irrestritas, pode-se argumentar que o conceito de proteção efetiva dos direitos humanos tem que considerar a possibilidade de um cidadão se proteger por meio da tecnologia (...)" "Assim, a restrição da disponibilidade e eficácia da encriptação como tal constitui uma interferência na liberdade de expressão e no direito à privacidade, uma vez que protege a vida privada e a correspondência. Portanto, deve ser avaliada em termos de legalidade, necessidade e propósito (Schulz e Hoboken, 2016, p. 55).

Por outro lado, a problematização trazida pela criptografia, segundo essa abordagem, típica dos últimos anos do dilema cripto, é que, na medida em que ela opera como um escudo difuso das trocas e armazenamentos informativos, ela impede que o Estado acesse o conteúdo inteligível através de suas práticas tradicionais de formação da prova – v.g. interceptação -, ainda que sejam adotados os mecanismos de freios e contrapesos, isto é, os corolários do devido processo legal: supervisão judicial por mandado, ordem específica, proporcionalidade, interceptação controlada para fins específicos, etc.

E isso não seria necessariamente ruim, narra-se, pois outros valores, dito humanos, serão prestigiados. E, além disso, esse suposto decote de algumas práticas fiscalizatórias do Estado poderia ser compensado por outros meios. Então, qual

[59] No caso, constam os seguintes casos citados em relatório publicado pela UNESCO: i) no que toca a Suprema Corte dos EUA: New York Times Co. v. Sullivan, 376 U.S. 254 (1964) e Dombrowski v. Pfister, 380 U.S. 479 (1965); ii) No que toca ao Bundesverfassungsgericht alemão: BVerfG NJW 1995, 3303 (3304) e BVerfG NJW 2006, 207 (209); iii) e no que toca ao Tribunal Europeu de Direitos Humanos: Cumhuryiet Vafki e outros v. Turquia, CEDH 10.08.2013 - 28255/07; Ricci v. Itália, CEDH 10.08.2013 - 30210/06.

seria a solução franqueada ao Estado para que ele possa desempenhar seus poderes investigativos e fiscalizadores para além da flexibilização da criptografia?

A saída para o Estado tem sido ventilada através da mentalidade de que cabe ao Poder Público buscar *meios alternativos* de acesso aos dados sem que as medidas de segurança aplicadas sobre as TICs sejam enfraquecidas. Para tanto, recomenda-se a adoção de outras ferramentas e práticas encontráveis nesta Era de Ouro da Vigilância em que nos encontramos.

Ao comentar sobre os métodos investigativos na era da encriptação, Susan Landau (2017) sinaliza positivamente para o oceano de dados inaugurados pela revolução digital, as materialidades fornecidas pela Era de Ouro da Vigilância, afirmando que os desafios impostos pelas comunicações encriptadas e dispositivos seguros deve ser examinado dentro desse quadro mais largo.

Nessa linha, a autora sugere o recurso às utilidades investigativas proporcionadas pelos: *i)* metadados; *ii)* pela localização via GPS; *iii)* pelo monitoramento de redes sociais; *iv)* pelo acesso a dados armazenados em nuvem; *v)* pelo acesso à informação em dispositivos *smarts* caseiros, como a *smart* TV da *Samsung* ou o sistema *Alexa* da *Amazon*; *vi)* pelo compartilhamento[60] e integração de bancos de dados[61], entre outros meios.

[60] Para desdobramentos quanto ao ponto do compartilhamento de dados, relevantes são as ações diretas ADPF 695 e ADI 6649, ambas de Relatoria do Ministro Gilmar Mendes e pendentes de julgamento pelo STF. No caso, é discutido, à luz das disposições sobre privacidade e proteção de dados pessoais, a constitucionalidade de disposições do Decreto Federal n.º 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

[61] Stefano Rodotà, por exemplo, aponta para alguns riscos de violação à privacidade envolvendo a interconexão de bancos de dados. (RODOTÀ, Stefano – *A vida na sociedade da vigilância: a privacidade hoje*. Org. Maria Celina Bodin Moraes, Tradução Danilo Doneda w Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, pp.64-65; 99-100; 104 e 146). No mesmo sentido, Daniel J. Solove. (SOLOVE, Daniel J. – *Understanding Privacy*. Havard University Press, 2009, pp. 117-121). Recorde-se, ademais, que a proteção fornecida pela Lei Geral de Proteção de Dados não é estendida ao tratamento de dados envolvendo banco de dados para fins penais e processuais penais, por força dos limites hermenêuticos impostos por seu Art. 4º, III, "d", havendo, no momento, uma fragmentação, em nosso ordenamento, para essa sensível hipótese de tratamento, restando dispersa em outros atos normativos. Nesse horizonte, despontam algumas recentes disposições sobre segurança pública associadas ao tratamento de dados e, não raro, envolvendo justamente questões sobre bancos de dados: **I) Na Lei n.º 13.675/2018**, que criou a Política Nacional de Segurança Pública e Defesa Social (PNSPDS): a) o Art. 10, §4º - que versa sobre o acesso recíproco a bancos de dados pelos órgãos integrantes do Sistema Único de Segurança Pública (Susp) e; b) o Art. 35, IV – sobre banco de dados de perfil genético e digitais;
II) No Decreto n.º 9.489/2018, que regulamentou a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) instituída pela Lei citada anteriormente: o Art. 18, XI e o Art. 19, incisos I, "d", III e IX, todos dispondo sobre banco de dados de perfil genético e digitais;

Abre-se, no horizonte, uma nova proposta de sucedâneos investigativos-forenses.[62] Sucedâneos alimentados pelas próprias externalidades da infraestrutura digital. Novos métodos de formação probatória. Novos domínios para a formação de uma verdade jurídica e sua consequente distribuição de responsabilidades.

Na doutrina nacional, por exemplo, Aranha (2019), afirma que os métodos investigativos devem ser readaptados às características da infraestrutura comunicacional, recomendando que as autoridades busquem a coleta de metadados, a infiltração de agentes em comunidades e grupos de discussão, o acesso aos dados armazenados em nuvem, entre outras medidas.

Observando o presente tempo histórico, o autor pontua: "vivemos em uma era dourada da vigilância e esse é o verdadeiro desafio imposto pelo avanço da tecnologia aos esforços de investigação: como separar as fontes de informação útil e acurada em meio ao enorme volume de dados disponível" (Aranha, 2019, p. 34).

Muitos desses *meios alternativos de investigação* são endossados do outro lado do Atlântico pelo Grupo de Trabalho do Artigo 29[63], no entanto, ao

III) Decreto 10.822/2021 que, ao regulamentar o Art. 22 da Lei nº 13.675/2018 (Política Nacional de Segurança Pública e Defesa Social - PNSPDS), instituiu o Plano Nacional de Segurança Pública e Defesa Social para o período de 2021-2030. Uma disposição digna de nota decorrente deste ato infralegal diz respeito à ação estratégica n.º 07 contida em seu Anexo, à qual prevê a possibilidade do uso de "*machine learning*" para categorização e análise de bases de dados. Ressalte-se que a sua Lei de regência não previa o uso dessa ferramenta de automatização, em sendo, portanto, uma política adotada pelo atual governo federal em possível tensão com sua baliza legal. Eis a disposição: *"Ação estratégica 7: Padronizar tecnologicamente e integrar as bases de dados sobre segurança pública entre União, Estados, Distrito Federal e Municípios por meio da implementação do Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas - Sinesp e do Sistema de Informações do Departamento Penitenciário Nacional - Sisdepen e por meio dos dados obtidos do Sistema Nacional de Trânsito - SNT e de outros sistemas de interesse da segurança pública e defesa social, com o uso de ferramentas de aprendizado de máquina (machine learning) para categorização e análise."*;
IV) Decreto n.º 10.777/2021, que institui a Política Nacional de Inteligência de Segurança Pública, também regulamentando/densificando a Lei n.º 13.675/2018, que criou a Política Nacional de Segurança Pública e Defesa Social (PNSPDS);
V) Decreto n.º 10.778/2021, que aprova a Estratégia Nacional de Inteligência de Segurança Pública, igualmente regulamentando/densificando a Lei n.º 13.675/2018, que criou a Política Nacional de Segurança Pública e Defesa Social (PNSPDS);
VI) Lei n.º 14.069/2020, que criou o Cadastro Nacional de Pessoas Condenadas por Crime de Estupro;
VII) Lei n.º 14.232/2021, que institui a Política Nacional de Dados e Informações relacionadas à Violência contra as Mulheres (PNAINFO);
VIII) e mesmo disposições mais antigas, como a **Lei n.º 12.654/2012**, que introduziu a previsão sobre coleta de perfil genético como forma de identificação criminal.

[62] Susan Landau, por outro lado, apõe uma valoração positiva sobre o uso desses sucedâneos forenses através da exposição de alguns casos concretos. (LANDAU, Susan – *Listening In: Cybersecurity in an Insecure Age*. Michigan: Grand Rapids, 2017, pp.117-151

[63] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data*

comentarem tamanho estudo, Souza e Mangeth (2019) já expressam suas preocupações no sentido de que esses outros métodos possam atrair outros questionamentos do ponto de vista da privacidade.

Essas novas práticas às quais o Estado deve ir atrás, torná-las efetivas, essas filhas da Era de Ouro da Vigilância, certamente poderiam ser analisadas com maior espírito crítico à luz da privacidade. A introdução de novos métodos, novos meios e, sobretudo, de novos proprietários e gestores da produção desses meios, enfim, de novas formas de produção de verdades jurídicas é um fenômeno de extrema relevância, tacitamente integrante do conflito sobre a criptografia, mas que, aparentemente, não é substancialmente valorado na balança. Sob certas formas de produzir uma verdade se erigem ordenamentos. O debate aponta para essa saída ao Estado, mas através dela fecha-se uma de suas portas.

Mas avancemos para as partes finais desse capítulo.

2.5 Síntese Preliminar

O atual quadro de discussão apresenta uma imensa tensão entre as pretensões persecutórias-judiciais de jurisdições locais e mercadores de infraestruturas informativas e comunicativas dotadas de fortes recursos criptográficos. Foi justamente esse acirramento que inaugurou a discussão na jurisdição constitucional nacional através da ADPF 403 e da ADI 5.527, exploradas no tópico 3.1.

O foco desse embate tem sido vertical. Isto é, parece gravitar em torno da modelagem interna de cada país a respeito do grau de intensidade da intervenção pública e das formas dessas intervenções nas infraestruturas conectadas. As exigências estatais seriam no sentido de garantir alguma forma de presença nas infraestruturas conectadas, variando o modo, de país em país, como seria materializado, tecnicamente, essa demanda política.

Discute-se se serão adotados padrões criptográficos X, Y ou Z; se serão enfraquecidos ou fortalecidos certos padrões e outras proteções cibernéticas; se serão introduzidos *backdoors* de uma forma A ou de uma forma B; num ou noutro

in the EU. Bruxelas, 2018. Disponível em: <https://www.aepd.es/sites/default/files/2019-09/art29-statement.pdf>. Acesso em: 21 mar. 2022.

sentido técnico. Vontades políticas. Operacionalizações de ordem técnica. Avaliações de viabilidades técnica, mas que produzem direcionamentos políticos.

Nesse sentido, as discussões sob o prisma vertical e interno de cada Estado parecem oscilar entre as pretensões políticas de acesso aos dados pelas jurisdições locais, de um lado, e as pretensões de blindagens das TICs pelas ferramentas de cibersegurança, de outro. No entanto, pode ser pertinente ressaltar que os atores gestores das TICs operam em escala transnacional: o fluxo informativo e, muitas vezes, o seu armazenamento se dá no nível horizontal, na rede conectada, essa arena comum à qual as diversas jurisdições se condicionam e recondicionam para acessar os dados. A premissa da transnacionalidade pode introduzir uma complexa luta jurisdicional transnacional pelo acesso ao inteligível.

Ademais, é comum apresentar o debate, conforme retromencionado, sob premissas que valoram positivamente, de antemão, a criptografia, associando-a diretamente, e também de antemão, à proteção da pessoa humana, notadamente através dos institutos da privacidade, da liberdade de expressão e, agora, uma inicial extensão dessa última: as comunicações irrestritas e a integridade das infraestruturas informacionais comunicativas.

No entanto, em resgate ao que abordamos nesse capítulo, nós pudemos ver, ainda que em linhas sintéticas, que a criptografia é apenas uma técnica que protege a inteligibilidade de um objeto; que introduz uma seletividade comunicativa; e, assim, não sabe, por si só, o que protege. Também dispusemos que esse objeto pode ser uma expressão da privacidade humana, mas também pode ser qualquer outro símbolo comunicativo, dinheiro, bits, propriedades intelectuais, conversas entre máquinas, entre outros assuntos. Sensíveis assuntos.

Também vimos que, ao menos no Brasil, *tecnologias de informação e automação* passaram a se chamar, no plano jurídico, *tecnologias de informação e comunicação.* E pudemos constatar que a criptografia é essencial para garantir que as máquinas “conversem” entre si. Con-ver-sem ponto a ponto, seguramente. Um possível ativo, da ordem da necessidade, direcionada à integridade de certos modos interativos. Os tempos mudam, a representação de certos modos produtivos na linguagem também. Os interesses, nem tanto. Símbolos absorvendo símbolos e mudando de nome.

Ademais, visualizamos a evolução do dilema cripto à luz da História, do pós-guerra até o presente momento, revelando uma série de dinâmicas e atores que orbitam esse fenômeno, e que operam, não raro, através da opacidade, sobretudo através da luta pela influência dos padrões criptográficos ou mesmo por meio de acordos informais entre empresas e outros governos para acessar dados de forma alternativa, conforme se revelou no marco histórico traçado por Edward Snowden.

Mapeamos algumas diferenças entre as guerras criptográficas. Constatamos que a primeira guerra criptográfica foi iniciada na década de 1970 e finalizada, aparentemente, em 2000. Ela teve por objeto o controle de quem estabeleceria os padrões criptográficos e quais produtos e serviços utilizando recursos criptográficos poderiam ser comercializados, ressalte-se, transnacionalmente.

A segunda guerra criptográfica, que hoje permeia o debate, tem por objeto, generalizadamente, justamente o tal conflito entre forças de segurança internas do Estado e mercadores de infraestrutura tecnológica dotada de padrões criptográficos aptos a dificultarem as práticas investigativas tradicionais, mas mercadores que operam transnacionalmente.

Uma diferença importante entre os dois momentos, apontada por Landau (2017), é o fato de que após o final da primeira guerra criptográfica, em 2000, a Inteligência estadunidense avalizou a expansão da criptografia, de modo que, posteriormente, muitos oficiais sêniores desse *establishment* tomaram publicamente o lado da *Apple*. Ou seja, a semente da expansão criptográfica foi ratificada pela principal agência de espionagem do mundo, pela mais tecnicamente sofisticada parte do governo mais poderoso do mundo.

Entretanto, aparentemente, a autora valora positivamente essa postura da Inteligência. Segundo Landau, o que se observou no caso da *Apple* foi uma cisão entre, de um lado, as forças de segurança comuns, protagonizados pelo FBI e pelas polícias em geral, e, de outro lado, a comunidade da Inteligência, espelhando diferentes maneiras como essas instituições responderam à revolução digital em geral, de modo que caberia ao FBI se adaptar aos novos tempos.

Por outro lado, pensamos ser razoável algum grau de desconfiança e prudência aqui no hemisfério Sul, sobretudo do ponto de vista nacional e se também considerarmos a ampla história do debate. O fato de a criptografia estar sendo

ratificada pela principal agência de espionagem do mundo não é de se descartar. Isso não significa uma postura refratária à técnica. Não mesmo. Apenas que outras circunstâncias podem ser mais bem consideradas.

Não custa recordar que os vazamentos de Snowden revelaram, além dos acordos informais com as principais empresas de tecnologia que hoje se valem da criptografia forte, também uma série de *backdoors* nos mais diversos produtos e serviços utilizados no mercado e explorados pela Inteligência estrangeira.

Será que um *establshment* tão bem aparelhado e dotado de um imenso quadro de criptoanalistas teria renunciado a seus poderes de escuta e monitoramento de forma tão resignada diante desta segunda revolução digital e da expansão criptográfica ponta a ponta, *by default*, sobretudo quando antes havia uma colaboração opaca com as principais empresas com operação transnacional?

Por fim, constatamos que uma das soluções apresentadas pelos especialistas técnicos e pela doutrina para o aparato persecutório-judicial do Estado - e sua prerrogativa de formação da prova jurídica – não seria agir sobre as infraestruturas blindadas pela criptografia, mas buscar novos sucedâneos investigativos, novas formas de formação probatória através das alternativas fontes de dados encontráveis na consentânea Era de Ouro da Vigilância. Nas palavras de Landau: "à medida que as tecnologias de comunicação mudam os métodos de interceptação também devem mudar" (Landau, 2017, p. 119). Constatamos, por fim, que essa solução pelos meios alternativos poderia ser submetida a uma crítica oportuna, à luz da privacidade, através de um novo estudo com maiores fôlegos.

No próximo capítulo, primeiramente, discutiremos a recepção do debate pela jurisdição constitucional através da ADPF 403 e da ADI 5.527. Depois, abordaremos como se formam as vulnerabilidades/*backdoors*, suas fontes, independentemente dos *backdoors* criados artificialmente em favor do Estado. Também analisaremos como essas fontes de vulnerabilidades atraem a *expertise* de outros atores opacos e que possuem meios sub-reptícios de acesso os dados à revelia da criptografia. Abordaremos, igualmente, os desdobramentos da premissa da transnacionalidade e toda a insegurança que lhe envolve.

2.6 Post Scriptum

Recordemos, leitor(a), que a análise sobre o que é a criptografia desperta, inevitavelmente, uma família de ideias e propriedades que lhe orbitam. Ideias que ora são elementares da criptografia, ora lhe são conexas, tais como: comunicação; saberes técnicos; segredo; polos remetente e destinatário; pontos que trocam informações com outros pontos; terceiros indesejados que não devem compreender a informação; ininteligibilidade relativa do objeto; e, sobretudo, a seletividade da compreensão de um objeto. Selecionar, tal como decidir, sempre será um ato eminentemente político.

Mas por que cifrar? Por que tornar algo ininteligível? Por que embaralhar um objeto, escondê-lo?

Talvez, porque desejamos que certos conhecimentos não sejam acessíveis a todos. Porque desejamos ser compreendidos por uns, mas não por outros. Porque desejamos que certas confidências sejam seletivas. Apenas para alguns, não para todos. Porque "quem" pode saber sobre "o que", "quando" e "de que forma" pode ser arriscado e danoso. Nem todos podem ter as chaves. Nem todos devem tê-las. Porque nem tudo pode ser compartilhado. Conhecer pode ser perigoso. Trocar conhecimentos, mais ainda.

A própria noção de privacidade lançada pelo pioneiro Alan Westin se alimenta da premissa do que desejamos e do que não desejamos que outros conheçam. A vontade do que pode ser exposto e do que não deve ser exposto. Segundo Westin (1967), a privacidade seria a capacidade de um indivíduo (ou organização) decidir quando, como e até que ponto as informações pessoais serão divulgadas. Nessa estrutura não poderia estar contida a decisão sobre "o que", "o quando", "o como" e "a quem" uma informação será transmitida?

Na mesma linha, Stefano Rodotà (2008) sobre a privacidade como o controle das informações pessoais. Quando encriptamos um objeto, pensamos, introduzimos uma potência de controle sobre quem, quando e como outros sujeitos de conhecimento acessarão a inteligibilidade desse objeto. Quem tem as chaves, quando as terão, sob quais condições?

Criptografia, privacidade, segredo são conceitos inter-relacionáveis, que operam sob a função-mãe da exclusão/inclusão de informações segundo uma lógica de seletividades. Quem pode conhecer o que, quando e de que forma?

Esse “o que”, esse confidencial, essas confidências, esses objetos que desejamos expressar seletivamente, que desejamos compartilhar restritivamente pode ser qualquer coisa ao sabor do(a) leitor(a): um segredo íntimo, um vídeo pornográfico de vingança, uma escolha existencial[64], um código genético, um código-fonte, um sentimento humano expresso em palavras, uma figurinha de *WhatsApp*, um segredo de Estado, uma propriedade intelectual, uma conversa entre amantes ou entre máquinas, dinheiro digital, um bit, 1, 0, 1.0, 1.1, 0.1, 0.0, . . “.”

Escolhamos e reflitamos sobre como cada um desses objetos podem ser trocados numa arena transnacional chamada internet sob um regime temporal 24/7.

A criptografia apenas protege o que lhe é interno. Ela não sabe o que protege, tampouco apõe um juízo moral sobre o que é protegido. Ela possui uma neutralidade protetiva em relação ao seu objeto, mas não em relação aos sujeitos que lhe orbitam. Esses sujeitos podem representar diferentes modos de interagir e de habitar um mesmo lugar, um mesmo território, um mesmo planeta. Todos estes diferentes modos de habitar e produzir interações possuem as suas respectivas infraestruturas de suporte. Alguns modos não possuem mediação alguma. Quais são mais fortes? Por que não atravessarmos essa jornada com essas perguntas em aberto como um incômodo não resolvido, mas necessário?

Do ponto de vista do altar da ciência jurídica, uma infraestrutura de forças delegáveis em que os juízos de valor informam a sua essência, institutos dotados de neutralidades valorativas em relação ao seu objeto, mas igualmente munidos de uma potência de seletividades, são um convite àqueles que se lembram de que não existem valores postos de antemão.

[64] Sobre as escolhas existenciais, ver *RODOTÀ, Stefano. La vida y las reglas*. Entre el Derecho y el no Derecho. trad. Andrea Greppi, Trotta, Madrid, 2010. p. 127

3. CRIPTOGRAFIA E BACKDOORS COMO SABERES DA (DES)PROTEÇÃO DE INFRAESTRUTURAS E DO ACESSO AO INTELIGÍVEL

Nesta etapa, apresenta-se os reflexos da criptografia na jurisdição constitucional através das diferenças e semelhanças entre a ADPF 403 e a ADI 5.527. Em seguida, volta-se para a investigação das circunstâncias que podem se acoplar ao debate sobre a criptografia e os backdoors, mas que, aparentemente, não são devidamente enfatizadas. Primeiramente, através de uma breve análise das fontes dos backdoors nas infraestruturas conectadas para, em seguida, apresentar um conjunto de atores e de saberes que podem explorar essas fontes com maior facilidade e, assim, acessar dados e outras informações à revelia da proteção estabelecida pela criptografia, sobretudo através de privilegiados métodos sub-reptícios de acesso ao conteúdo inteligível. Nesse sentido, ao contextualizarmos essa dinâmica sob o prisma da transnacionalidade e da opacidade entre intermediários privados e outros governos, por força de acordos informais de colaboração, buscamos sinalizar para outras possíveis funções da criptografia, introduzindo uma tensão entre diferentes jurisdições e assimetrias de acesso a dados subordinados às infraestruturas interconectadas.

3.1. O Marco Brasileiro na Jurisdição Constitucional

A discussão sobre a criptografia na jurisdição constitucional brasileira ganhou relevância por meio de dois marcos jurídicos: a ADPF 403/SE[65], de Relatoria do Ministro Edson Fachin, ajuizada em 03 de maio de 2016 e a ADI 5.527/DF[66], de Relatoria da Ministra Rosa Weber, ajuizada poucos dias depois, em 16 de maio de 2016.

Contudo, cabe advertir, desde já, que essas duas ações não enfrentam diretamente as perplexidades dos *backdoors*, ao menos em termos formais de

[65] BRASIL. STF, ADPF 403 SE. Relator: Ministro Edson Fachin. 03/05/2016. JusBrasil. 2016. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500>. Acesso em: 20 mar. 2021.

[66] BRASIL. STF, ADI 5.527 DF. Relatora: Ministra Rosa Weber. 13/05/2016. JusBrasil. 2016. Disponível em: < https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282 >. Acesso em: 20 mar. 2021.

parâmetro – objeto. No entanto, ainda assim, é possível uma fecunda exploração entre os temas.

Inicialmente, para conhecermos as semelhanças e as pequenas diferenças entre as ações, bem como verificarmos a forma apressada como os respectivos objetos foram rapidamente ampliados para abranger a criptografia como um possível elemento a ser inserido em seus futuros dispositivos decisórios, é necessário, antes, identificarmos a base fática que antecedeu essas medidas.

Essa etapa nos permitirá contextualizar com maior rigor o debate, vislumbrando a disparidade entre o que foi propriamente postulado perante a jurisdição constitucional e, inadvertidamente, o modo como essa postulação vem sendo recebida pela Corte Suprema, isto é, ao menos, até o presente momento, nos termos do voto do Ministro Edson Fachin.

A base fática que precedeu as ações diretas, portanto, foi uma série de decisões judiciais oriundas de juízos criminais de 1ª instância, em que se determinou, no bojo da instrução processual penal, a suspensão da prestação do serviço de aplicações *WhatsApp* em todo o território nacional com base, segundo Souza e Mangeth (2019), em interpretações calcadas nos Artigos 10, 11 e 12 do MCI.

Eis as três decisões judiciais preexistentes ao protocolo das duas ações diretas. Detalhe para as datas das decisões e para os correspectivos remédios processuais adotados pelos próprios tribunais locais já à época do problema[67]:

> i) Em fevereiro de 2015, o MM. Juiz da Central de Inquéritos de Teresina/PI, no bojo da ação n. 0013872-87.2014.8.18.0140 determinou a interrupção dos serviços do referido aplicativo. Posteriormente, tal decisão foi suspensa liminarmente pelo Eg. Tribunal de Justiça do Piauí no Mandado de Segurança n. 2015.0001.001592-4;
> ii) Em dezembro de 2015, o MM. Juiz de Direito da 1ª Vara Criminal da Comarca de São Bernardo do Campo/SP, no bojo do procedimento de Interceptação Telefônica nº. 0017520-08.2015.8.26.0564, determinou a suspensão temporária das atividades do WhatsApp pelo prazo de 48 (quarenta e oito) horas em todo o território nacional. Contudo, tal decisão foi cassada por decisão liminar proferida pelo Eg. Tribunal de Justiça do Estado de São Paulo nos autos do Mandado de Segurança nº. 2271462-77.2015.8.26.0000.
> iii) Em 2 maio de 2016, o MM. Juiz Titular da Vara Criminal de Lagarto-SE expediu determinação a todas as operadoras de telefonia móvel e provedoras de internet no sentido de obstar a continuidade dos serviços do aplicativo em todo o

[67] As três referidas decisões foram colhidas da própria petição inicial da ADI 5.527, distribuída em 16 de maio de 2016.

> território nacional pelo prazo de 72 (setenta e duas) horas. Posteriormente, no dia 3 de maio, a suspensão do aplicativo foi revertida no âmbito do Eg. Tribunal de Justiça do Estado de Sergipe no Mandado de Segurança n. 2016.00.1.1089-9.

Posteriormente a essas decisões, foram ajuizadas as duas ações diretas. No curso delas, todavia, surgiu uma quarta decisão judicial que também teve por objeto a suspensão do *WhatsApp*. Trata-se da decisão da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ, de 19 de julho de 2017, também no mesmo sentido: bloqueio/suspensão do *WhatsApp.*

Mas por qual motivo esses juízos determinaram uma medida drástica como a suspensão de um serviço de troca de mensagens tão popular como o *WhatsApp*, ainda mais em todo o território nacional?

Porque ao determinarem que a empresa o fornecesse o conteúdo de comunicações privadas de usuários dessa plataforma, usuários investigados, os juízos se depararam com uma resposta impactante. No caso, a empresa opôs o argumento da impossibilidade técnica de disponibilização do conteúdo das comunicações. Isso porque a política de privacidade interna era ancorada na criptografia ponta a ponta, de modo que nem a própria empresa poderia acessar o conteúdo trocado entre os usuários investigados, semelhantemente ao conflito espelhado pelo *going dark* entre Apple e FBI, tratado no tópico 2.3.

O argumento da empresa é o de que, uma vez encriptados, somente os interlocutores podem ter acesso ao conteúdo trocado. Apenas os polos possuem as chaves da inteligibilidade do objeto. Supostamente, nem mesmo a *WhatsApp* conseguiria acessar o teor das comunicações privadas, pois as chaves de decriptação dos dados permaneceriam com os próprios usuários, remetente e destinatário[68].

Essas objeções de ordem técnica certamente não foram valoradas positivamente pelos juízos criminais, sobretudo se considerarmos que a possibilidade de se requisitar o acesso ao conteúdo privado por autoridades competentes é, por enquanto, possível no ordenamento nacional, desde que observados os mecanismos de freios e contrapesos, em sendo pertinentes, para

[68] Ressalte-se que o Superior Tribunal de Justiça possui precedente sobre a impossibilidade de aplicação de multa contra o *WhatsApp* pelo fato de a empresa não conseguir interceptar as mensagens trocadas pelo aplicativo e que são protegidas por criptografia de ponta a ponta. BRASIL. STJ - RMS 60.531-RO, Rel. Ministro NEFI CORDEIRO, Rel. Acordão Ministro RIBEIRO DANTAS, Terceira Seção, julgado em 09/12/2020, DJe 17/12/2020.

tanto, as disposições do Art. 5º, XII, da CF/88 combinada com o Art. 1º, parágrafo único da Lei 9.296/96[69] e do Art. 10, §2º[70] do MCI, as quais não foram objeto, por ora, de declaração de inconstitucionalidade.

Nesse sentido, é uma prática tradicional dos juízos criminais de todo o país, nos termos dessas fontes normativas, determinarem o acesso ao conteúdo de comunicações privadas, observados os limites constitucionais e legais.

Não custa recordar, ademais, que a criptografia ponta a ponta não era uma técnica de segurança originária da plataforma, fundada em 2009[71]. Pelo contrário, a adoção dessa espécie de criptografia forte foi adotada pela empresa em meados de 2014[72], enquanto nos EUA se desenrolava a segunda guerra criptográfica representada pelo embate entre *Apple* e FBI num contexto pouco posterior ao marco Snowden.

Por sua vez, as decisões brasileiras que determinaram a suspensão do serviço de aplicação são de 2015 e 2016, pouco posteriores à internalização do modelo ponta a ponta pela plataforma, além de se situarem num contexto de reação judicial a um argumento de ordem técnica de empresa que não praticava tamanha proteção da privacidade em sua origem. Não custa recordar, ademais, que a empresa fora comprada em 2014 pelo *Facebook*[73], outra empresa cujos vazamentos de

[69] Nessa hipótese, cuida-se da coleta/interceptação do conteúdo de informações em trânsito justamente no momento em que a comunicação ocorre entre os polos participantes envolvidos. Há uma contemporaneidade entre a comunicação e o acesso do Estado ao teor informativo trocado. Eis as disposições: CF/88, Art. 5º, 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; Lei n.º 9.296/96, Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça; Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

[70] MCI, 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; § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

[71] Informação retirada de: <https://pt.wikipedia.org/wiki/WhatsApp>. Acesso em: 20 abr. 2022.

[72] Informação retirada de: <https://www.theguardian.com/technology/2016/apr/05/whatsapp-rolls-out-full-encryption-to-a-billion-messenger-users>. Acesso em: 20 abr. 2022.

[73] Informação retirada de: <https://archive.nytimes.com/dealbook.nytimes.com/2014/02/19/facebook-to-buy-messaging-start-up/>. Acesso em: 20 abr. 2022.

Snowden demonstraram possuir acordos informais com órgãos estrangeiros como a NSA.

Ato contínuo, um dia após a terceira decisão que suspendeu o *WhatsApp*, no exato dia em que o próprio Tribunal de Justiça sergipano revertera a decisão, a ADPF 403 foi distribuída. Eis o pedido que foi formulado e, ao lado, o provisório quadro decisório da ação, nos termos dos votos dos Relatores:

PEDIDOS DA ADPF 403	ATUAL QUADRO DECISÓRIO DA ADPF 403
Ex positis, o Partido Popular Socialista requer: a) LIMINARMENTE, nos termos do art. 5º §1º da Lei 9.882/99, diante da grave violação ao direito à comunicação livre e irrestrita, seja deferida a liminar pelo relator de plano, ad referendum do Tribunal Pleno, para suspender os efeitos da decisão do Juiz da Vara Criminal de Lagarto, Marcel Maia Montalvão, nos autos do Processo nº 201655000183, bloqueou o aplicativo de comunicação WhatsApp por 72 horas, de forma que o mesmo volte a operar imediatamente; b) EM PROVIMENTO FINAL E DEFINITIVO, que seja julgado o presente pedido de arguição de descumprimento de preceito fundamental, para reconhecer a existência de violação ao preceito fundamental à comunicação, nos termos do art. 5º, inciso IX, com a finalidade de não mais haver suspensão do aplicativo de mensagens WhatsApp por qualquer decisão judicial;"	Após o voto do Ministro Edson Fachin (Relator), que julgava procedente o pedido formulado na arguição de descumprimento de preceito fundamental para declarar a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º, quanto do inciso III do art. 12 da Lei 12.965/2014, de modo a afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet; e do voto da Ministra Rosa Weber, que acompanhava o Ministro Relator, mas dava interpretação conforme à Constituição a esses dispositivos, pediu vista dos autos o Ministro Alexandre de Moraes. Ausentes, justificadamente, o Ministro Celso de Mello e, por motivo de licença médica, o Ministro Dias Toffoli (Presidente). Presidência do Ministro Luiz Fux (Vice-Presidente). Plenário, 28.05.2020 (Sessão realizada inteiramente por videoconferência - Resolução 672/2020/STF).

Por sua vez, poucos dias depois, ajuíza-se a ADI 5.527. Eis o mesmo modelo, pedidos e atual decisão da Ministra Relatora:

PEDIDOS DA ADI 5.527	ATUAL QUADRO DECISÓRIO DA ADI 5.527
a) A concessão de medida cautelar para suspender a vigência dos incisos III e IV do art. 12 da Lei n. 12.965, de 23 de abril de 2014, até o julgamento definitivo do mérito da presente Ação Direta de Inconstitucionalidade; b) No mérito, a declaração da inconstitucionalidade dos incisos III e IV do art. 12 da Lei n. 12.965/14, bem como a interpretação conforme do art. 10, §2º, a fim de que seja limitado o seu alcance aos casos de persecução criminal; c) Subsidiariamente, requer-se a adoção da técnica de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº.12.965/14, de forma a afastar a sua aplicação aos aplicativos de troca de mensagens virtual; ou, por último, que se dê interpretação conforme a tais dispositivos, condicionando-se, em consequência, a aplicação das sanções de suspensão temporária e de proibição do exercício das atividades somente após as sanções previstas no art. 12, I e II, mostrarem-se frustradas.	(i) julgo improcedente o pedido de declaração de inconstitucionalidade do art. 12, III e IV, da Lei nº 12.965/2014; (ii) julgo procedente o pedido de interpretação conforme a Constituição do art. 10, § 2º, da Lei nº 12.965/2014, a fim de assentar exegese segundo a qual "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º, e para fins de investigação criminal ou instrução processual penal"; (iii) julgo improcedente o pedido sucessivo de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº 12.965/2014, à compreensão de que não abrangido em sua hipótese de incidência o conteúdo que dele se pretende excluir; (iv) julgo parcialmente procedente o pedido sucessivo de interpretação conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014 apenas para (a) assentar que as penalidades de suspensão temporária das atividades e de proibição de exercício das atividades somente podem ser impostas aos provedores de conexão e de aplicações de internet nos casos de descumprimento da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos

	dados pessoais e ao sigilo das comunicações privadas e dos registros, (b) ficando afastada qualquer exegese que – isoladamente ou em combinação com o art. 7º, II e III, da Lei nº 12.965/2014 – estenda a sua hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação.

Nota-se que os pedidos da ADPF 403 são razoavelmente simples: *i)* cautelarmente: afastar a concreta decisão sergipana que suspendera o *WhatsApp*, mas que já fora cassada pelo próprio Tribunal sergipano, restando prejudicado o pedido e; *ii)* no mérito, afastar futuras decisões judiciais que venham a suspender o aplicativo, na medida em que seria uma violação ao preceito fundamental das liberdades comunicativas (CF, 5º, IX[74]).

Apesar de as ações diretas possuírem causas de pedir abertas, os pedidos não o são. E foi nesse sentido que o Ministro Fachin adotou uma premissa equivocada quanto ao objeto da ADPF 403, escapando à congruência necessária, senão vejamos:

> o objeto da presente arguição é (i) saber se é constitucional a ordem judicial de acesso por órgãos do Estado ao conteúdo de comunicações protegidas por criptografia, conforme previsão constante do art. 7º, II, do Marco Civil da Internet; e, em sendo constitucional, (ii) saber se a sanção prevista no inciso III do art. 12 do mesmo diploma legal pode ser aplicada pelo Poder Judiciário.

Não havia, nos pedidos da ADPF 403, a complexa e profunda análise acerca dos limites do acesso Estatal às comunicações privadas na internet, o que pressuporia uma verificação não apenas do Art. 7º, II, mas também a do Art. 10, §2º do MCI - base normativa para o acesso às comunicações privadas. Tampouco

[74] CF/88, Art. 5º, IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.

consta menção para que não mais fosse franqueado ao Estado o acesso às comunicações privadas em razão dessas infraestruturas encontrarem-se eventualmente protegidas pela criptografia ponta a ponta.

O pedido da ADPF 403 não objetivava reconhecer o ponto "(i)" considerado por Fachin: "saber se é constitucional a ordem judicial de acesso por órgãos do Estado ao conteúdo de comunicações protegidas por criptografia, conforme previsão constante do art. 7º, II, do Marco Civil da Internet."

O Ministro Fachin busca enfrentar, sem que haja pedido para tanto, o sentido e o alcance do Art.7º, II, do MCI. Isto é, os limites que o Estado deveria observar no que toca ao sigilo das comunicações privadas pela internet, condição esta que também possui profundo contato com o parágrafo único do Art. 1º da Lei 9.296/96[75], mas que também não fora atacado.

Diferentemente, o que se pede na ADPF 403 é que o Estado-juiz não mais suspenda o serviço da empresa *WhatsApp* em território nacional como mecanismo sancionatório e de coerção indireta, sobretudo em razão de interpretações judiciais equivocadas do Art. 12 do MCI.

Digno mencionar que o próprio parecer da Procuradoria-Geral da República afirmou que:

> O desiderato desta ADPF não é afirmar, tampouco infirmar, a eventual compatibilidade da tecnologia da criptografa de ponta a ponta com o marco regulatório brasileiro. Também não se trata de aquilatar se a implantação de vulnerabilidade (*backdoor*) é medida exigível ou se as autoridades públicas devem necessariamente se valer de outros métodos para a interceptação, a exemplo da técnica *man in the middle* (MITM).
> Cinge-se a controvérsia a saber se juízes podem bloquear, nacionalmente, o serviço de aplicativo *WhatsApp* ou se esta conduta viola preceito fundamental.

Cingindo a controvérsia à análise do bloqueio/suspensão do aplicativo, o parecer da PGR foi no sentido de que a medida seria desproporcional, pois existem alternativas menos drásticas, tais como a cominação de *astreintes*.

[75] Para uma defesa, na doutrina nacional, da inconstitucionalidade da interceptação legal em infraestruturas informáticas e telemáticas, tendo por objeto o Art. 1º, parágrafo único, da Lei n.º 9.296/96 e por parâmetro o inciso XII do Art. 5º da CF/88. (QUEIROZ, Rafael Mafei Rabelo. Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de troca de mensagens, *in*: DONEDA, Danilo e MACHADO, Diego. *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. pp.35-48).

Digno mencionar que à época do juízo de admissibilidade da ADPF 403, o então Procurador-Geral da República, Rodrigo Janot, ao analisar o pedido principal no sentido de que fosse afastada toda e qualquer futura decisão judicial de bloqueio ou suspensão do aplicativo, manifestou-se pela extinção da ação sem resolução do mérito por inépcia da inicial, expondo as seguintes razões:

> Em realidade, o arguente requer, por meio da ADPF, impedir decisões judiciais futuras que suspendam o programa de comunicação *WhatsApp* com o que interfere na atuação judicial e cria verdadeira imunidade jurisdicional em favor da empresa que explora essa ferramenta, a WhatsApp Inc., com sede na Califórnia, Estados Unidos da América. O pleito, em última análise, impossibilita ex ante que autoridades judiciais apreciem as peculiaridades de cada caso e apliquem a legislação pertinente, independentemente das circunstâncias, dos fundamentos e da causa de pedir, além de militar em favor de empresa específica de comunicação. Além disso, procedência do pedido implicaria provimento tipicamente normativo pelo Supremo Tribunal Federal, de aberta atividade legiferante positiva, uma verdadeira causa de impossibilidade jurídica de pedidos futuros, inadmissível de ser apreciado em arguição de descumprimento de preceito fundamental. Por consequência, a petição inicial deve ser indeferida, e extinto o processo sem resolução de mérito.

Por sua vez, a ADI 5.527 possui pedidos mais sofisticados do que os da ADPF 403, na medida em que se demanda uma discussão sobre a própria constitucionalidade de dispositivos do MCI, mas tampouco enquadra, em seu objeto, a criptografia. Nesta ação, não se discute, propriamente, a decisão judicial concreta e determinativa da suspensão de uma aplicação de mensagens, tal como delineado na ADPF 403.

Na ADI 5.527, os pedidos são mais ousados: objetiva-se, primeiro, declarar que as disposições normativas que preveem a sanção de suspensão temporária e a sanção de proibição de operação, incisos III e IV do Art. 12 do MCI[76], respectivamente, sejam declaradas inconstitucionais.

Subsidiariamente, pede-se que esses dois tipos de sanções estampadas nos referidos incisos III e IV: *i)* ou não sejam aplicadas aos serviços que tenham por objeto a troca de mensagens, o que, pensamos, constituir-se-ia num privilégio de

[76] MCI, 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: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

concorrência econômica em relação a outras aplicações e serviços comunicativos que concorrem na internet e/ou mesmo em outras infraestruturas, como a telefonia tradicional, por exemplo; *ii)* ou, se essas duas sanções forem passíveis de incidência, então que o sejam segundo um escalonamento: que sejam aplicadas somente após a incidência de outras medidas sancionatórias mais leves, como a advertência e a multa (incisos I e II do Art. 12 do MCI), criando-se, assim, um regime de subsidiariedade punitiva sem previsão legal.

Portanto, a discussão na ADI 5.527, em rigor, também está circunscrita ao sistema sancionatório previsto no MCI, não se estendendo ao sentido e ao alcance da tensão entre as comunicações privadas na internet dotadas de criptografia e as prerrogativas de acesso excepcional do Estado, ainda que essa temática possa subsidiar o debate.

Até poderíamos cogitar, por outro lado, que essa discussão estaria presente dentro do pedido de interpretação conforme do Art. 10, §2º ventilado na ADI 5.527 (pedido "b", retromencionado). No entanto, apenas se pede que, nessa hipótese, o acesso às comunicações privadas na internet seja limitado aos casos de persecução penal, em sendo afastado o acesso para fins cíveis. Igualmente, não se pede a inconstitucionalidade do acesso às comunicações privadas, tampouco que esse acesso investigativo seja remodelado à luz da incidência da criptografia sobre a infraestrutura telemática.

Há uma diferença, portanto, entre analisar a (in)constitucionalidade dos bloqueios como medida sancionatória[77] e analisar a constitucionalidade da

[77] A análise sobre a (in)constitucionalidade dos bloqueios, no entanto, é realizada por Carlos Affonso de Souza e Ana Lara Mangeth. No caso, adverte-se sobre as medidas que afetam diretamente a infraestrutura da rede, demonstrando grande preocupação com a naturalização de decisões judiciais como as que precederam as ações diretas, pouco cautelosas, na medida em que, ao operarem diretamente sobre a infraestrutura da rede, estendem o seu raio de alcance e potencial dano para além dos envolvidos. Para tanto, recordam o princípio da "inimputabilidade da rede" enunciado pelo Comitê Gestor da Internet - CGI, além das potenciais violações ao Art. 13, item 3 do Pacto de San José da Costa Rica e à Resolução do Conselho de Direitos Humanos da ONU de 27 de junho de 2016. Ademais, os autores avançam e afirmam que decisões como tais não podem ser extraídas do próprio MCI. Pelo contrário, essa fonte normativa vedaria decisões judiciais que determinem o bloqueio das aplicações diretamente na infraestrutura. Os autores explicam, através de uma interpretação sistemática entre o inciso III do art. 12 e o caput do art. 11, que a referida sanção de suspensão de atividades possui aplicabilidade bastante restrita. É de se indagar: quais atividades podem ser suspensas? Os autores respondem que somente podem ser suspensas aquelas atividades tipificadas no caput do Art. 11: coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de internet. Vale a íntegra da passagem: *"o artigo 12, III, do Marco civil da internet, apenas permite a suspensão das atividades listadas no caput do artigo 11, o que é completamente diferente de um bloqueio na infraestrutura. As atividades definidas*

criptografia ponta a ponta aplicada em comunicações privadas, de modo que esse design possa, de antemão, dificultar, ou mesmo afastar, a prerrogativa de acesso ao conteúdo dos dados pelo Estado. O presente trabalho busca abordar a problemática envolvendo a criptografia, não os eventuais equívocos judiciais a respeito da interpretação do sistema sancionatório do MCI como meio de coerção indireta de particulares, tema este que compõe, justamente, o correto objeto dessas ações.

Todavia, considerando o fato de que, além da causa de pedir ser aberta, a criptografia também fora a justificativa técnica oposta pela empresa *WhatsApp*, deflagrando a reação do Judiciário nacional mediante decisões suspensivas das aplicações de internet, é pertinente que ela seja ventilada no bojo das deliberações entre os Ministros e, nesse sentido, o voto de Fachin, apesar de avançar demais em seu dispositivo decisório, apresenta pontos relevantes em sua fundamentação, antecipando possíveis discussões sobre o tema no Plenário do STF.

Para o relator da ADPF 403, por exemplo, o MCI autoriza apenas o fornecimento de informações não protegidas por sigilo, os chamados metadados,

---

no artigo 11 do Marco civil da internet que podem ser suspensas são as seguintes: 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. Assim, a Lei apenas permite a suspensão das atividades de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet não autorizando a total indisponibilidade do aplicativo ou site, o que ocorreria com bloqueio propriamente dito. A suspensão da coleta, armazenamento, guarda e tratamento de registros, de dados pessoais, ou de comunicações por provedores de conexão e de aplicações de internet representa uma punição para o provedor que não respeita os deveres previstos nos artigos 10 e 11 do Marco civil da internet, uma vez que a coleta desses dados é fonte essencial de receita nas atividades econômicas exercidas por provedores que oferecem serviços na internet" (Souza e Mangeth, 2019, pp. 81-82). Aparentemente, os autores espelham uma preocupação de ordem geopolítica, porque o bloqueio diretamente na infraestrutura da internet pode afetar a comunicação de outros países, cujas respostas podem ser pelo desvio de suas conexões para outras rotas, não bloqueadas, denunciando, assim, os problemáticos efeitos extraterritoriais de uma decisão local. (SOUZA, Carlos Affonso e MAGETH, Ana Lara. A Criptografia entre Flexibilização e Bloqueio de Aplicações: lições internacionais e a experiência brasileira, *in*: DONEDA, Danilo e MACHADO, Diego. *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. pp.79-83). Ademais, ressalte-se a convergência entre as referidas lições doutrinárias e a parte final do voto da Ministra Rosa Weber, relatora da ADI 5.527: *"julgo parcialmente procedente o pedido sucessivo de interpretação conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014 apenas para (a) assentar que as penalidades de suspensão temporária das atividades e de proibição de exercício das atividades somente podem ser impostas aos provedores de conexão e de aplicações de internet nos casos de descumprimento da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, (b) ficando afastada qualquer exegese que – isoladamente ou em combinação com o art. 7º, II e III, da Lei nº 12.965/2014 – estenda a sua hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação*."

referentes ao usuário e à utilização do aparelho. Por sua vez, o *conteúdo* das informações trocadas entre os usuários estaria completamente tutelado pela criptografia, alinhando-se ao que esboçamos no tópico 2.1.4.

O interessante no voto do relator é que ele apresenta, ainda, considerações sobre o suposto *trade-off* entre comunicações privadas tuteladas pela criptografia e a efetividade de práticas tradicionais da segurança pública, espelhando, em muito, a argumentação dos especialistas técnicos – tópico 2.4 – no sentido de que a introdução de vulnerabilidades para garantir o acesso excepcional seria mais prejudicial do que o eventual uso da criptografia pela criminalidade como um possível escudo de suas práticas:

> (...) embora haja o risco de que criminosos se utilizem de mensagens criptografadas para acobertar suas ações, o risco causado pelo uso da ferramenta ainda não justifica a imposição de soluções que envolvam acesso excepcional ou que diminuam a proteção garantida por uma criptografia forte" (BRASIL. STF, ADPF 403 SE. Relator: Ministro Edson Fachin.- JusBrasil. 2017)

Também é relevante o ponto em que o voto tenta definir contornos conceituais e finalísticos para a criptografia, ressalvando, ainda, que o anonimato não se confunde com ela:

> A criptografia é um meio de proteger a privacidade das pessoas no ambiente digital. A criptografia nada mais é do que um processo matemático de conversão de mensagens, informações ou dados que os torna ilegíveis por qualquer pessoa a não ser o destinatário da mensagem.
> A criptografia serve, assim, para proteger o conteúdo da mensagem, mas ela não protege os chamados "metadados", como, por exemplo, o endereço de IP. O anonimato visa, precisamente, a evitar a identificação desses dados. Exemplos de tecnologias empregadas para esse fim (proteção do anonimato) são a criação de redes privadas virtuais (VPNs), serviços proxy, e redes peer-to-peer (A/HRC/29/32, par. 7, 8 e 9).

A premissa do Relator é a de que a criptografia seria direcionada ao conteúdo da informação, ao passo que o anonimato, aparentemente, seria direcionado aos metadados (ex: IP, hora da mensagem, etc.), os quais não estariam protegidos pela criptografia.

O problema, pensamos, é que são justamente os metadados que contribuem substancialmente para a formação de perfis humanos[78] e os padrões de

[78] Para uma visão sobre a genealogia de métodos de formação de perfis humanos com base na mobilidade do corpo e para fins de rastreamento humano: (CHAMAYOU, Grégoire. *Patterns of*

comportamento, hipóteses que entram em fricção direta com a autonomia privada. O Ministro Fachin sinaliza para o anonimato[79], mas não nos parece ter estendido a proteção aos metadados. O ponto pedirá maiores estudos, oportunamente.[80]

Por fim, importante recordarmos que uma coisa é a (in)constitucionalidade dos bloqueios como medida sancionatória[81], outra é a constitucionalidade da

---

life: a very short history of schematic bodies. The Funambulist, [S. l.], v. 57, p. 1-1, 4 nov. 2014). Disponível em: <https://thefunambulist.net/editorials/the-funambulist-papers-57-schematic-bodies-notes-on-a-patterns-genealogy-by-gregoire-chamayou>. Acesso em: 24 mar. 2022.

[79] Para reflexões sobre o anonimato na internet: (MACHADO, Diego e DONEDA, Danilo. *Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no Direito Brasileiro*. Revista de direito civil contemporâneo, v. 7, n. 23, p. 95-140, abr./jun. 2020. Revista dos Tribunais, 2020). Para uma defesa do anonimato através da análise de aspectos procedimentais: (CUNHA E MELO, Mariana. *Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças ao direito à privacidade no Brasil*. 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf>. Acesso em: 1 jun. 2022. Por sua vez, para uma perspectiva da aplicação do anonimato ao contexto da Internet das Coisas - Internet of Things/IoT: (MAGRANI, Eduardo Jose Guedes e ABRAHÃO, Luiz QUEIROZ. Internet das Coisas Anônimas (AnIoT): Considerações Preliminares, *in*: DONEDA, Danilo e MACHADO, Diego. *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. pp.165-182). Para uma crítica ao combate das *fake knews* através de medidas que flexibilizam o anonimato online, ver: <https://www.jota.info/coberturas-especiais/liberdade-de-expressao/mirando-em-fake-news-e-acertando-em-vigilancia-24062020>. Acesso em 10 ago. 2020. No mesmo sentido: <https://politica.estadao.com.br/blogs/fausto-macedo/o-debate-sobre-o-anonimato-no-caso-do-sleep-giants-brasil/>. Acesso em: 15 dez. 2020. Igualmente interessante, por outro lado, também é verificar a subsunção de algumas tecnologias do anonimato na rede ao sistema de patentes. Nesse sentido, apenas exemplificativamente, ver em <https://ppubs.uspto.gov/pubwebapp/static/pages/landing.html>. Acesso em: 20 abr. 2022.: ***i)*** A **patente US 9710671 B1** concedida à *Amazon Technologies, Inc*, envolvendo anonimização de dados como mecanismo contributivo às novas hierarquias comunicativas dos sistemas computacionais, descentralizadas, conforme esboçado sumariamente no tópico 2.1.5; ***ii)*** A **patente US 10743178 B2** concedida à *Apple Inc*., envolvendo anonimização e localização geográfica de dispositivos móveis/usuários; ***iii)*** A **patente US 7765152 B2**, que dispõe sobre sistemas e métodos para detectar oportunidades de negociação nos mercados financeiros, mantendo o anonimato dos envolvidos, concedida à antiga *Codestreet, LLC*, que por sua vez foi comprada pela *Tradeweb Markets LLC*, uma das expoentes no mercado financeiro global de renda fixa e derivativos. Neste último sentido <https://www.tradeweb.com/newsroom/media-center/news-releases/tradeweb-markets-llc-acquires-codestreet-llc/>. Acesso em: 20 abr.2022.; ***iv)*** A **patente US 11194866 B2** concedida ao *Google*, e que dispõe sobre sistemas e métodos para conteúdo quase-personalização ou recuperação de conteúdo anonimizado por meio de histórico de navegação agregado de uma grande pluralidade de dispositivos, como milhões ou bilhões de dispositivos; ***v)*** A **patente US 8458349 B2** concedida à *Microsoft Corporation*, que dispõe sobre a possibilidade de se proteger da identificação em diferentes interações na rede. Interessante seria utilizar esse serviço para se proteger, por exemplo, de um *cookie* da própria Microsoft em seu sítio ou até mesmo da assistente virtual inteligente *Cortana*. O velho *win-win* nunca é obsoleto na aposta dos novos direitos digitais. Direitos cuja materialização em grande parte dependa, agora, de licenças, porém não governamentais.

[80] Importante pontuar, ademais, que na ADPF 403 o Ministro Fachin enfrenta a *historicidade* do "*anonimato*" na Constituição em sede de *obter dictum*, dentro da qual cita a história de sua previsão, em que era proibido até mesmo o pseudônimo, e avança em favor dos novos tempos conferindo uma *interpretação restritiva à vedação ao anonimato*: *"(...) a melhor interpretação constitucional da expressão "vedado o anonimato" é a de, minimamente, garantir a responsabilidade, sempre ulterior, de quem abusa de sua liberdade. Assim, desde que assegurada a responsabilização nos casos de abuso, o anonimato online não violaria o direito à liberdade de expressão."*

[81] Acrescente-se, por fim, que a questão sobre o bloqueio de aplicações é um tema ainda em discussão no STF, renovado, sobretudo, através das decisões tomadas pelo Ministro Alexandre de

criptografia ponta a ponta aplicada às comunicações privadas, de modo que esse design possa, de antemão, afastar qualquer possibilidade de acesso aos dados pelo Estado.

Os temas se relacionam, mas uma decisão sobre o último tema demanda maior amadurecimento por meio de uma análise mais exauriente sobre os diversos aspectos que não foram considerados, mas que orbitam o dilema cripto. Isso significa que, para tanto, também devem ser consideradas outras questões, mais complexas, que problematizam o debate, como por exemplo, as diversas medidas de contorno da criptografia sob domínio de atores opacos, a forma como os *backdoors*/vulnerabilidades são formadas, a perspectiva transnacional do debate, entre outros pontos a serem abordados nos tópicos 3.3, 3.4 e 3.5.

No entanto, antes de problematizarmos esses aspectos nos tópicos supracitados, apresentaremos, na doutrina nacional, a abordagem de Filipe Medon (2019) a respeito de uma leitura funcionalizada da criptografia e do problema de se valorar, de antemão, um direito em detrimento de outro, tal como o fizera o voto do Ministro Fachin.

3.2. Criptografia e Funcionalização

Medon (2019) procura apresentar uma análise do instituto da criptografia à luz da metodologia civil constitucional, abordando primeiramente a estrutura do instituto e, depois, a sua dimensão funcional para fins de verificação do merecimento de tutela. Esse iter metodológico, segundo o autor, seria necessário à resposta da principal indagação: "*será possível a sua quebra*[82]?".

Quanto à estrutura, inicialmente, é indagado se a criptografia seria um direito autônomo ou se seria um direito albergado no seio de outros direitos, como a privacidade e, acrescentamos, a liberdade de expressão. Nessa linha, seria um direito ou uma técnica? A resposta dada é:

Moraes através da análise da Petição n.º 9.935/DF entre 17 e 20 de março de 2022, envolvendo o bloqueio das atividades da empresa *Telegram*, para fins de cumprimento de decisões judiciais num contexto de investigação da propagação de desinformação – *fake knews*. Para maiores detalhes, ver: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/DecisaoTelegram20mar.pdf>. Acesso em: 21 mar. 2022.

[82] Salvo melhor juízo, a palavra "quebra" é empregada no sentido de afastamento da criptografia, o que atrai as ideias decriptação, decifragem, inteligibilidade do conteúdo, etc.

> É de se indagar, ainda, a sede da proteção desse chamado direito à criptografia no Direito Brasileiro. Neste sentido, parece ser mais coerente se pensar que o direito à criptografia é um desdobramento do direito à privacidade, pois seu escopo é a tutela daquele. Trata-se de uma técnica, isto é, um instrumento a serviço da concretização do direito à privacidade. Mas nem por isso deixa de gozar de certa autonomia metodológica, na medida em que concretiza também outros direitos, como a liberdade de expressão e de comunicações. Por isso, se defende que esta técnica pode ser vista como um direito. Contudo, resta avaliar quais os limites impostos ao seu exercício (Medon *in*: Anais do VI Congresso do Instituto Brasileiro de Direito Civil, 2019, p. 314).

A despeito de a criptografia estar sendo reconhecida como instrumento protetivo no âmbito de Direitos Humanos, como a privacidade e a liberdade de expressão, a preocupação expressada pelo autor é quanto ao seu enquadramento como um potencial direito absoluto, o qual, por razões técnicas, não poderia ser relativizado.

A preocupação é extremamente pertinente e, pensamos, foge ao lugar comum do debate, fenômeno em que se verifica, majoritariamente, uma onda que abraça automaticamente a criptografia como instrumento protetivo da privacidade quando, em paralelo, essa "privacidade", não raro, pode funcionar como um escudo da segurança patrimonial das grandes empresas do ramo.

Esse ponto não deixa de passar pelo crivo cético do autor que, ao contestar o argumento consequencialista de que o enfraquecimento da criptografia traria prejuízos econômicos e uma evasão[83] de empresas do país, indaga se o patrimônio, notadamente, o lucro empresarial, deveria ser a causa defensiva do setor privado.

Nesse ponto, Medon reconhece a importância do argumento da comunidade técnica de que o enfraquecimento da criptografia engendraria possíveis danos colaterais advindos da intervenção nas infraestruturas comunicativas, o que conduziria a uma possível insegurança digital. No entanto, essas razões não poderiam ser causas da constituição de um direito absoluto, apontando, portanto, para a possibilidade de flexibilização da criptografia:

> O que se critica não é a quebra, mas a quebra que desproteja as demais pessoas. Resta saber se esses outros meios invocados efetivamente dão conta do problema. Se a resposta for negativa, a quebra deve acontecer. E, caso se defenda a quebra, esta deve tentar vulnerar o menos possível os sistemas e os usuários. E esta é uma

[83] O argumento da evasão econômica corporativa é antigo, semelhantemente presente, por exemplo, nas próprias razões do veto presidencial do ex-presidente Fernando Collor em 1991 direcionado à Lei n.º 8.248/91 e expostas no tópico 2.1.5.

> tarefa que deve ser compartilhada entre o Estado e as sociedades empresárias de tecnologia (Idem).

Ao apresentar o ponto de vista de quem trabalha com a realidade prática das interceptações do conteúdo comunicativo em fluxo no Judiciário, o autor busca demonstrar que dentro desse debate, por vezes, é imprescindível[84] a captura do

[84] Pensamos ser uma pergunta consentânea aos axiomas do debate a seguinte: já que a criptografia blinda o conteúdo comunicado, quais condutas reprováveis, para fins de apuração efetiva, dependem do conhecimento desse conteúdo? Nesse sentido, por exemplo, desperta como um incômodo, ainda que sumário e pendente de uma análise exauriente, a conduta do *Insider Trading*, um crime contra o mercado de capitais, introduzido na Lei n.º 6.385/76 (Lei do Mercado de Valores Mobiliários) através do Art. 27-D e já modificado em 2017 pela Lei nº 13.506. Eis a redação originária e a redação atual do tipo: Redação originária: *Art. 27-D. Utilizar informação relevante ainda não divulgada ao mercado, de que tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. (Artigo incluído pela Lei nº 10.303, de 31.10.2001).* Redação Atual: *Art. 27-D. Utilizar informação relevante de que tenha conhecimento, ainda não divulgada ao mercado, que seja capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiros, de valores mobiliários.* Seja qual for a redação, salvo melhor juízo, uma maior efetividade e celeridade no combate desse tipo de conduta pressuporia o conhecimento do teor da informação relevante trocada, sobretudo num mundo interconectado, em que a agilidade das comunicações e da troca instantânea de mensagens pode produzir, imediatamente, um conhecimento privilegiado para outro ator do outro lado do mundo, influenciando mercados, desestabilizando-os, entre outros efeitos, inclusive transnacionais. Não é menos relevante o fato de que essa espécie de conduta reprovável, tão relevante para a economia, possua tão poucas condenações. Nesse sentido, ver: <https://www.infomoney.com.br/mercados/crime-de-insider-trading-teve-so-uma-condenacao-penal-em-20-anos/>. Acesso em: 13 jan. 2022. Ou mesmo: <https://amecbrasil.org.br/noticia-publicada-pelo-portal-jota-apenas-8-dos-casos-de-insider-trading-vao-ao-judiciario/>. Acesso em: 13 jan. 2022. Para análise sobre uma condenação inédita da conduta do *insider trading* pelo Superior Tribunal de Justiça: <https://www.vbso.com.br/stj-tem-condenacao-inedita-por-insider-trading/>. Acesso em: 13. jan. 2022. Por sua vez, constata-se uma análise mais ampla, envolvendo a conduta e elementos de ativos criptográficos em: <https://ilr.law.uiowa.edu/print/volume-105-issue-1/crypto-assets-and-insider-trading-laws-domain/>. Acesso em: 15 jan. 2022. Em sentido contrário, por outro lado, SUSAN LANDAU afirma que o crime do *Insider Trading* pode ser apurado através dos "meios alternativos de investigação", justamente aquele conjunto de novos métodos investigativos introduzidos pela Era de Ouro da Vigilância, os quais foram apontados nos tópicos 2.4 e 2.5. Nessa linha, ela cita como paradigma o caso Raj Rajaratnam. (LANDAU, Susan. *Listening In: Cybersecurity in an Insecure Age*. Michigan: Grand Rapids, 2017, pp.13-15). Para maiores detalhes do caso, também ver: <https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1022&context=ecf_capstones>. Acesso em: 15 jan. 2022. Independentemente de a apuração da conduta do *Insider Trading* depender ou não da inteligibilidade do conteúdo trocado, para fins de condenação, parece plausível - do ponto de vista daqueles Estados que não estão afinados com os novos sucedâneos forenses - que o não conhecimento do conteúdo compartilhado dificulta a investigação e a persecução, na medida em que o teor informativo possui grande relevância para a certeza da apuração da conduta. No caso, não acessar o conteúdo trocado por sujeitos dotados de informações privilegiadas, agora blindadas pela encriptação, parece forçar o Estado a recorrer aos novos métodos forenses para a formação de uma verdade processual, para a formação de uma outra qualidade de instrução probatória, caso queira atuar eficientemente sobre esse tipo de conduta. Nesse sentido, também pensamos ser pertinente, do ponto de vista social, perguntar: que tipo de atores são os sujeitos ativos dessa conduta reprovável? Em que andar da pirâmide social eles se encontram? A criptografia, nesse caso, poderia estimular, sutilmente, uma política criminal indireta, encriptada, nas entrelinhas, favorável ao colarinho branco, na medida em que pode dificultar a persecução sobre essa classe de atores? Não encontramos discussões a respeito.

conteúdo no exato momento em que ele é trocado para fins de tutelar outros direitos. Nesse sentido, conclui que:

> a existência de um mecanismo que seja completamente intransponível em qualquer situação não deve ser merecedora de tutela, porque privilegiaria abstratamente um direito em face de outro, o que é incompatível com o sistema vigente. Não se pode admitir a existência de um direito absoluto em si e que não comporte ponderação diante do caso concreto (Idem, p. 318).

Para além do ponto de vista técnico, é importante avaliarmos que, do ponto de vista jurídico, o que pode estar em jogo, aqui, não é necessariamente a colisão entre, de um lado, um direito e, de outro, outro direito. Mas a própria (im)possibilidade de ponderação no caso concreto, engendrando, via defesa da inviolabilidade técnica da criptografia, a adoção de valorações de antemão, abstratas, o que é bastante problemático para a ciência jurídica e, sobretudo, para aquelas escolas que se ancoram na concretude das circunstâncias.

Pode-se argumentar, por outro lado, que a ponderação não será afastada, pois existiriam métodos alternativos de se alcançar a informação, tal como vimos no primeiro capítulo ao abordarmos a investigação por meio da Era de Ouro da Vigilância (tópicos 2.4 e 2.5). Entretanto, esses outros sucedâneos também não receberam a devida crítica à luz de uma privacidade estritamente funcionalizada ao ser humano. Necessários serão novos avanços sobre esse ponto obscuro do debate.

Em sede de conclusão e endereçando para o próximo tópico, vimos que as ações diretas em curso no STF possuem um objeto bastante restrito: avaliar, em rigor, o regime sancionatório previsto no MCI, notadamente as duas sanções mais drásticas ali previstas, quais sejam, a suspensão temporária das atividades do provedor ou mesmo a proibição do exercício de suas atividades (incisos III e IV do Art. 12) como meio coerção judicial.

As ações não abordam diretamente o problema dos *backdoors*/*vulnerabilidades*, tampouco as exigências estatais pela criação dessas falhas para fins de execução de suas prerrogativas constitucionais, o que é o emblema representativo da segunda guerra criptográfica e que foi suscitado no caso *Apple* x FBI, ainda que esse tenha sido solucionado, de modo alternativo, através da compra sigilosa de um sucedâneo forense que permitiu o acesso ao conteúdo do telefone do terrorista morto em São Bernardino (tópico 2.3).

Vimos também, no tópico 2.4, a advertência formulada pela comunidade técnica a respeito da introdução dessas vulnerabilidades propositais em favor do aparato persecutório do Estado. A conclusão desse segmento foi a de que tamanha postura poderia conduzir a um estado de insegurança generalizado na infraestrutura tecnológica, atraindo a ação de terceiros indesejados quanto a exploração das vulnerabilidades, entre outros pontos envolvendo custos econômicos e políticos.

No entanto, a problematização dessa discussão pressupõe algumas perguntas: como se engendram as vulnerabilidades nas TICs? O conhecimento dessas falhas se encontra sob a *expertise* de quais atores? A criptografia representaria um verdadeiro obstáculo para atores bem aparelhados e portadores de saberes privilegiados?

Para ingressarmos nessa trilha, antes é necessário conhecermos os dilemas da conectividade e como se formam as vulnerabilidades/*backdoors*. Eis o próximo tópico.

3.3. Conectividade e Autofagia: O Mapeamento das Fontes de Vulnerabilidades/*Backdoors*

Tornou-se um lugar comum nos debates sobre criptografia e *backdoors* a conclusão de que a introdução de vulnerabilidades intencionais – aquelas favoráveis ao aparato persecutório do Estado – traria consigo a majoração de riscos dentro da própria infraestrutura comunicacional (TICs). Riscos estes aptos a serem explorados por terceiros mal intencionados. Terceiros estes que podem constituir ameaças cibernéticas (ciberameaças)[85].

[85] Duane C. Wilson explica que a noção de ciberameaça pode ser vaga, havendo confusões entre o que seria uma ameaça e o que seria um ataque propriamente dito a um sistema. No entanto, inclina-se a relacionar as ciberameaças aos possíveis atores que desempenhariam o acesso não autorizado ou ataque ao sistema. Nesse sentido, lista como exemplos: terroristas, espiões industriais, organizações criminosas, ativistas *hackers*, *hackers* como lobo solitários, *insiders* descontentes, concorrentes de negócios, entre outros. No entanto, chama especial atenção para os atores de maior relevância, os próprios Estados-nações e seus governos nacionais. (WILSON, Duane C. – *Cybersecurity*. Cambridge, Massachusets: The MIT Press, 2021, pp.69-71). Essa valoração dos Estados como as principais ciberameaças foi reforçada, inclusive, pela atual Estratégia Nacional de Contrainteligência dos EUA para o período de 2020-2022, em que se convoca à parceria com seu governo não apenas as empresas estadunidenses, mas também os líderes acadêmicos (EVANINA, William R. National Counterintelligence Strategy of the United States of America 2020-2022, p. 11) Disponível em: <https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf>. Acesso em: 01 jun. 2022.

Nesse sentido, argumentou-se, sobre o fortalecimento da criptografia. Essa postura estimularia, de um lado, a privacidade, garantiria maior segurança digital, fortaleceria as infraestruturas informativas e comunicativas em rede, ainda que, por outro lado, a blindagem oferecida pela criptografia pudesse ser utilizada, também, pelo crime organizado, dificultando o trabalho da segurança pública.

Diferentemente, também se argumentou sobre o enfraquecimento da criptografia, sobretudo através do paradigma *backdoors*. Enfraquecer os sistemas criptográficos para permitir que o Estado intervenha nas infraestruturas e colete as informações necessárias às suas tradicionais prerrogativas. Nesse caso, afirmara-se que tamanha postura teria por efeito fragilizar a integridade das infraestruturas, igualmente franqueando-as à ação de terceiros mal intencionados, além de que a operacionalização desse acesso traria altos custos financeiros, reverteria um atual estado de boas práticas vigentes na internet, e enfrentaria sérias dificuldades operacionais em uma escala transnacional, por exemplo, a quem seria confiada, no cenário internacional, as chaves da decriptação?

Entretanto, pouco é debatido sobre como se formam as deficiências contidas na própria infraestrutura informacional comunicativa. Como se formam os *backdoors*? Quais as suas fontes?

O foco, em rigor, versa sobre aqueles *backdoors* funcionalizados ao Estado a serem introduzidos nas infraestruturas. Mas existem outros *backdoors*, dito não artificiais, "espontâneos", acidentais, difusos num sistema interconectado? E mais, essas vulnerabilidades estão sob o domínio de saber de quem? Eis o que começaremos a discutir.

Seriam apenas as vulnerabilidades propositadamente criadas em favor do Estado as únicas fontes de riscos engendradas na infraestrutura das TICs?

A resposta a essa pergunta pressupõe a problematização de como se formam as vulnerabilidades nas tecnologias de informação e comunicação. E isso se dá por meio da análise de dois eixos conceituais: primeiramente, pela própria ontologia da conectividade e, depois, pela sua relação com a característica autofágica dos instrumentos técnicos de cibersegurança, como a criptografia.

Sobre a conectividade, Duane C. Wilson (2021), ao comentar as origens da cibersegurança, explica que a apesar de a internet ser um grande portal para

negócios, governos e outras instituições, provendo acesso remoto para a troca de segredos, registros médicos e dados financeiros, ela também está sujeita ao "*paradoxo da conectividade*". Mas o que seria o paradoxo da conectividade?[86]

Trata-se de um pressuposto que leva em consideração a própria infraestrutura física da rede e as potências interativas dos dispositivos a ela conectados. Conforme Wilson (2021) explica, quanto mais conectados estiverem os nossos sistemas computacionais, mais expostos eles estarão aos ciberataques, tais como, tentativas de vazamento/roubo de dados, destruição de *softwares*, operações de disrupção e, até mesmo, danos físicos em *hardwares* e infraestruturas em rede.

Nesse sentido, o paradoxo da conectividade, em linhas sintéticas, busca ilustrar a relação de pressuposição recíproca entre, de um lado, a complexificação de sistemas conectados e, de outro, a majoração de riscos cibernéticos. Esse paradoxo conduz à máxima de que a complexificação é inimiga da segurança, ao passo que a simplificação é amiga da segurança. Quanto mais dispositivos estiverem conectados e interagindo reciprocamente, maiores as chances de vulnerabilidades surgirem e, consequentemente, serem exploradas como *backdoors*, caso as superfícies de ataque abertas não forem devidamente remediadas.

Recuperando o argumento de Landau (2017), a razão dessa majoração de riscos decorrente da simples opção política e, aqui advertimos, histórica, pela conectividade, se dá pelo fato de que a complexificação de sistemas muitas vezes engendra inesperadas interações entre diferentes funcionalidades, criando-se

[86] Advirta-se que a expressão "*connectivity paradox*" também é empregada em outros estudos, mas referentes ao campo do teletrabalho e da alienação social. Nesse sentido, ver: (FONNER, Kathryn L. e ROLOFF, Michael E. *Testing the Connectivity Paradox: Linking Teleworkers' Communication Media Use to Social Presence, Stress from Interruptions, and Organizational Identification. Communication Monographs*. Vol. 79, No. 2, June 2012, pp. 205-231). E também: (LEONARDI, Paul M., TREEM, Jeffrey W. e JACKSON, Michele H. - *The Connectivity Paradox: Using Technology to Both Decrease and Increase Perceptions of Distance in Distributed Work Arrangements. Journal of Applied Communication Research*. Vol. 38, No. 1, February 2010, pp. 85-105). Advertimos, no entanto, que não é nesses sentidos que empregamos o termo. Aqui, o paradoxo da conectividade é expressamente mencionado no trabalho de cibersegurança de Duane C. Wilson (2021), e implicitamente no trabalho de Susan Landau (2017) como representativo de uma relação de benefícios e malefícios decorrente da ontologia dos dispositivos conectados. Toma-se como premissa as formas como diferentes dispositivos não humanos e sistemas se conectam para proporcionar uma comunicação, trazendo alguns benefícios sociais, mas também certos inconvenientes. O ponto é explicado no corpo do texto.

vulnerabilidades. Nesse sentido, ela afirma que “sistemas simplificados são mais fáceis de serem protegidos” (2017, p.81).

Landau dá o exemplo da construção de um helicóptero militar projetado pela agência *Defense Advanced Research Projects Agency* (DARPA) para jamais ser hackeado. A premissa básica em sua linha de construção era a de que a infraestrutura central do veículo deveria ser composta apenas pelo essencial, mediante um design simplificado.

No caso, optou-se pelo isolamento e pela proteção mais rigorosa dos *softwares* centrais do veículo, como o código de comunicação com o solo e o código de manuseio da máquina. Tamanho isolamento e sobreposição de camadas protetivas ao redor desses pontos evitariam que o esqueleto do veículo fosse contaminado caso alguma terceira funcionalidade, menos importante, fosse comprometida por um ataque lateral e, por força da conectividade interativa, chegasse ao sistema central.

Entretanto, há uma diferença fundamental entre os dispositivos militares e o maquinário utilizado na indústria e na sociedade civil. Conforme Landau explica, no âmbito militar, as preocupações com a segurança da infraestrutura conectada sobrepõem-se às demandas por eficiência e por múltiplas funcionalidades, mas raramente esse pensamento é replicado na indústria e na sociedade civil.

Caso tentássemos reproduzir as medidas de segurança aplicadas ao helicóptero da DARPA em um item de consumo – um carro ou um *smartphone* – encontraríamos sérios problemas, isso porque carros possuem múltiplas funcionalidades e diferentes canais de comunicações, tais como *Bluetooth*, GPS, ou outros sistemas de entretenimento, explica a autora.

Por sua vez, nossos *smartphones* estão ancorados no massivo uso de diferentes aplicativos cujos padrões de segurança não se encontram adequadamente uniformizados, mas, ainda assim, integram um inventário de serviços contido num mesmo dispositivo físico, o telefone na palma de nossas mãos. Um receptáculo móvel da convergência de diferentes funcionalidades interativas.

Não foi à toa que durante o suposto término da primeira guerra criptográfica, em 2000, os produtos com recursos criptográficos customizados – aqueles com um projeto específico e diferenciado, feito sob encomenda – tenham permanecido sob

controle de exportação do governo estadunidense, ao passo que os produtos de prateleira, sujeitos à produção em massa e, assim, menos seguros, porém mais aptos às conveniências e múltiplas funcionalidades exigidas pela ordem consumerista, tenham sido liberados e vendidos em todos os cantos do globo.

Suas múltiplas conveniências, múltiplas funcionalidades e múltiplas interações trariam consigo, paradoxalmente, uma menor segurança. Conforme pontua Wilson, "as pessoas preferem pagar por conveniência, não por segurança, especialmente quando os benefícios dos protocolos de segurança não são transparentes" (2021, p. 51).

Por sua vez, Landau (2017) afirma que a busca da eficiência pela concorrência econômica levou os construtores da revolução digital a produzirem sistemas complexos em rede, mas sem medir as consequências para a segurança dessa própria infraestrutura. Segundo a autora, o ex-diretor da equipe de resposta e emergências cibernéticas de sistemas de controle industrial do Departamento de Segurança Nacional dos EUA, Marty Edwards, explica que as políticas da eficiência engendraram uma situação demarcada por muitos riscos cibernéticos, de modo que desconectar os sistemas industriais da rede reduziria os riscos, mas como essa medida aumentaria os custos da produção, dificilmente seria adotada.

Quanto mais sistemas e funcionalidades se conectam, maior a possibilidade de eficiência econômica, no entanto, também se amplia a possível superfície de ataque em favor de um terceiro. Sob a perspectiva de Aranha (2019), uma das formas prediletas para redução da superfície vulnerável seria através da máxima simplificação do sistema. Em rigor, pontuamos: *i)* evitando-se a conectividade recíproca entre sistemas; *ii)* objetivando-se descontinuidades. Que nem todos os dispositivos estejam conectados entre si.

Carissa Véliz, por sua vez, explica esse problema recorrendo à analogia:

> usamos portas corta-fogo para conter possíveis incêndios em nossas casas e edifícios, e compartimentos estanques para limitar possíveis enchentes em navios. Precisamos criar divisórias semelhantes no ciberespaço. Cada nova conexão em um sistema é um possível ponto de entrada (Véliz, 2021, pp. 191-192).

Nesse sentido, a autora cita como exemplo a possibilidade de que um telefone seguro seja hackeado simplesmente por estar conectado a uma chaleira

inteligente e menos segura, portanto, acrescentamos: mais vulnerável e sujeita a *backdoors*.

Outro meio de se reduzir a superfície de ataque seria através da solução tecnocrática. Como? Mediante o recurso às tecnologias de cibersegurança, dentre as quais a criptografia moderna desponta como uma das mais relevantes[87].

O paradoxo da conectividade engendra, portanto, uma relação de probabilidade: quanto mais nos conectamos e tornamos nossos sistemas complexos, mais vulnerabilidades são possíveis. Se, de um lado, a complexificação nos beneficia com as conveniências interativas dos inúmeros dispositivos no reino do consumo e, na indústria, fomenta a eficiência e reduz os custos produtivos, por outro lado, esse paradoxo também causa a criação de vulnerabilidades infraestruturais.

Esse paradoxo é um pressuposto ontológico para se compreender as fontes das vulnerabilidades. Um elemento estruturante do estudo das vulnerabilidades/*backdoors*.

Para Wilson (2021), esse paradoxo possui um corolário: o postulado do ponto mais frágil, de modo que uma rede ou uma TIC será tão segura quanto o for seu ponto mais frágil. É justamente nesse nódulo, uma espécie de calcanhar de Aquiles cibernético – se convém alguma analogia – que o ataque costuma ser deflagrado. Conforme Carissa Véliz aponta, "a segurança de seu telefone é apenas tão forte quanto seu aplicativo mais fraco" (2021, p. 238).

Retomamos, portanto, a pergunta retórica: seriam apenas as vulnerabilidades propositadamente criadas em favor do Estado as únicas fontes de riscos engendradas na infraestrutura das TICs?

A resposta é: não, pois a própria conectividade engendra suas próprias vulnerabilidades. A opção política por vivermos mediados por tecnologias de informação e comunicação traz o seu ônus: vulnerabilidades e insegurança.

Estas vulnerabilidades não necessariamente têm como fonte as falhas artificiais propositalmente introduzidas na infraestrutura para serem exploradas pelo Estado. Existem, também, as vulnerabilidades acidentais, decorrentes da

[87] Esse ponto, o uso da criptografia como medida técnica de segurança, será melhor explorado no tópico 4.2.

própria infraestrutura tecnológica e dos diversos dispositivos conectados em suas inúmeras interações inseguras.

É com base nessa distinção que classificamos as vulnerabilidades/*backdoors* entre: vulnerabilidades intencionais e vulnerabilidades acidentais, justamente aquela contemplada pela ANATEL, nos termos expostos no tópico 2.1.6. Trata-se de uma pequena diferenciação classificatória adequada à reduzida proposta desse estudo, mas em nada imune de críticas à luz dos rigores conceituais da ciência da cibersegurança.

Recordando. Para os fins aqui propostos, quando nos referirmos às vulnerabilidades criadas e/ou exploradas para e em favor do Estado, estaremos nos referindo às vulnerabilidades intencionais[88], falhas lícitas – por força de lei – na infraestrutura, que tem por objetivo assegurar, tecnicamente, o acesso autorizado em favor do Estado para o cumprimento de suas competências constitucionais. Se o Estado o exerce de forma abusiva, isto já é outro assunto.

No entanto, foi justamente sobre a problematização dessas vulnerabilidades intencionais que se descortinou boa parte dos debates sobre o *going dark* e a controvérsia cripto vistos no tópico 2.3, e a subsequente conclusão dos especialistas técnicos de que tamanhas falhas propositais engendrariam novos riscos, pois seriam capturadas por terceiros, atraindo uma insegurança cibernética, tal como exposto no tópico 2.4.

Certamente as falhas em prol do Estado amplificam o inventário de vulnerabilidades e introduzem novos riscos[89], na medida em que majoram a superfície de ataque das infraestruturas TICs. No entanto, há de convir que a infraestrutura, por si só, não é imune a outros riscos igualmente relevantes, mas

[88] Ronald Deibert, por sua vez, emprega a expressão "back doors engineered for lawful interception". Eis a transcrição da passagem: "By definition, back doors engineered for lawful interception are engineered vulnerabilities by a diferente name. In these and likely numerous other undiscovered cases, those vulnerabilities offer a direct point of access for exploitation." (DEIBERT, Ronald J. - *Shutting the backdoor: The perfils os National Security and Digital Surveillance Programs*. Canadian Defence e Foreign Affairs Institute (CDFAI), 2013).

[89] Carlos Augusto Liguori Filho, por exemplo, afirma que a exploração dessas vulnerabilidades "seria muito mais difícil de acontecer em um sistema sem vulnerabilidades intencionais" (LIGUORI FILHO, Carlos Augusto. Criptografia em debate: modelos regulatórios ao redor do mundo, *in*: DONEDA, Danilo e MACHADO, Diego. *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 94).

engendrados pela sua própria ontologia e pela própria concorrência econômica pelas invenções.

Isso desperta algumas perguntas provisórias, cujas respostas buscaremos adiante: existem atores historicamente mais bem preparados para explorar essas vulnerabilidades acidentais? Atores que já estejam no jogo muito antes do aparato persecutório do Estado, das forças de segurança internas começarem sua pauta de exploração dessas vias para fins de garantir as suas tradicionais práticas?

Nesse sentido, pensamos ser razoável alargar a discussão para incluir e enfatizar as perplexidades trazidas pelo próprio paradoxo da conectividade e as vulnerabilidades acidentais que permeiam diversos produtos e sistemas TICs, sobretudo os sujeitos de conhecimento desses elementos acidentais e o poder adquirido dessa possibilidade.

Mas como essa problemática se relaciona com a criptografia, sobretudo com a sua natureza autofágica? O que é isso?

Aranha (2019) afirma, por exemplo, que em razão da quase inafastável presença de vulnerabilidades em *softwares*, problematiza-se diariamente a área de Segurança Computacional, que tem por objeto a redução da superfície de ataque disponível a um atacante.

Uma das principais medidas remediadoras dessas vulnerabilidades seria a redução da superfície de ataque através da criptografia, "também um tema de cibersegurança, pois essas técnicas são medidas de segurança computacional" (2019, p. 139).

A criptografia certamente é uma das mais emblemáticas técnicas de cibersegurança empregadas sobre as TICs. No entanto, também já sabemos que essas tecnologias engendram suas próprias vulnerabilidades, seja através da criação de falhas artificiais e propositais, seja através do próprio exercício da liberdade de invenção humana, que introduz novos bens, serviços e insumos na cadeia de tecnologia de informação e comunicação, sempre remodelando novos regimes de interações e funcionalidades aptos a produzirem supervenientes vulnerabilidades.

Nessa linha, é pertinente indagar se a criptografia, como técnica de segurança da informação e, agora, também da integridade da própria infraestrutura, consegue acompanhar o conjunto de variáveis que engendram as constantes

vulnerabilidades do mundo cibernético. Essa indagação nos leva ao segundo eixo conceitual desse tópico: a característica autofágica da criptografia.

Comentando a referida característica, Aranha (2019) afirma que o progresso da criptografia se dá justamente em razão da demonstração da vulnerabilidade das técnicas protetivas, promovendo-se, subsequentemente, a substituição por outras técnicas, estas mais seguras e resistentes a adversários mais poderosos. Doneda e Machado (2019) corroboram o pensamento de Aranha.

Por fim, cabe transcrever uma passagem em que o autor relaciona obsolescência de técnicas protetivas, segurança e a capacidade de atacar vulnerabilidades através da *criptoanálise*:

> a evolução da Criptografia segue então o observado em outras ciências, com a distinção de que técnicas obsoletas se tornam também perigosas, por fornecer falsa sensação de segurança aos que confiam em sua segurança para depositar segredos. O esforço de atacar técnicas criptográficas para antecipar e prevenir eventuais ataques reais com interesses diversos é estudado pela criptoanálise e representa etapa crucial na forma como essa ciência progride (Aranha, 2019, p. 25).

Recorde-se que suscitamos, no tópico 2.1.1, o objeto da *criptoanálise*: estudar e aplicar métodos de ataque aos sistemas encriptados para fins de diagnosticar suas vulnerabilidades e, assim, superá-los.

Deibert (2013, Apud. Landau, p. 7), por sua vez, recorda que poucas vezes é sopesado o fato de que alguns *backdoors*, hoje remediados por técnicas de cibersegurança, podem se tornar vulneráveis com a passagem do tempo à medida que as capacidades técnicas de ataque progridam e o conhecimento das vulnerabilidades se espalhem, revelando, assim, pensamos, um incessante quadro de superveniências de inseguranças cibernéticas. Trata-se do “fator tempo.”

A relação entre o paradoxo da conectividade e a autofagia das técnicas protetivas é que, de um lado, deparamo-nos com inúmeras fontes de vulnerabilidades acidentais, engendradas, em sua maior parte, em razão da própria opção política por se viver através da mediação de sistemas de tecnologia de informação e comunicação, pois a complexificação das diversas interações de funcionalidades que permeiam esse ramo, por si só, engendra uma potência de acidentes de insegurança. Por outro lado, o remédio para esse problema político tem

sido, também, a solução tecnológica[90]: as medidas de cibersegurança, dentre as quais desponta a criptografia. Sucede que a efetividade desses remédios é de índole autofágica, precária, contingente, sob o eterno retorno[91] dos prazos de validade. Uma segurança sob perpétua condição resolutiva.

Salvo melhor juízo, esse traço introduz a ideia de contínua precariedade do estado da arte protetiva e, por que não, uma potência de insegurança animada, ora pela variável das invenções humanas, ora pelos investimentos nas expertises de ataque.

Analisar, portanto, a relação entre criptografia e *backdoors* à luz das capacidades de ataque de terceiros pode ser bastante pertinente ao debate, sobretudo para o pensamento crítico situado em localidades globais em que essas ferramentas não estão sob o domínio local.

Isso porque, de um lado, as principais controvérsias do dilema cripto enfrentadas atualmente particularizam o debate sob um prisma em que o acesso excepcional em favor do Estado é enfatizado como fonte de insegurança cibernética, e, de outro, é dentro desse mesmo quadro infraestrutural sob a qual as principais narrativas têm desestimulado a presença do Estado, notadamente a de seu aparato persecutório judicial, que também se vislumbram a presença de uma gama de outras vulnerabilidades, acidentais, fontes aptas à exploração e interceptação transnacional por outros atores historicamente mais bem aparelhados tecnicamente do que as forças de segurança domésticas de um ou outro Estado, contudo, não raro, cercados por uma imensa opacidade.

Se a criptografia tem sido um obstáculo de acesso aos dados pelos aparatos persecutórios do Estado, por outro lado, essa técnica também seria um empecilho para outros atores, opacos, acessarem os dados, mas de forma sub-reptícia? É o que abordaremos nos próximos tópicos.

[90] Para uma crítica sobre a solução tecnocrática para um problema político, ver (METAHAVEN. Captives of the Cloud, Part III: All Tomorrow's Clouds, in: ARANDA, Julieta; WOOD, Brian Kuan; VIDOKLE, Anton. *The Internet Does Not Exist*. E-journal: Sternberg Press, 2015, pp. 270-273).

[91] Valho-me, aqui, da expressão nietzschiana "eterno retorno" apenas para ilustrar a condição em que nos encontramos no que toca a segurança cibernética, como um ciclo que sempre se renova e destrói o modelo anterior. (Nietzsche, Friedrich Wilhelm – A gaia ciência. São Paulo, Companhia das letras, 2012). Não é à toa, ademais, que a autofagia seja representada pela alegoria do *ouroboros*: a serpente que, permanentemente, devora a sua própria cauda.

3.4. Meios Sub-Reptícios de Acesso aos dados e a Expertise de Atores Opacos

A passagem da era analógica para a era digital dificultou a coleta e decodificação de alguns objetos, os novos sinais comunicativos. Novos tempos, novos desafios. Para aqueles cuja atividade-fim sempre foi trabalhar na coleta e decodificação de sinais, a criptografia inerente ao reino digital introduziu imediatamente um escudo difuso em favor das comunicações e armazenamentos privados.

O que a Inteligência fez? Antevendo o curso da História, deu o primeiro passo para o lado, mas estrategicamente. Existiriam novas formas de coleta e decodificação dos dados ininteligíveis para além do raio de alcance protetivo da criptografia? Quais atores possuiriam essa expertise?

Os assentimentos de um quadro interno da NSA, o ex-diretor Michael, imprimem uma concretude ao debate. Comentando o paradigma da época, o ex-servidor da NSA publiciza, hoje, o que era segredo:

> antes do 11 de setembro, quando estávamos olhando para as telecomunicações modernas, … dissemos que tínhamos o problema do que chamaríamos … V ao cubo – volume, variedade e velocidade – que as telecomunicações modernas estavam explodindo em variedade e tamanho (…) Mas também sabíamos que nossa espécie estava colocando mais conhecimento em uns e zeros do que jamais havia feito em qualquer momento de sua existência. Em outras palavras, estávamos divulgando o conhecimento humano de uma forma que era suscetível à inteligência de sinais. Então, para ser muito sincero, quero dizer, nossa visão mesmo antes do 11 de setembro era que se pudéssemos ser bons em dominar essa revolução global das telecomunicações, esta seria a era de ouro da inteligência de sinais. E francamente, foi isso que a NSA se propôs a fazer (Chamayou apud. Hayden, 2015, p. 7).

A corrida pelo acesso ao ininteligível foi deflagrada por diferentes atores, em diferentes momentos históricos. O marco da largada não foi comum, tampouco isonômico em relação a todos os potenciais envolvidos.

Pensamos ser importante que em toda discussão sobre segurança da infraestrutura, os vazamentos de Snowden sejam considerados fatos públicos e incontroversos da existência de um conjunto de métodos sub-reptícios de acesso à

informação, que superam largamente o principal óbice oposto à captura dos dados armazenados e em fluxo: a criptografia[92].

Os documentos revelaram, por exemplo, que a NSA atuava – atuava?[93] - em diferentes níveis operacionais e por meio de múltiplos atores. Seus braços não se resumiam ao nível operacional tecnocrático interno, consistente na exploração das vulnerabilidades da segurança de diversos dispositivos digitais por um quadro de servidores especialistas técnicos no assunto, os criptoanalistas.

Seus braços também avançavam sobre a edição das normas técnicas a serem observadas na própria fabricação dos dispositivos. Como? Através de uma proximidade nociva ao NIST[94], o órgão com competência técnica para delimitar a modelagem criptográfica dos produtos comercializáveis[95].

---

[92] O jornal "The Guardian" contempla extensa demonstração das capacidades técnicas da Inteligência, apresentando um profícuo estudo a respeito dos métodos sub-reptícios de coleta de dados. Para maiores detalhes, ver: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>. Acesso em: 14 jan. 2021.

[93] Atuava ou ainda atua? Não se sabe.

[94] O NIST é um órgão subordinado ao Departamento de Comércio dos EUA e, conforme expusemos no tópico 2.3, foi um dos atores relevantes na primeira guerra criptográfica justamente pelo embate travado nos anos setenta com a própria NSA, tendo sido conferido àquele, formalmente, a competência técnica mediante a Lei dos Computadores de 1987. Um raciocínio *contrário sensu* nos é despertado: seria prudente para algum país, do ponto de vista da sua Inteligência e segurança nacional, conferir formalmente e publicamente o controle dos padrões criptográficos ao seu órgão de espionagem? O que os demais países pensariam? "Agora comercializamos produtos projetados pela nossa própria Espionagem, querem comprar?" Esse seria o horizonte caso fosse concedido formalmente a competência à NSA. Não faria sentido algum. O estrategista mais ingênuo saberia disso. Competência de direito x Competência de fato?

[95] Em setembro de 2013, logo após os vazamentos de Snowden, o NIST negou que tivesse enfraquecido os padrões criptográficos em prol da NSA, afirmando o seguinte: "NIST would not deliberately weaken a cryptographic standard. We will continue in our mission to work with the cryptographic community to create the strongest possible encryption standards for the U.S. government and industry at large." Muito embora também tenha reconhecido o seguinte: The National Security Agency (NSA) participates in the NIST cryptography development process because of its recognized expertise. NIST is also required by statute to consult with the NSA." Para maiores detalhes, ver: <https://www.nist.gov/news-events/news/2013/09/cryptographic-standards-statement>. Acesso em: 15 jan. 2022. Por sua vez, em julho de 2014, o NIST publica um guia para o desenvolvimento de padrões criptográficos em que se encontra a seguinte passagem: "Clarification of the Relationship with NSA: NIST may seek the advice of the NSA on cryptographic matters but it must be in a position to assess it and reject it when warranted. This may be accomplished by NIST itself or by engaging the cryptographic community during the development and review of any particular standard. The VCAT recommends that NIST senior management reviews the current requirement for interaction with the NSA and requests changes where it hinders its ability to independently develop the best cryptographic standards to serve not only the United States Government but the broader community." (NIST. *Cryptographic Standards and Guidelines Development Process Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology*. 2014, p. 4). Disponível em: <https://www.nist.gov/system/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf>. Acesso em: 19 jun. 2022. Ressalte-se, por fim que, muito recentemente, em maio de 2022, consta a informação de que, em face do possível

A agência influenciava a própria gênese dos padrões criptográficos que integrariam o sistema de segurança dos dispositivos, de modo que fossem reproduzidos pelos fabricantes, demonstrando, assim, a captura de importante estrutura técnico-legiferante do Estado, notadamente a de um órgão integrante do Departamento de Comércio.

É importante recordar, para fins de contextualização, que a primeira guerra criptográfica teria se encerrado em 2000, justamente com a autorização de que produtos de prateleira dotados de criptografia pudessem passar a ser exportados. Medida, à época, avalizada pela NSA (tópico 2.3).

Essa perniciosidade interna entre NSA e NIST demonstra que os produtos ora disponibilizados ao mundo, publicizados como seguros, confiáveis e inquebráveis, eram, na verdade, dotados de *backdoors*. Mas *backdoors* cujas superfícies de ataque eram – ao menos de largada – de conhecimento exclusivo de um único segmento mais bem estruturado e que operava, e ainda opera, à sombra do debate.

Não se pode subestimar a Inteligência. Conforme recorda Deibert (2013), ela é a segunda profissão mais antiga do mundo.

As capacidades de ataque e de exploração de vulnerabilidades pela Inteligência não são especulativas. Um exemplo de instrumento sub-reptício de acesso aos dados criptografados é o serviço *Key Provisioning Service* (2013, NY Times)[96]. Esse serviço representa não um simples banco de dados, mas um banco de chaves de decriptação. Uma espécie de inventário de chaves ao sabor do sistema. Um molho de chaves cibernéticas.

Por sua vez, as capacidades de ataque da agência sobrepõem-se, inclusive, a uma boa prática – *best pratice* – massivamente utilizada na internet. A

advento da computação quântica e seu potencial de quebra de todos os padrões criptográficos mais fortes existentes no mundo, o NIST irá editar novos padrões com a colaboração da NSA no processo, mas dessa vez, ao que parece, sem que essa agência possa superá-los. <https://www.bloomberg.com/news/articles/2022-05-13/nsa-says-no-backdoor-in-new-encryption-scheme-for-us-tech>. Acesso em: 19 jun. 2022.

[96] Para maiores detalhes sobre a aludida ferramenta, ver: <https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>. Acesso em: 22 mai. 2022.

possibilidade de contornar a criptografia de um padrão historicamente considerado seguro, o "HTTPS", através do projeto *Bullrun*[97].

Grégoyre Chamayou (2015), por sua vez, chama a atenção para uma parceria revolucionária na Inteligência de sinais agora em nível geoespacial. Trata-se da colaboração entre NSA e, segundo o autor, a sua *gêmea siamesa*: a Agência de Inteligência Geoespacial - *National Geospatial-Intelligence Agency* (NGA).[98]

Susan Landau explica que a NSA é uma agência de inteligência de sinais, acrescentando que uma agência desse tipo tem por essência escutar: "eles podem fisicamente grampear linhas telefônicas, arrancar sinais foras dos receptores de rádio, ou enviar esses satélites para o espaço" (2017, p. 120. Tradução livre)[99]. A autora sustenta que eles buscam desfazer as proteções das comunicações, mas de uma forma em que se garanta que eles e ninguém mais, além do emissário e do receptor, possam compreender as mensagens interceptadas.

Conforme recorda Aranha (2019), a inexorabilidade das vulnerabilidades em *softwares* é convidativa, justamente, às agências de Inteligência, sendo muitas vezes possível a captura da informação antes mesmo dela ser encriptada. Acrescentamos que essas vulnerabilidades são igualmente convidativas à formação de saberes muito segmentados e opacos a respeito dos meios de contorno da criptografia.

[97] Informação colhida de: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> Acesso em 23. mai. 2022.

[98] Nas palavras do autor: "*Esta parceria entre a NGA e a NSA foi descrita como constituindo uma 'mudança crítica'. A revolução consistiu em uma síntese perceptiva: ver o que se ouvia e observar o que se ouvia. Essa síntese foi alcançada juntando 'os olhos e ouvidos' da máquina de guerra; isto é, fundindo o que no jargão poderia ser chamado de duas 'fenomenologias'. No processo, as duas agências criaram um modelo híbrido que combinava seus respectivos know-hows. O resultado foi uma nova disciplina, 'Análise Geoespacial SIGINT'. A fim de treinar analistas nesta disciplina emergente, um curso especial foi implementado, o bootcamp Geocell na base Goodfellow no Texas. Também foram desenvolvidas várias ferramentas de processamento de dados, como o software Analyst Notebook, que, como sublinha o manual de instruções da IBM, permite a conversão de quase todos os dados disponíveis em 'um quadro analítico que combina análise geoespacial, de associação e temporal"* (CHAMAYOU, Gregoire. Oceanic enemy: A brief philosophical history of the NSA, Radical Philosophy, 191, maio/junho 2015, p. 9).

[99] Landau (2017, p. 120) também cita como exemplo de superação da NSA, por exemplo, o caso das rádios transmissões e do satélite *Rhyolite*. Nas décadas iniciais da guerra fria, as comunicações soviéticas viajavam através de rádio de alta frequência. Para conseguir interceptar esse tipo de tecnologia, os Estados Unidos tiveram que construir estações localizadas na periferia da União Soviética justamente para a captura desses sinais. Contudo, nos anos 70, houve uma modificação na tecnologia do rádio, que passou a ser transmitido através de micro-ondas. Inicialmente, a NSA não estava aparelhada tecnicamente para capturar esse tipo de sinal, entretanto esse problema técnico foi remediado com o lançamento do satélite *Rhyolite*.

Essas constatações nos levaram a um incomodo, mas que pode ser representado muito melhor por meio de perguntas. Se, numa ótica vertical, focada na política criptográfica interna de um Estado, a criptografia é apresentada como uma função protetiva das comunicações privadas, a qual, necessariamente e de imediato, por outro lado, introduz sérias dificuldades à efetividade de tradicionais práticas do aparato persecutório-judicial interno do Estado, então, não seria pertinente perguntar: a quem ou a quais segmentos está reservada a expertise dos meios sub-reptícios de contorno dos sistemas criptográficos e, consequentemente, se estes sujeitos, por essas vias, conseguem acessar o mesmo dado que aquele aparato não consegue ter êxito? Desse outro ponto de vista, qual seria a função da criptografia? Uma ilusão de óticas?

Nessa linha, seria prudente, ao menos do ponto de vista de um pensamento crítico da margem global, refletir também à luz de um outro estudo de especialistas técnicos para além do paradigmático *Keys Under Doormats*. No caso, o estudo *Surreptitiously Weakening Cryptographic Systems* (Schneier et al., 2015), publicado meses antes ao anterior, mas que tem por objeto justamente expor as sub-reptícias capacidades de ataque técnicas aptas ao contorno e/ou enfraquecimento da criptografia.

O próprio estudo, do qual também faz parte Bruce Schneier (2015)[100], adverte que a maior parte do trabalho acadêmico vem se concentrando em analisar a viabilidade da introdução de vulnerabilidades/*backdoors*, mas pouca atenção tem sido dispensada à construção de uma criptografia resiliente e, nesse sentido, propõem estudos de caso para fins de construção de uma taxonomia das fraquezas.

Recorde-se, ademais, que o campo de estudo sobre as fragilidades de um sistema criptográfico é a criptoanálise, de modo que através do ataque à defesa do sistema sejam diagnosticadas suas vulnerabilidades e, consequentemente, formado o conhecimento apto ao progresso da segurança. Conforme Aranha (2019) recorda, estamos diante de uma ciência autofágica. Uma ciência que progride à luz de suas falhas. Falhas estas que são constantemente renovadas, conforme visto no tópico 3.3.

[100] *Keys Under Doormats* e *Surreptitiously Weakening Cryptographic Systems* são dois estudos elaborados por um conjunto de especialistas. Em ambos, Bruce Schneier aparece como signatário. Para maiores detalhes sobre seus apontamentos, ver seu portal, constantemente atualizado: <https://www.schneier.com/>. Acesso em: 08 mar. 2022.

O procedimento de se reconhecer as vulnerabilidades de um objeto, analisando suas propriedades defensivas à luz dos instrumentos de ataque é muito semelhante a estratégia militar, sobretudo no que toca a formação de um conhecimento antecipado sobre os possíveis cenários futuros. Prever para agir eficientemente.

Conhecer as potências de um objeto consideradas as circunstâncias defensivas e ofensivas que lhe o cercam e, sobretudo, avaliar sobre qual domínio e em favor de quais sujeitos essas capacidades defensivas e/ou ofensivas estão submetidas podem ser condições necessárias à formação de uma política interna destituída de ingenuidades. Uma política que não enxerga apenas os seus limites territoriais, mas que pondera sobre os elementos geopolíticos que animam o debate através das sombras.

Para que não caiamos numa linguagem demasiado tecnocrática, como sois ocorrer nos últimos tempos, pensamos ser de bom tom recorrermos à tradicional sabedoria sobre ataque e defesa, ainda atual e que pode ser transplantada para os novos tempos:

> Quando dois conceitos constituem uma verdadeira oposição lógica, a saber, quando um é o complemento do outro, cada um está então fundamentalmente implicado pelo outro. Mesmo quando o poder limitado do nosso espírito não basta para captar ambos com um único olhar, nem para reconhecer por simples oposição a totalidade de um na totalidade do outro, pelo menos um lançará sempre sobre o outro uma poderosa luz e em muitos aspectos suficiente (Clausewitz, 2010, p. 739).[101]

No caso, a criptoanálise compõe um segmento epistemológico muito privilegiado no que toca ao atual estado da arte das comunicações privadas. As técnicas de defesa autofágicas, como a criptografia, engendram a formação, recíproca, dos saberes da proteção, mas, também, dos saberes da desproteção da informação e das infraestruturas a ela associadas animados por uma incessante dialética entre ataque e defesa.

Alguns desses saberes passam ao domínio público, compõem padrões técnico-normativos, políticas públicas criptográficas, acoplam-se a direitos em que

[101] Por sua vez, para uma linguagem mais atualizada e voltada para infraestruturas digitais, ver também, para o lado da defesa, os métodos sub-reptícios de defesa de sistemas em: (COLLBERG, Christian e NAGRA, Jasvir – *Surreptitious Software: obfuscation, watermarking, and tamperproofing for Software Protection*. Boston: Pearson Education, 2010, pp.06-07 e 86-113).

a informação seja elemento constitutivo de sua estrutura, integram o interesse de infraestruturas comunicativas, imiscuem-se em bens de consumo[102]. Outros saberes, por outro lado, são segmentados e muito bem guardados, o que atrai inevitavelmente incentivos de atores mais sofisticados – estatais e não estatais – no que toca a cooptação desse conhecimento qualificado para, assim, conseguirem concretizar o que outros, eventualmente amputados pela tecnologia de plantão disponibilizada, não conseguem: acessar.

Nesse sentido, avaliamos ser importante a transcrição de uma ampla passagem presente em relatório publicado pela UNESCO, que toca na questão da divisão de saberes sobre a cibersegurança e as capacidades de ataque:

> Finalmente, a encriptação de dados armazenados ou transmitidos, mesmo quando implementada e executada corretamente, pode ser violada ou burlada por autoridades competentes para garantir o acesso legal a informações e comunicações, sem o envolvimento de um usuário ou provedor de serviços. Por exemplo, autoridades relevantes podem obter acesso a informações não encriptadas em dispositivos do usuário final com a instalação de *key loggers* ou outros meios, como ataques de canais laterais. Estes poderiam aproveitar as falhas de implementação em *software* criptográfico e implementações. Intensos debates vêm sendo travados sobre as formas pelas quais ocorrem a exploração de vulnerabilidades de softwares (chamadas de "zero-days"), pois, ao invés de corrigirem as inseguranças, acabam por prolongá-las aos usuários da Internet de maneira geral. Finalmente, a mais controversa das opções acima tem sido a interferência documentada na segurança dos padrões criptográficos em contextos de configurações padrão. Isso levou a reações de profunda preocupação por parte da comunidade técnica, e especialistas internacionais questionaram a falta de separação de recursos relacionados à capacidade de encriptação ofensiva da garantia de informações em agências relevantes dos EUA. Especificamente, a preocupação é que a missão de garantir a segurança defensiva seja prejudicada por aqueles, na mesma agência, focados em capacidades ofensivas. A regulamentação legal e o escrutínio constitucional, de acordo com a legislação dos EUA, sobre o uso de métodos distintos com o objetivo de violar ou quebrar a segurança da encriptação, ainda está no começo (Schulz e Hoboken, 2016, p. 33).

As condições de acesso ao inteligível parecem ser historicamente, tecnologicamente e financeiramente assimétricas entre os diversos atores envolvidos, sobretudo entre as diferentes jurisdições. Se considerarmos, por benefício da dúvida, que existe uma forte assimetria de acesso por diferentes atores dentro de uma infraestrutura comum, qual seria a função da criptografia para esses

[102] Para maiores detalhes sobre os poderes de criptoanálise da NSA, sobretudo em relação aos produtos com recursos criptográficos majoritariamente utilizados no cotidiano, ver o trabalho de BRUCE SCHNEIER em: <https://www.schneier.com/blog/archives/2013/09/the_nsas_crypto_1.html> Acesso em 1 jun. 2022.

atores que não podem superá-la? A criptografia estaria funcionalizada ao ordenamento ou seria o ordenamento que estaria funcionalizado à criptografia? Criptografia de quem? De quem pode superá-la?

Um caso emblemático em que se observou a existência desse precioso e segmentado conhecimento sobre as vulnerabilidades acidentais de um sistema foi o caso *The Shadow Brokers – Wannacry*. Conforme explica Liguori Filho (2019), um grupo *hacker* chamado *The Shadow Brokers* invadiu os sistemas da própria NSA, roubou e divulgou uma série de informações em poder da agência, mas que tinham por objeto justamente o conhecimento de diversas vulnerabilidades de sistemas de segurança e *softwares* populares, por exemplo, o *Windows* 8.

Segundo o autor, uma vez que o conhecimento dessas vulnerabilidades escapou ao controle exclusivo da NSA, terceiros utilizaram esses saberes para desenvolver um *software* malicioso, o *Wannacry*, que atacou diversas instituições ao redor do mundo, desde hospitais britânicos[103], até mesmo o Tribunal de Justiça paulista. Nesse sentido, importa ressaltar que o caso *Wannacry* é paradigmático e representativo do controle de informações privilegiadas envolvendo atores opacos dotados de saberes segmentados.

Quanto ao ponto, colhe-se de Thomas Rid (2020) uma provocação: se uma agência de Inteligência perde o controle dos seus saberes envolvendo vulnerabilidades alheias e, nessa linha, é possível que terceiros indesejados explorem esse conhecimento, tirando vantagens dessas ferramentas e saberes, não caberia a Agência de Inteligência notificar imediatamente os fabricantes a respeito das vulnerabilidades presentes em seus produtos? E esses fabricantes, por sua vez, não teriam o dever de notificar seus clientes, além de promover céleres medidas para fechar esses *backdoors*?

Refletindo sobre possíveis desdobramentos futuros envolvendo problemas análogos: seria realmente interessante, do ponto de vista da Inteligência, notificar a esfera pública a respeito do seu conhecimento sobre vulnerabilidades alheias, ainda que tenha perdido eventualmente o controle desses saberes? No que isso poderia repercutir no instituto da Responsabilidade Civil por omissão, tanto do Estado,

[103] Para maiores detalhes sobre a auditoria envolvendo esse ataque na Inglaterra, ver: <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>. Acesso em: 03 jun. 2022.

quanto de particulares? Esses são possíveis pontos de contato com o problema aqui abordado.

Além do mais, essas colocações são correlatas ao que abordaremos no tópicos 4.3, sobre Incidentes de segurança, e no tópico 4.5, em que apresentaremos um caso concreto em que se consolidam diversos aspectos discutidos ao longo desse estudo.

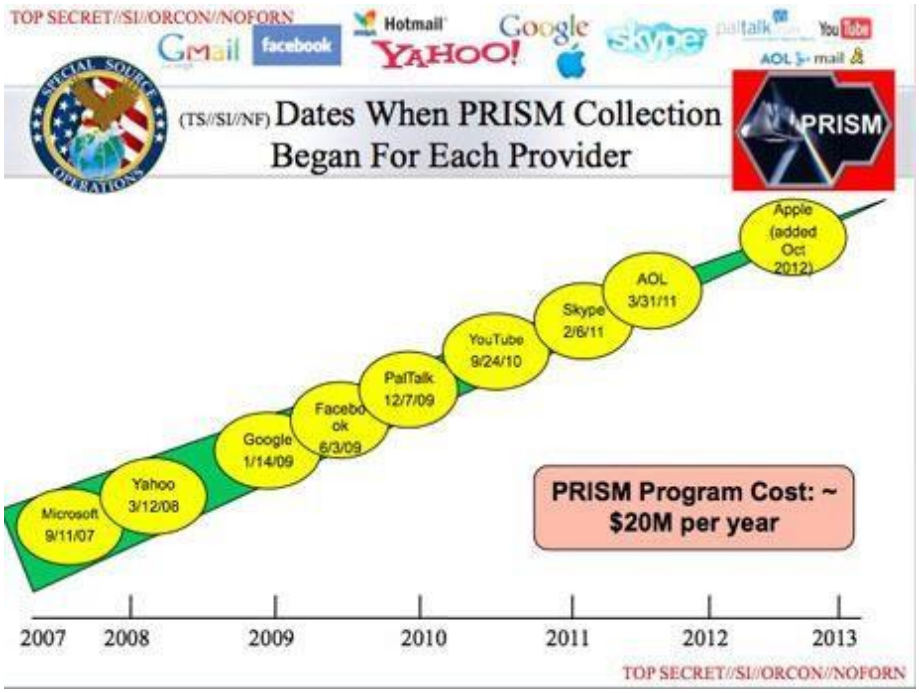
Avancemos para a questão da opacidade colaborativa de certos atores no que toca o acesso aos dados.

A discussão sobre a criptografia se torna ainda mais espinhosa se consideramos que boa parte do segmento que hoje emprega essa técnica em seus dispositivos, transnacionalmente e em fricção com jurisdições locais, é composto por grupos empresariais que, à luz dos vazamentos de Snowden, possuíam sigilosos acordos[104] com o governo de suas sedes, no caso, os EUA.

O *slide*[105] abaixo, utilizado pela própria NSA para explicar como funcionava a interface entre o serviço das empresas e os *backdoors* franqueados seletivamente à agência, revela as datas em que cada acordo informal foi iniciado com as principais empresas. Não custa contextualizar que era um período em que os *smartphones* e as principais redes sociais começavam a se expandir no âmbito consumerista.

[104] A ideia de um chamado à colaboração da iniciativa privada com seus governos locais não é nova. Nesse sentido, ver o "Apelo de JFK" já em 1961 ao setor empresarial americano diante do fortalecimento Soviético: <https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-newspaper-publishers-association-19610427>. Acesso em: 16 out. 2020. Verifica-se igualmente, mesmo após sessenta anos, a tensão que anima o chamado colaborativo, mas agora na guerra da Ucrânia: <https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/>. Acesso em: 15 jun. 2022.

[105] Informação colhida de: <https://nsa.gov1.info/dni/prism.html>. Acesso em: 22 jun. 2022



A divulgação de que o dinheiro dos contribuintes foi usado para cobrir os altos custos financeiros que as empresas suportaram para operacionalizar o programa colaborativo PRISM adiciona mais uma camada de opacidade entre o Vale do Silício – hoje um setor paladino na defesa da privacidade e da criptografia – e a NSA[106].

A ironia de tudo, ademais, é que no debate sobre o dilema cripto, um dos principais argumentos refratários à introdução de vulnerabilidades em favor do aparato persecutório do Estado também seria o alto custo financeiro.

Pontue-se, por sua vez, que as discussões sobre os acordos informais de co-operação público-privada não são de exclusividade dos EUA. Nessa seara, não faltam acusações recíprocas de regimes colaborativos também perpetrados por

[106] Em rigor, ao serem indagadas a respeito do reembolso dos custos, medida autorizada por decisão de 2011 do Tribunal secreto – FISA, as principais empresas deram respostas evasivas. Para maiores detalhes, ver: <https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid>. Acesso em 25 jun. 2022.; Para acessar a decisão da Corte FISA: <https://pt.scribd.com/document/162016974/FISA-court-opinion-with-exemptions>. Acesso em 25 jun. 2022.

outros países, como a China[107], a Rússia[108] e outros países envolvendo o *Five Eyes*.[109]-[110]

No entanto, conforme reconhecido em relatório publicado pela UNESCO (2016), a legislação dos EUA tem sido bastante permeável à colaboração voluntária e aos acordos informais público-privados, situação agravada pelo fato de que as empresas de internet de maior sucesso internacional estão sediadas naquele país.

As colaborações foram abaladas com as revelações de Snowden, mas o evento, por si só, além de ainda não lançar luzes sobre a permanência das eventuais parcerias nos dias atuais, também em nada impede que elas tenham sido remodeladas, derivando em outros meios colaborativos.

Comentando, por sua vez, os efeitos dos vazamentos de Snowden sobre as grandes empresas de tecnologias, Landau (2017) afirma que muitos países passaram a exigir que os servidores de armazenamento de dados fossem realocados fora do

[107] Para uma análise sobre acusações a respeito do sistema financeiro chines ter colaborado com o governo, ver: <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/>. Acesso em: 14 jan. 2022. Ou acusações a respeito da gigante chinesa de tecnologia, Huawei, ter espionado em favor de seu governo: <https://www.reuters.com/article/us-huawei-security-britain-chairman-idUSKCN1SK1HL>. Acesso em: 1 jun. 2022.

[108] No caso, cuida-se de acusações do governo estadunidense a respeito da colaboração de pessoas naturais, *hackers*, com o governo russo: <https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical>. Acesso em 10 jun. 2022. Ainda nessa linha, pertinente é a seguinte passagem colhida do próprio Departamento de Justiça dos EUA a respeito da colaboração de empresas norte-americanas no que toca aos litígios com a Rússia: "The department is also grateful to Google, including its Threat Analysis Group (TAG); Cisco, including its Talos Intelligence Group; Facebook; and Twitter, for the assistance they provided in this investigation. Some private sector companies independently disabled numerous accounts for violations of the companies' terms of service." <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>. Acesso em 10 jun. 2022.

[109] O Five Eyes é uma aliança internacional de comunidades de Inteligência envolvendo países do sistema anglo-saxônico: EUA, Reino Unido, Canadá, Austrália e Nova Zelândia para compartilhamento de inteligência entre seus integrantes. Sua formação derivou do antigo acordo informal entre EUA e o Reino Unido durante a segunda guerra mundial, no que foi chamado de UKUSA Agreement. Como relevante documento histórico, atualmente não é mais sigiloso e pode ser acessado em: <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/ukusa/agreement_outline_5mar46.pdf>. Acesso em 30 jun. 2022.; Digno ressaltar, ainda, que mais recentemente, em 2021, formou-se uma nova aliança, de ordem militar, AUKUS, composta por EUA, Reino Unido e Austrália para atuar na região do índico-pacífico, sob o pretexto de conter a ação Chinesa na região. O pacto envolve o compartilhamento de Inteligência e medidas de cibersegurança, entre outros pontos. Para maiores detalhes, ver: (https://researchbriefings.files.parliament.uk/documents/CBP-9335/CBP-9335.pdf) Acesso em 30 jun. 2022.

[110] No sentido da colaboração privada para as comunidades de Inteligência dos países do Five Eyes, ver o relevante papel da empresa *Palantir*, em (https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/) Acesso em 1 jul. 2022.

território estadunidense no intuito de torná-los menos acessíveis à Inteligência estadunidense.

No entanto, o mais interessante nessa passagem, ao menos do ponto de vista de um país periférico como o Brasil é a expressão "*home team advantage*" em que se sinaliza para uma relação de parceria através dos serviços de armazenamento em nuvem e, aparentemente, a assunção tácita de quem realmente seria o beneficiado com tamanho arranjo jurídico. Algo como a "vantagem da equipe de casa". Eis o inteiro teor, em tradução livre:

> Após as divulgações de Snowden, as empresas de tecnologia dos EUA perderam clientes. Serviços de computação em nuvem, que fornecem recursos de computação compartilhada, foram particularmente atingidos; Várias empresas e países queriam localizar seus data centers fora dos Estados Unidos para torná-los menos acessíveis à inteligência dos EUA. Apesar das tensões, empresas de tecnologia dos Estados Unidos como Google e Facebook continuaram sendo os repositórios de grandes quantidades de informações pessoais de cidadãos em todo o mundo; isso se deu em grande parte porque os consumidores confiam neles. A lei dos EUA e as comunidades de segurança nacional se beneficiam; isso dá uma vantagem da equipe da casa para obter dados sob ordem judicial. (Landau, 2017, p. 166).

Se considerarmos o ponto de vista de outras equipes presentes no globo, então, talvez haja alguma desvantagem, quanto ao acesso aos dados[111], mas

[111] O mais interessante dessa suposta desvantagem ou "vantagem do time de casa" no que toca o acesso aos dados é que ela pode ser desdobrada na discussão travada na ADC 51, de relatoria do Ministro Gilmar Mendes, pendente de julgamento, e movida pela Federação das Associações das Empresas Brasileiras de Tecnologia da Informação – ASSESPRO Nacional, para garantir que o acesso das autoridades brasileiras aos dados armazenados no exterior, ainda que sob a gestão de empresas com matriz estrangeira, observem os ritos normativos da cooperação jurídica internacional através dos tratados de assistência jurídica mútua (Mutual Legal Assistance Treaty – MLAT). (BRASIL. STF, ADC 51 DF. Relator: Ministro Gilmar Mendes. 28/11/2017. JusBrasil. 2017. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>. Acesso em: 15 mar. 2022. Essa discussão é problematizada se considerada a presença de instrumentos normativos estrangeiros que preveem a extraterritorialidade do acesso aos dados por forças estrangeiras, conforme ocorre com o *Cloud A*ct estadunidense, que introduz facilidades de acesso em favor de autoridades americanas em relação as empresas de matriz norte-americana. Para uns, o rito dos tratados, para outros, os novos ritos da extraterritorialidade. Para maiores detalhes sobre o *Cloud Act*, ver: (https://www.justsecurity.org/wp-content/uploads/2018/02/Cloud-Act.pdf). Acesso em 15 mar. 2022. Pertinente, ainda, ao ponto do acesso aos dados por outras vias e envolvendo autoridades estrangeiras na formação da prova, verifica-se que no ano de 2020 o ex-presidente Lula levou ao Superior Tribunal de Justiça discussão a respeito do acesso aos pedidos de cooperação internacional formulados entre as autoridades brasileiras e estadunidenses decorrentes da "lava jato". Ele objetiva acessar o conteúdo do que foi trocado transnacionalmente entre esses dois Estados. No caso, argumentou-se que a autoridade nacional responsável por intermediar a colaboração jurídica entre Procuradores da República e os norte-americanos, o ex-ministro José Cardozo, teria sido alijado por diversas vezes do procedimento cooperativo. (FISHMAN, Andrew; VIANA, Natalia; SALEH, Maryam. *The Intercept Brasil*. Disponível em: <https://theintercept.com/2020/03/12/lava-jato-driblou-governo-ajudar-americanos-doj/). Acesso em: 15 dez. 2020. Posteriormente, em março de 2022, o STJ determinou que o Ministério da Justiça informasse ao ex-presidente sobre a existência,

desvantagens das equipes de fora daquela casa, e que estejam espraiadas por diferentes ordenamentos jurídicos diante dessa estrutura de co-operação opaca de alternativas de acesso ao inteligível, para além da criptografia, envolvendo o setor privado e o setor público de um ou outro governo mais preparado tecnologicamente, sobretudo se considerado um elemento comum aos envolvidos: a transnacionalidade dos fluxos informativos.

Verifiquemos um pouco mais sobre essa problemática envolvendo a questão do plano transnacional no que toca a busca do Estado pelo acesso aos dados, mas no próximo tópico.

3.5. Transnacionalidade, o Problema do País Menos Seguro e os Efeitos Extraterrioriais

Vimos nos tópicos anteriores que a criptografia inaugurou uma tensão entre empresas com operação – por vezes, *co-operação* com outros governos – transnacional e jurisdições locais no que toca o acesso aos dados manejados através dos suportes tecnológicos do setor privado, sobretudo quando estes estejam sob a tutela de institutos cuja função primordial seja operacionalizar o poder de exclusão do que pode ser conhecido, do quem pode conhecer, do quando se pode conhecer e de que forma se pode conhecer, como o sigilo ou a privacidade.

Diante da dificuldade técnica de acessar os dados em razão de as políticas empresariais adotarem, em seus serviços, fortes padrões criptográficos, muitas jurisdições reagiram sancionando as empresas, não raro, com a suspensão de suas atividades no território local, a exemplo do caso brasileiro, situações fáticas que conduziram à ADPF 403 e à ADI 5.527, pendentes de decisão final no STF e discutidas no tópico 3.1.

ou não, de pedidos de cooperação técnica formulados por autoridades brasileiras ou dos Estados Unidos para a obtenção de informações relacionadas à Petrobras, no âmbito da Operação Lava Jato. Acrescentou-se, ainda, que em caso de efetiva existência dos atos de cooperação, devem ser revelados apenas o nome da autoridade responsável, a investigação a que se referem, a descrição das provas ou informações solicitadas e a sua finalidade. Caso não tenha havido cooperação pelos meios oficiais, tal informação também deverá ser prestada à defesa do ex-presidente. (BRASIL. STJ – MS 26.627/DF, Rel. Ministro SÉRGIO KUKINA, Primeira Seção, julgado em 09/03/2022, - DJe 27/04/2022).

As medidas de bloqueio de aplicações de internet foram apenas um exemplo de que uma determinada decisão, de cunho jurídico, formalmente interna e doméstica, possui a aptidão de produzir, materialmente, imediatos efeitos políticos extraterritoriais.

Comentando o caso brasileiro do *WhatsApp*, Souza e Mangeth (2019) recordam que as ações interventivas diretas na infraestrutura impactam seu funcionamento técnico, cuja reação de países vizinhos, que se interconectam à internet, seria desviar suas conexões para diferentes rotas não bloqueadas, optando pela conexão via outros países, como o Panamá ou os EUA, ao invés da passagem pelo território nacional.

Mas há também outra fonte de efeitos extraterritoriais. Fontes que não decorrem necessariamente de um ato decisório como a suspensão de um aplicativo. Mas que podem decorrer da própria modelagem de cibersegurança de um ator conectado transnacionalmente. Um exemplo desse caso são os próprios *backdoors* inseridos na infraestrutura comunicativa. Eis o que pontuam Souza e Mangeth:

> não apenas as medidas de bloqueio podem ter efeitos extraterritoriais, mas que a própria criação de uma vulnerabilidade no sistema criptográfico por certo o governo termina por gerar uma fragilidade que ultrapassa os limites de suas fronteiras nacionais (2019, p. 83).

No tópico 3.3, pudemos constatar que as fontes dos *backdoors* podem ser voluntárias, concedidas em razão e para o Estado, ou acidentais, oriundas da própria dinâmica das interações entre dispositivos conectados. O grande problema é que a simples exploração dessas vulnerabilidades por um país produz imediatas e relevantes ressonâncias em outro.

Conforme explica Liguori Filho (2019), ainda que diferentes países debatam as mesmas questões, a solução por uma ou outra regulação doméstica tem a aptidão de produzir efeitos extraterritoriais, impactando transnacionalmente a regulação de outra jurisdição e a integridade do sistema criptográfico em nível global. Quanto ao ponto, Liguori Filho alinha-se a Souza e Mangeth (2019) no que toca aos efeitos transnacionais de regulações locais: eventual fragilização produzida na criptografia por um país afetará inevitavelmente outros países que utilizem a ferramenta.

É que a abordagem tradicional do dilema cripto costuma levar em conta apenas um foco vertical e nacional sobre como deve ser a modelagem[112] entre a política criptográfica e o acesso aos dados pelo governo local quando, na realidade, deveria, segundo os autores, ser enfrentada uma pré-condição factual do problema: o fato de que os serviços de comunicação e armazenamento de dados são operacionalizados globalmente através de um fluxo transfronteiriço de dados.

Em relatório publicado pela UNESCO (2016) já se reconhecera que a encriptação e os seus mecanismos de contorno possuem uma dimensão internacional significativa em função da natureza internacional das redes de comunicação e da Internet, bem como das dimensões do comércio, globalização e segurança nacional. Nessa linha, reconhece-se que a transnacionalidade dos fluxos informativos embota as linhas divisórias entre as dimensões internacionais e as nacionais, de modo que as políticas de encriptação necessitam de acordos internacionais para serem efetivas.

Essa dinâmica de ação interna-reação externa introduz o problema mais espinhoso do debate sobre as modelagens de segurança cibernética e suas ressonâncias transnacionais, tema do qual o subconjunto da criptografia e seus meios de contorno fazem parte.

Esse problema vem sendo nomeado como o "*problema do país menos seguro*" (*least trusted country problem)*, apresentado na doutrina nacional por Liguori Filho com ancoro em Swire e Ahmad, em que se apresenta a máxima: "regulações domésticas, impactos transnacionais" (Liguori apud. Swire e Ahmad, 2019, p. 104-105).

Mas o que é exatamente o "*problema do país menos seguro*"?

[112] Na doutrina nacional, já foram apontados alguns dos principais modelos regulatórios da criptografia adotados no mundo através de uma perspectiva de Direito Comparado. Os autores apontam, exemplificativamente, sete principais modelos: a) proibição/criminalização da criptografia; b) Limitação do tamanho de chaves criptográficas; c) obrigação de assistência (genérica); d) obrigação de assistência (específica); e)Licença/autorização governamental para criptografia; f) Estímulo à criptografia e; g) mecanismos alternativos de investigação – exploração de vulnerabilidades pelo governo. (SALVADOR, João Pedro Favaretto; LIGUORI FILHO, Carlos Augusto; DOS SANTOS, Guilherme Kenzo e GUIMARÃES, Tatiane B. Criptografia e Direito: uma perspectiva comparada, *in*: DONEDA, Danilo e MACHADO, Diego. *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, pp. 107-119). Por sua vez, para um mapeamento da criptografia em cada país, ver o paradigmático portal *Crypto Law Survey* do professor Bert Jaap-Koops, em (JAAP-KOOPS, Bert. Crypto Law Survey Version 27.0, 2013. Disponível em: <http://www.cryptolaw.org/>. Acesso em: 16 out. 2021.

Um exemplo dado por Liguori Filho ilustra melhor o problema:

> se um cidadão holandês se comunica com alguém na Índia por meio de um aplicativo que cumpre as regulamentações indianas sobre limitação de chaves os seus dados estão tão seguros quanto o governo indiano permite, independentemente da localização do holandês (2019, p. 104-105).

Segundo Liguori Filho, esse problema implica na conclusão de que os dados compartilhados entre usuários de diferentes países estarão tão seguros quanto o país menos seguro dos polos da comunicação.

Propomos, com a devida licença e de boa-fé, considerar que não se trata apenas das proteções adotadas pelo país-polo emissário e pelo país-polo destinatário. Não apenas emissário e receptor. Mas todos aqueles países – e, por que não, atores não estatais? - pelos quais os dados passem durante o caminho entre emissor e destinatário. Nesse sentido, os dados compartilhados entre usuários de diferentes países estarão tão seguros quanto o ator menos seguro pelos quais os dados passem na execução da comunicação.

Pensamos, assim, que esse problema introduz o critério da menor proteção[113], uma espécie de postulado do ponto frágil da infraestrutura conectada.

[113] Interessante pode ser a possibilidade de analogia. Um outro campo em que uma regulação local possui impactos extraterritoriais diretos é o meio ambiente, justamente pelo fato de que a poluição não conhece fronteiras. Seu raio de ação é ontologicamente transnacional. Neste campo, por sua vez, consta o critério da norma mais protetiva, mas ainda assim não é raro vislumbrarmos, na realidade concreta da vida, que os desejos de grandeza se sobrepõem à racionalidade protetiva. Se no espaço comum por excelência, o ambiente, ainda assim uma mesma poluição é enfrentada sob diferentes filtros técnicos de segurança ambiental, mas aplicados às diferentes indústrias, sob as variáveis das diferentes localidades normativas, engendrando, pois, diferentes assimetrias de proteção da vida, há de convir que é quase que romântico crer que haverá uma proteção paladina num campo menos central à vida humana, como são as comunicações interconectadas. No entanto, o pessimismo, ou realismo para alguns, não pode ser paralisante. Ele apenas deve levar em conta a hipótese mais danosa possível antes da ação planejada, de modo que estejamos a par da realidade concreta, compreendendo a primazia do problema, o qual pode encontrar respostas através da colaboração do que já foi discutido em outros ramos. Conforme leciona o professor Perlingieri, "*o fracionamento da matéria jurídica e do ordenamento em ramos, se tem sentido porque divide por competência e necessidade de exposição uma matéria em si mesma única, não deve significar que a realidade, logo o ordenamento, seja divisível em diversos setores dos quais um seja autônomo em relação ao outro a ponto de proclamar-se independente. O estudo do direito não deve ser feito por setores pré-constituídos, mas por problemas, com especial atenção às exigências de vez em vez emergentes como, por exemplo, a habitação, a saúde, a privacidade, etc. Os problemas concernentes às relações civilísticas devem ser enfocados de modo a recuperar os valores publicísticos para o direito privado e os valores privados para o direito público."* (PERLINGIERI, Pietro. O Direito Civil na Legalidade Constitucional. 1ª ed., Editora: Renovar, 2008, pp. 149-150). Por sua vez, para uma defesa da analogia como ferramenta essencial ao ensino jurídico, sobretudo em campos nos quais os caminhos ainda não foram devidamente pavimentados, ver: (WEINREB, Lloyd L. *A Razão Jurídica: o uso da analogia no argumento jurídico.* São Paulo: WMF Martins Fontes, 2008, pp. 97-142).

Avaliamos, ainda, ser pertinente a relação entre o problema do país menos seguro e o paradoxo da conectividade, explicado no tópico 3.3, na medida em que aquele problema – do país menos seguro – opera como uma possível particularização, de índole jurídico-política, deste último – paradoxo da conectividade – que é de ordem ontológica. Ambos tomam como denominadores comuns a infraestrutura de TICs e o fluxo informativo que corre por ela numa escala transnacional, de modo que a segurança do todo pressupõe o diagnóstico das vulnerabilidades intermitentes e difusas espraiadas em múltiplos atores (ou dispositivos, ou países, ou sujeitos, etc.).

O problema do país menos seguro considera a política regulatória cibernética de um ou outro país (modelagens dos países A, B, C, D, etc.). Se ela for frágil, a proteção do todo também o será. O paradoxo da conectividade, por sua vez, também opera sob essa lógica: à medida que se complexificam os sistemas e diferentes funcionalidades interagem, novos pontos frágeis se abrem, supervenientes vulnerabilidades se formam e as capacidades de ataque são redirecionadas para o ponto mais frágil. Se um nódulo da conectividade for frágil, a proteção será medida à luz da segurança desse nó, tal como o exemplo fornecido por Carissa Véliz (2021), no tópico 3.3, de que seu telefone estará tão seguro quanto o for o seu aplicativo menos seguro.

Circunscrevendo esse ponto frágil: um país menos seguro. Um ator menos seguro na conectividade total.

Resta monitorar onde se aloca, na infraestrutura, esse "calcanhar de Aquiles cibernético", ou "calcanhares", que estão sempre mudando de lugar à medida que a conectividade evolui e as técnicas protetivas autofágicas não mais cumprem o seu papel. Vulnerabilidades difusas e dinâmicas. Remédios tecnocráticos sob condição resolutiva.

O conhecimento desses problemas compõe, historicamente, o conjunto de saberes privilegiados e segmentados das comunidades de Inteligência e, atualmente, estão sendo assimiladas e exploradas por parte do setor privado mediante o crescimento da indústria privada da ciber(in)segurança,[114] beneficiada pela

[114] Para maiores detalhes sobre a consolidação dessa indústria da ciber(in)segurança, como um desdobramento dos conhecimentos da espionagem, mas agora aplicados pelo setor privado, ver: <https://web.archive.org/web/20090205143528/http://michaelsmithwriter.com/pdf/intelligence_co

ausência da regulação, ainda que muitas das práticas mercantis deflagradas por esse segmento venham sendo condenadas, por exemplo, pela Anistia Internacional.[115]

Dentro desse jogo de regulações locais, efeitos extraterritoriais, ademais, não faltam trocas de acusações entre os Estados a respeito do grau de segurança conferido aos dados, numa arena de (des)confiança recíproca, mas, por vezes, pontuando-se uma certa valoração positiva em favor do Ocidente quanto ao papel protetivo dispensado aos dados e, por outro lado, um desvalor em relação a outros países, circunstância que revela pequenos traços maniqueístas, ainda que involuntários, pois o realismo político e a experiência sempre atestam que não há, no cenário internacional, virtudes, mas interesses.

Eis uma longa passagem que representa as diversas questões envolvidas e as pequenas sutilezas patrióticas:

> O maior impedimento para o acesso excepcional pode ser a jurisdição. Incorporar o acesso excepcional já seria arriscado o suficiente, mesmo que apenas uma agência de aplicação da lei no mundo o possuísse. Mas, isso não é apenas um problema dos EUA. O governo do Reino Unido promete editar legislação que obrigue os provedores de serviços de comunicações, incluindo corporações sediadas nos EUA, a conceder acesso às agências policiais do Reino Unido, e outros países certamente seguirão o exemplo. A China já sugeriu que pode exigir

mpanies.pdf>. Acesso em 20 abr. 2022.; Para exemplos de repercussões dessas práticas nos EUA, ver <https://www.wired.com/story/the-murky-merits-of-a-private-spy-registry/>. Acesso em 20 abr. 2022; Ou na Inglaterra, ver: <https://www.voanews.com/a/london-spy-industry-private-sector/3718445.html>. Acesso em 20 abr. 2022; E mesmo no Brasil, no que toca as tentativas de contratação de um software espião Israelense, o *Pegasus*, pelos Procuradores da Lava-Jato: <https://www.cartacapital.com.br/politica/procuradores-da-lava-jato-tentaram-comprar-programa-espiao-israelense-pegasus/> Acesso em 12 mai. 2022.; Em um momento posterior, por sua vez, verifica-se a tentativa do governo federal negociar outro *software* espião, também de origem israelense, outrora utilizado durante a Primavera Árabe, o *Dark Matter* <https://revistaforum.com.br/politica/governo-bolsonaro/2022/1/18/darkmatter-software-espio-negociado-pelo-gabinete-do-odio-usado-por-ditaduras-108884.html>. Acesso em 12 mai. 2022.; Um instrumento interessante e que vem sendo mercantilizado abertamente através do regime privado do Direito do Consumidor é o *IMSI Catcher*. Segundo Bruce Schneier, uma ferramenta móvel que emula torres de telefonia de celular, sendo capaz de coletar conversas telefônicas, mensagens de texto e navegação na web daqueles celulares que estejam sob o seu raio de ação. (SCHNEIER, Bruce. Data and Goliath. London: W.W. Norton & Company, 2015, p.68). Procuramos a comercialização do referido bem no mercado nacional e encontramos pelo valor de R$ 6.000.000,00 (seis milhões de reais), na data de 20/04/2022. em <https://mercadoespiao.com.br/poderoso-coletor-portatil-de-imsi-imei-tmsi-com-interceptacao-celular.html>. Acesso em 20 abr. 2022. Interessante seria verificar seu raio de ação para coletar a possível proximidade de dispositivos móveis e seus possíveis identificados, mas em zonas residenciais onde as decisões políticas fundamentais da República são tomadas nos bastidores. Ou em zonas periféricas em que se aplica a necropolítica. Talvez, num futuro próximo, a Urbe seja planejada levando-se em conta essa dinâmica tecnológica, agora terceirizada no balcão do consumo.

[115] Informação colhida de <https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/>. Acesso em: 01 jun. 2022.; E também de: <https://www.amnesty.org/en/latest/news/2022/04/spain-pegasus-spyware-catalans-targeted/>. Acesso em: 1 jun. 2022.

> acesso excepcional. Se um desenvolvedor com sede na Inglaterra implanta um aplicativo de mensagens usado pelos cidadãos da China, este deve fornecer acesso excepcional às agências chinesas? Quais países têm suficiente respeito pelo Estado de Direito para participar de uma estrutura internacional de acesso excepcional? Como essas determinações seriam feitas? Como as aprovações em tempo hábil seriam concedidas para os milhões de novos produtos com recursos de comunicação? E como esse novo ecossistema de vigilância seria financiado e supervisionado? Os governos dos EUA e do Reino Unido têm lutado muito para manter a governança da Internet aberta, diante das demandas de países autoritários que defendem o controle estatal. A pressão por acesso excepcional não representa uma forte inversão política? (Abelson et. al. *in: Keys Under Doormats*, 2015, p. 3 – Tradução livre).

Uma pergunta muito simples e que pode ser direcionada a esse ambiente em que o princípio ordenador é a desconfiança: há alguma garantia de que absolutamente nenhum governo, nenhuma polícia, nenhuma agência de espionagem, nenhuma empresa em concorrência industrial, nenhum coletivo privado – criminoso ou não –, nenhum indivíduo sequer jamais irá explorar as vulnerabilidades acidentais engendradas pelas próprias TICs?

Aparentemente, a segurança cibernética em nível transnacional está ancorada em uma imensa desconfiança recíproca por todos os lados, tendo por premissa de sua dinâmica a insegurança, isso porque a efetiva e substancial proteção dos dados e/ou das infraestruturas através da renúncia à exploração de *backdoors* – os quais são incessantemente renovados – pressupõe um acordo recíproco, universal e estável, o que pode revelar um certo romantismo à luz da experiência prática. Pressupõe-se uma autocontenção difícil de entregar na geopolítica. O movimento de um único ator tem a aptidão de reverberar nas bases do todo.[116]

[116] A constatação do problema das reatividades recíprocas, sobretudo quando diante da introdução de novos métodos, os quais podem ser tecnológicos, pode ser mais antiga do que parece. Uma curiosa relação entre invenções, Defesa e supervisão pública pode ser colhida, por exemplo, da filosofia política de Leo Strauss, o qual, com ancoro em Maquiavel, disserta a respeito dos ensinamentos do Realismo Político, no próprio nascimento da Modernidade, e no que toca a incessante introdução de novos métodos. Como é de sua filosofia, Strauss, por meio de Maquiavel, fala nas entrelinhas com o leitor, em obra de 1954, no bojo da guerra fria. No entanto, as lições são atuais. Eis a passagem: *"Ao homem moderno, exatamente como ocorria com o homem pré-moderno, não é possível escapar à imitação da natureza tal como ele a entende. Imitando um universo em expansão, o homem moderno veio se expandindo cada vez mais, tornando-se, assim, cada vez mais raso. Confrontados com esse assombroso processo, não conseguimos deixar de nos perguntar que deficiência fundamental da filosofia política clássica pode ter dado ensejo à aventura moderna enquanto um empreendimento que se pretendia razoável. Desconsideramos as muitas respostas que pressupõem a verdade das premissas modernas. Os clássicos eram, para todos os propósitos práticos, o que hoje se chama de conservadores. Entretanto, em contraste com muitos dos conservadores atuais, eles sabiam que não é possível desconfiar da mudança política ou social sem desconfiar das mudanças tecnológicas. Por isso, não favoreciam ou incentivavam as invenções, a não ser, talvez, nas tiranias, isto é, nos regimes cuja mudança é manifestamente desejável. Eles exigiam a estrita supervisão moral e política das invenções; à cidade boa e sábia cabe determinar*

O mero desrespeito por um único Estado, ou mesmo por algum ator não estatal, inaugura um processo reativo em cadeia, remodelando posicionamentos de atores públicos e privados, ante a ausência de regras comuns que impliquem em renúncias recíprocas de posições de poder/saberes. Ainda que existisse um regramento, difícil crer que exista paz por decreto.

Por sua vez, as perplexidades levantadas pela comunidade técnica a respeito de como seria realizada uma supervisão das tecnologias – tópico 2.4 – aparentam ser sintomas de um problema histórico mal colocado: a ideia de que a internet é um espaço livre, não ocupado por opacos segmentos de poder. O fato de não haver uma autoridade pública central na internet, visível, não implica numa necessária descentralização material, simétrica e/ou equânime dessa arena. Pelo contrário. O mapa de seu controle é que é pode estar embotado.[117]

A problemática introduzida pelos *backdoors*, na verdade, por qualquer outra modelagem de cibersegurança jurisdicionalmente assimétrica também passa pela necessidade de reconhecer o espaço cibernético como uma arena pública mais transparente, de premissas que possam ser compartilhadas, valores publicísticos e comuns, justamente tudo o que ameaça o protagonismo de uma atual arquitetura reservada a poucos atores dominantes.

De acordo com relatório publicado pela UNESCO (2019), por ora, ressalta-se a necessidade da construção de uma coordenação internacional na formulação das políticas criptográficas. Também deve ser enfatizado, nesse problema, o papel dos intermediários. Intermediários compreendidos como os agentes de tratamento de dados com escala de operação transnacional, justamente porque eles são, ao menos para os fins iniciais do debate, o elemento comum entre as diversas jurisdições e suas modelagens internas de cibersegurança.

---

quais invenções devem ser utilizadas e quais devem ser suprimidas. Contudo, eles foram obrigados a permitir uma exceção crucial. Eles tiveram de admitir a necessidade de incentivar as invenções relativas à arte da guerra. Eles tiveram de se curvar à necessidade da defesa ou da resistência. Isso significa, porém, que eles precisaram admitir que a supervisão moral e política das invenções pela cidade boa e sábia se encontra necessariamente limitada pela necessidade de se adaptar às práticas de cidades moralmente inferiores que desdenham essa supervisão porque o seu fim é a aquisição ou o conforto." (STRAUSS, Leo. *Reflexões sobre Maquiavel*. Tradução e apresentação à edição brasileira Élcio Verçosa. 1ª.ed. São Paulo: É Realizações 2015, p. 361-362.)

[117] Para uma ampla discussão a respeito da metáfora do ciberespaço livre, e a consequente associação de diferentes partes da internet à diferentes jurisdições ver (GOLDSMITH, JACK e WU, Tim – *Who Controls the internet?: illusions of a Borderless World*. New York: Oxford University Press, 2006).

A transnacionalidade e a insegurança são pré-condições de ordem factuais do fenômeno, realistas, necessárias ao caminho para o coração do problema. O problema do país menos seguro pode ser sintomático de uma abordagem excessivamente verticalizada, calcada numa visão de túnel. Ela embotaria a visão de que há um problema de enfraquecimento de soberanias[118] no subterrâneo da segurança cibernética e que a criptografia pode desempenhar uma função capital. Um incômodo que poderia ser mais bem explorado nos estudos futuros.

Apesar da relevância desses ponto, essa condição é constatada em relatório publicado pela UNESCO, mas de forma muito tímida e através de um único parágrafo. Detalhe para a passagem em que se afirma "o que não é suficientemente reconhecido" e para a passagem sobre o "uso dos métodos criptográficos" como meio de desviar *jurisdições*. É pertinente a longa citação, em tradução livre:

> Nos debates sobre política criptográfica, a questão do acesso legal pelo governo – e as condições sob as quais esse acesso deve ocorrer para respeitar os direitos humanos – tem um foco vertical e nacional. O que se entende aqui é que a discussão aborda os deveres e responsabilidades do Estado em relação aos membros de sua própria sociedade, e as leis e regulamentos que devem ser estabelecidos em conformidade, respeitando os direitos humanos. Em cada país, a preocupação com o acesso normalmente está concentrada na falta de acesso pelas autoridades competentes. O que às vezes não é reconhecido suficientemente é o fato de que os serviços e ferramentas em foco não se encerram nas fronteiras. O mesmo se aplica ao governo e a outros atores que eventualmente busquem obter acesso à informação e à comunicação transnacionalmente. A dimensão internacional e a possibilidade de acesso transnacional, efetivamente, significa que os agentes estrangeiros devem

[118] Um interessante julgado envolvendo soberania e tratamento de dados no âmbito da jurisdição constitucional, por exemplo, foi travada na ADI 4.829, de Relatoria da Ministra Rosa Weber, em que o STF entendeu pela constitucionalidade de disposições normativas sobre a dispensa de licitação na contratação de serviços de tecnologia da informação estratégicos à Administração Pública, no caso, a contratação do SERPRO. Nesse sentido, decidiu-se que os postulados constitucionais da inviolabilidade do sigilo de dados pessoais (art. 5º, XII e XXXIII, da CF) e da soberania nacional (Arts. 1º, I, e 170, I, da CF) reclamam a imposição de restrições ao tratamento de dados pessoais, por entidades privadas, para fins de segurança pública, defesa nacional ou segurança da informação do Estado e dos administrados. Assim sendo, os Artigos 170, parágrafo único, e 173, caput, da CF autorizam o legislador a restringir o livre exercício de atividade econômica para preservar outros direitos e valores constitucionais, destacando-se, no caso de serviços estratégicos de tecnologia da informação contratados pela União, os imperativos da soberania, da segurança nacional e da proteção da privacidade de contribuintes e destinatários de programas governamentais. (BRASIL. STF, ADI 4.829 DF. Relatora: Ministra Rosa Weber. 09/08/2012. JusBrasil. 2012. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282) Acesso em: 01 jun. 2022; Por outro lado, conforme aponta Sérgio Amadeu, no dia 27 de maio de 2020, o Ministério da Ciência e Tecnologia assinou um acordo com a empresa norte-americana Cisco para a construção de uma plataforma digital inteligente para o governo federal. Na mesma linha, o SERPRO, estatal responsável pela proteção das informações da Receita Federal, agora, no governo Bolsonaro, acaba de fechar parceria com a *Amazon* para a revenda de espaços na nuvem da *Amazon Web Services, Inc*. (SILVEIRA, Sérgio Amadeu da. *Brasil, colônia digital.* Disponível em: <http://www.ihu.unisinos.br/600360-brasil-colonia-digital-artigo-de-sergio-amadeu>. Acesso em: 14 dez. 2020.

> ser incluídos nos modelos de ameaças para proteção de dados e políticas de segurança cibernética. Esse é um dos motivos pelos quais os métodos criptográficos podem ser ativamente explorados para restringir e moldar o acesso transnacional aos dados pelos governos (Schulz e Hoboken, 2006, p. 57).

Se os agentes estrangeiros devem ser incluídos na modelagem da proteção de dados e da criptografia, então seria de bom tom reconhecermos, ao menos, as capacidades de ataque desses agentes, seu conjunto de saberes opacos e os seus meios sub-reptícios de acesso aos dados à revelia da criptografia em uma escala transnacional como marcos para o desenvolvimento de uma defesa mais substancial e menos ingênua, tanto da privacidade de cada um de nós, quanto da soberania.

Suponhamos, provisoriamente, que no Brasil se reconheça a primazia da criptografia sobre a interceptação, de modo que o entendimento se consolide na impossibilidade de os órgãos nacionais de investigação acessarem o conteúdo dos dados, tal como desenhado no voto do Ministro Fachin.

Suponhamos, agora, que empresas de tecnologia da informação de matriz estrangeira operem no Brasil, mas com acordos de espionagem com seus respectivos governos, seja através de *backdoors* acidentais, frutos de falhas técnicas na "normalidade" da cadeia industrial, seja por meio da submissão e cooperação com órgãos de inteligência estrangeira como impõem os diversos acordos informais opacos.

Qual seria o efeito desse conjunto? Não poderíamos ser empurrados para uma espécie de assimetria soberana-persecutória? Uma mesma empresa, de matriz internacional, ainda que considerada nacional através da "lavagem" jurídica do Código Civil, quando submetida às requisições realizadas pelo aparato persecutório nacional estaria protegida pela interpretação que acoberta o conteúdo dos dados pela criptografia, podendo argumentar, assim, que não possui acesso ao conteúdo das mensagens, ora escorando-se no respeito à criptografia como um elemento inerente à integridade de sua própria matriz tecnológica, ora invocando decisão judicial superior em seu favor.

Por outro lado, se essa mesma empresa colabora com um outro Estado soberano através de *backdoors* em sua tecnologia, de modo que os órgãos de investigação desse outro Estado tenham acesso ao conteúdo das informações, até mesmo por outros meios mais sofisticados e sub-reptícios de acesso, então não nos

encontraremos numa posição de fragilidade persecutória-judicial já de largada? Uma postura de automutilação involuntária do próprio sistema persecutório-judicial doméstico a pretexto de boas intenções protetivas das comunicações privadas? Seria o "sim, agora" para órgãos estrangeiros mais bem aparelhados e o "não, ainda não" para órgãos nacionais historicamente deficitários de meios efetivos, sobretudo quando confrontados com a luta histórica, cripta, pelo acesso ao inteligível. O resultado dessa ética não poderia ser um convite à sobreposição de ordenamentos opacamente?

Essa série de problemas certamente não pode nos levar à conclusão de que eventual solução para essa assimetria de acessos às informações tuteladas pelas técnicas de cibersegurança – como a criptografia – seria ignorar por completo o potencial protetivo dessas ferramentas e, assim, franquear-se o amplo acesso aos dados pelos órgãos de repressão nacionais, numa espécie de compensação investigativa-competitiva. O correto seria o respeito recíproco entre os atores envolvidos, sejam órgãos nacionais, sejam órgãos externos e/ou atores privados. Mas o mundo não é simples e romântico assim. E, nesse sentido, voltamos a recair naquele problema esboçado pouco acima de que a pacificação do problema pressupõe uma forte autocontenção, muito difícil de entregar transnacionalmente, ou seja, na geopolítica. Desconfianças e hesitações no horizonte.[119]

O *trade-off* que envolve a criptografia pode ser muito mais amplo e profundo do que se ventila. Não apenas Privacidade vs. Segurança, tampouco Segurança vs. Segurança. Ele parece envolver a própria presença de uma ou outra jurisdição na luta pela intensidade do acesso aos dados transnacionalmente, bem como as ressonâncias desse conflito não apenas no que tange à tutela dos direitos fundamentais de seus cidadãos, mas também no que toca, para começar, a própria

[119] "Quando a posição é tal que nenhum dos lados terá vantagem em fazer o primeiro movimento, é chamado de campo a contemporizar." (Sun Tzu, sobre os Terrenos, em A Arte da Guerra, p.120). Eis também um interessante diálogo: " - Andy Muller-Maguhn: "Só estou tentando fazer com que a gente pense de um jeito positivo o que seria uma boa política. O que você acabou de elaborar, para mim, neste estágio, é um pouco complicado demais. Estou tentando simplificar um pouco. Tem um cara chamado Heinz von Foerster - o padrinho da cibernética - que elaborou um conjunto de regras, e uma das regras era: "Sempre haja de modo a aumentar as opções". Então, com as políticas, com a tecnologia, com o que for, sempre faça o que levar a mais e não há menos opções. - Julian Assange: Na estratégia do xadrez também." (ASSANGE, Julian, APPELBAUM, Jacob, MULLER-MAGUHN, Andy, ZIMMERMANN, Jeremy. *Cypherpunks: liberdade e o futuro da internet*. Tradução Cristina Yamagami, São Paulo: Boitempo, 2013. p. 116). Eis um interessante imperativo categórico.

concorrência geopolítica entre efetividades de diferentes aparatos persecutórios-judiciais nacionais, possivelmente prejudicando, sobretudo, aqueles Estados cuja formação da verdade jurídica não esteja afinada com a nova e sutil introdução de novos métodos de produção da prova, hoje renovados através do convite dourado pregado no mural daqueles que imprimem a *nova Era de Ouro*, daqueles que possuem a gestão de imensos oceanos de informação e que, agora, aprenderam que os dados possuem externalidades positivas, de índole forense, prontas para serem consumidas pelo Estado.

Esse âmago poderia receber maiores atenções. Soluções? No mínimo ter uma consciência de onde nos situamos na História. O escopo é curto e já nos estendemos.

Como podemos, ao menos para fins iniciais, tentar nos proteger dos *backdoors* com os institutos jurídicos disponíveis em nosso ordenamento? Se, de um lado, isso for possível, quais obstáculos, por outro lado, seriam colocados logo de saída? Como a proteção técnica pela criptografia se encontra com institutos jurídicos nacionais relacionados à internet, à privacidade e à proteção de dados? Como a eventual (des)confiança nos elementos comuns da transnacionalidade, os intermediários, poderia ser mais bem enfrentada institucionalmente? E em quais institutos uma ação institucional zelosa pelos dados esbarraria? Necessário um último capítulo.

4. A PROTEÇÃO PELA SEGURANÇA E PELA TRANSPARÊNCIA

Nesta última etapa, buscamos apresentar algumas proteções contra os *backdoors* através dos institutos jurídicos ora disponíveis no ordenamento nacional, momento em que traçamos o enquadramento da criptografia como medida de segurança técnica da proteção de dados e das comunicações seguras na internet, atraindo disposições da Lei Geral de Proteção de Dados e do Marco Civil da Internet. Ademais, no afã de confrontar a opacidade e a desconfiança que pode pairar sobre eventuais intermediários colaboradores de outros governos, sinalizamos para ferramentas de transparência na LGPG, mas, desde já, apontamos para as possíveis dificuldades existentes nesse caminho.

Como a relação entre criptografia e *backdoors* pode ser endereçada para a Lei Geral de Proteção de Dados? Sucintamente, através das disposições sobre segurança, notadamente as medidas técnicas de segurança, tendo por eixo principal o Art. 46 da LGPD[120]. Mas, antes, alguns esclarecimentos são necessários.

4.1. Esclarecimentos Preliminares

Vimos nos capítulos anteriores que os *backdoors* representam vulnerabilidades presentes na infraestrutura comunicativa, falhas na segurança de um sistema aptas à exploração, seja para fins ilícitos ou para fins lícitos (ex: interceptação legal). A exploração dessas falhas pode ser realizada por atores autorizados ou por atores não autorizados.

Por outro lado, há um conjunto de medidas de segurança que tem por objeto justamente reduzir a superfície de ataque dessas vulnerabilidades à ação de terceiros não autorizados. A criptografia é um exemplo de medida de segurança, mas de ordem técnica. Para os fins aqui propostos, também poderemos utilizar a expressão medida técnica de cibersegurança.

[120] LGPD, Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Recordemos que toda a discussão a respeito da exploração de vulnerabilidades introduzidas para garantir o acesso autorizado do Estado foi travada no tópicos 2.2, no final do tópico 2.3 e no tópico 2.4, além de problematizada a questão das fontes das vulnerabilidades acidentais no tópico 3.3.

Na hipótese em que se discutiu a presença do Estado na infraestrutura comunicativa, foram apresentadas as matizes do dilema cripto, representadas pela tensão entre o aparato persecutório do Estado e os mercadores de tecnologia pelo fato de que a criptografia, como medida técnica de cibersegurança, bloquearia justamente esse acesso autorizado estatal, dificultando ou suprimindo algumas práticas constitucionais tradicionais, o que derivou na discussão sobre o *going dark* e, no Brasil, nos bloqueios do *WhatsApp*, levando às duas ações diretas expostas no tópico 3.1.

Nessa linha, se supormos provisoriamente que seriam constitucionais os *backdoors* do Estado, não faria sentido algum abordá-los através do subsistema da segurança de dados previsto na LGPD, pois o seu Art. 46, caput, cuida expressamente das hipóteses de acesso não autorizado. Portanto, eventual *backdoor* que garanta o acesso autorizado de algum órgão estatal não atrairia a aplicação do Art. 46.

Por outro lado, também vimos, através da lente dos especialistas técnicos, que essas próprias vulnerabilidades na segurança, viabilizadoras do acesso autorizado ao Estado, correm o risco de serem capturadas pela ação de terceiros mal intencionados.

É justamente essa hipótese de captura das vulnerabilidades de segurança por terceiros não autorizados que atrai a LGPD. Por exemplo, por alguma ação *hacker*[121] sobre o sistema. Um terceiro que se aproveitou do *backdoor* franqueado ao Estado. Nesse caso, haverá acesso, mas não autorizado, ainda que a exploração tenha se operado sobre uma vulnerabilidade particularizada para a ação estatal, atraindo o Art. 46.

Há, ainda, a hipótese em que não haja o acesso de qualquer ator, seja ele um ator autorizado ou um ator não autorizado, mas que as próprias vulnerabilidades

[121] Correlatamente, acrescente-se que em 27 de maio de 2021 o Código Penal foi alterado pela Lei n.º 14.155 para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet.

acidentais de um sistema, sequer capturadas por algum sujeito, engendrem situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento[122] inadequado ou ilícito (Art. 46, caput, parte final). Nesse caso, aplica-se a Lei.

Um dos remédios para tratar dessas vulnerabilidades é justamente a criptografia, conforme expusemos nos tópicos 2.2 e 3.3, na medida que se trata de uma técnica apta a reduzir a superfície de ataque de um sistema. E é sobre as disposições normativas que dialogam com essa relação que iremos nos concentrar agora.

Resumindo, o ponto cuida justamente da exploração das vulnerabilidades:

i) ou por atores não autorizados (atores não credenciados constitucionalmente ao acesso autorizado)

ii) ou quando essas falhas, por si sós, acidentalmente, produzem situações-problema previstas na Lei: situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Em outras palavras, as vulnerabilidades funcionalizadas ao acesso autorizado dos eventuais órgãos credenciados[123] do Estado, vulnerabilidades

[122] A LGPD define tratamento em seu Art. 5º, X: tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[123] A expressão "órgãos credenciados" utilizadas aqui não diz respeito ao instituto jurídico do "credenciamento" propriamente dito, uma categoria própria do Direito Administrativo. Aqui, a expressão é empregada de modo informal, em sentido amplo, como sinônimo de órgãos públicos constitucionalmente autorizados à exploração de um *backdoor*, órgãos que, eventualmente, possuam o acesso autorizado às infraestruturas, muito mais no sentido de uma hipotética lista de atores constitucionalmente autorizados à exploração das vulnerabilidades para os estritos cumprimentos de seus fins constitucionais. Uma discussão não relacionada propriamente à exploração de *backdoors*, mas que é pertinente ao tema de um conjunto de órgãos públicos do Estado brasileiro e suas respectivas competências para o compartilhamento de acesso a dados para com a Agência Brasileira de Inteligência (ABIN) foi travada na ADI 6.529, em que se discutiu a constitucionalidade do condicionamento a ato da Presidência da República o fornecimento de dados à agência. Eis a decisão do STF, transitada em julgado: "O Tribunal, por unanimidade, confirmando cautelar deferida pelo Plenário do Supremo Tribunal, conheceu parcialmente da ação direta e deu interpretação conforme ao parágrafo único do art. 4º da Lei n. 9.883/1999 para estabelecer que: a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos

intencionais, não são objeto do enquadramento aqui proposto. No entanto, pontualmente, podemos pinçar essa hipótese e apresentar algum problema específico e relativo a essa espécie, mas que possa ter repercussões na discussão que ora se apresenta. Esse será o caso, mais adiante, em que trataremos da possibilidade de o Estado explorar essa vulnerabilidade intencional de forma abusiva.

Voltemos. O debate teórico a ser abordado dar-se-á em torno da proteção da segurança dos dados, mas com um olhar voltado para a ação dos agentes de tratamento[124] no que toca a adoção, por esses atores, de medidas técnicas preventivas ao dano, especificamente a criptografia. Assim sendo, estabelecemos um recorte em que não serão analisadas as ações repressivas ao dano[125], tampouco as medidas preventivas de segurança de ordem administrativa (Art. 46, caput, bem como os Artigos 50 e 51 da LGPD[126]).

fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso. Tudo nos termos do voto da Relatora. Plenário, Sessão Virtual de 1.10.2021 a 8.10.2021." BRASIL. STF, ADI 6.529 DF. Relatora: Ministra Carmén Lúcia. 04/08/2020. JusBrasil. 2020. Disponível em: < https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238 >. Acesso em: 15 dez. 2021.

[124] LGPD, Art. 5º Para os fins desta Lei, considera-se: IX - agentes de tratamento: o controlador e o operador; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

[125] Não é objeto desse estudo discutir as minúcias e os dissensos a respeito das teorias sobre a responsabilidade civil na LGPD. Para maiores detalhes quanto ao ponto na doutrina, ver, em vídeo, CAITLIN MULHOLLAND SAMPAIO em <https://www.youtube.com/watch?v=obJEro6QjRA>. Acesso em: 8 mar. 2022.; Ou, em texto, também (MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a lei geral de proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). Responsabilidade civil e novas tecnologias. Indaiatuba: Foco, 2020). Por sua vez, no sentido da responsabilidade subjetiva: (GUEDES, Gisela Sampaio da Cruz e MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro. 2ª Ed., São Paulo: Thomson Reuters Brasil, 2020, pp. 217-236). Diferentemente, no sentido de uma responsabilidade civil "proativa", nem subjetiva, nem objetiva, ver: (MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito proativo. Editorial. Civilística.com, a. 8. n. 3. 2019). Na jurisprudência, entretanto, consta recente julgado do STJ, tendo por objeto a responsabilidade civil envolvendo medidas de segurança. No caso, afastou-se a responsabilidade do provedor – Google – sob o fundamento de que a falha na segurança se deu por força exclusiva da vítima. BRASIL. STJ - REsp 1.885.201/SP, Rel. Ministra NANCY ANDRIGHI, Terceira Turma, julgado em 23/11/2021, DJe 25/11/2021.

[126] Para maiores detalhes quanto aos aspectos administrativos das medidas de segurança, ver os comentários ao Art. 50 da Lei Geral de Proteção de dados – LGPD em (PEROLI, Kelvin e FALEIROS JUNIOR, José Luiz de Moura. Art. 50, *in*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JUNIOR, José Luiz de Moura (coord.) – *Comentários à Lei Geral de Proteção de Dados: LEI 13.709/2018.* São Paulo: Editora Foco, 2022, pp.461-476).

O foco, aqui, por coerência ao que foi discutido ao longo desse trabalho, é verificar, inicialmente, a ação preventiva da proteção dos dados, de índole técnica, através da criptografia, e a cargo dos agentes de tratamento/intermediários, bem como a tangência dessas considerações com o instituto do incidente de segurança, o qual reputamos como uma etapa intermediária entre a ação preventiva e o dano.

Num segundo momento, discorreremos sobre a proteção dos dados através de uma possível ação institucional da ANPD sobre os agentes de tratamento considerando um quadro de desconfiança quanto ao zelo desses intermediários pela tutela da pessoa humana. Nesse momento, demonstraremos que alguns remédios protetivos podem, por sua vez, esbarrar em institutos jurídicos que fortalecem a opacidade corporativa, isso no bojo da própria Lei, tal como havíamos suscitado no último parágrafo do tópico anterior (3.5).

Por fim, mas sem procurar esgotar todas as possibilidades, abordaremos um caso envolvendo vulnerabilidades e transnacionalidade, uma referência concreta em que convergem diversos aspectos abordados ao longo desse trabalho, além de refletir uma abertura para a futura internalização de outros institutos ao problema aqui discutido.

Pois bem. Avancemos.

Uma pergunta inicial seria: por que enfatizar a segurança dos dados através dos agentes de tratamento e não por meio da ação dos próprios titulares?

Primeiramente, por uma questão de coerência, na medida em que ressaltamos ao longo desse estudo a relevância do papel dos atores que operam as infraestruturas tecnológicas, considerando-os um denominador comum dentro do problema da transnacionalidade dos fluxos e armazenamentos informativos.

Em segundo lugar, porque também somos forçados a assimilar uma pré-condição factual presente em qualquer debate que envolva a privacidade: a realidade concreta de que as pessoas humanas se encontram em uma posição desfavorável quanto à tutela de seus direitos, dependendo largamente da ação diligente de terceiros, sejam eles os fabricantes de tecnologia comunicativas, os agentes de tratamento, ou os provedores de internet.

Essa pré-condição é reconhecida em relatório publicado pela UNESCO (2016), no qual se sustenta que a segurança dos dados dos titulares depende

consideravelmente da ação protetiva dos *intermediários*[127] e do conhecimento de suas estruturas jurídicas[128], ainda que os titulares/usuários possam, por si mesmos, implantar suas próprias proteções.[129]

O relatório supracitado, ademais, aponta para a premissa de que paira sobre o titular um possível estado de resignação quanto à proteção de sua privacidade, de sorte que não lhe seria desejoso se preocupar em renovar, por diversas vezes, a segurança de suas comunicações, mas decidir sobre tanto uma única vez.[130]

---

[127] Ao longo de todo o artigo da UNESCO sobre criptografia é empregada a expressão *intermediários*. Trata-se de uma expressão ampla e benéfica, reproduzida muitas vezes em nosso estudo, justamente porque tem a aptidão de abranger, em relação a LGPD, o conceito de *agentes de tratamento*, um conjunto de atores composto por *controladores* e *operadores* e, por sua vez, em relação ao MCI, também assimila os conceitos de *provedores de conexão* e de *provedores de aplicações*. Ademais, o emprego do termo "*intermediários*", uma vez provindo de um órgão internacional, emissor de diretrizes protetivas para inúmeros países, também estimula a possibilidade do compartilhamento de uma linguagem comum, condição esta que favorece a democratização do conhecimento através do compartilhamento de premissas. Para maiores detalhes, a expressão é empregada nas pp. 8; 52; 56; 57; 58; 62; 63 e 76: (SCHULZ, Wolfgang e HOBOKEN, Joris van - *Human rights and encryption*. UNESCO - Paris 07 SP, France, 2016). Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000246527?1=null&queryId=e05fdd78-68b9-4ff3-b7ce-b998b0c0cf01>. Acesso em: 20 dez. 2020.

[128] Verifica-se em relatório publicado pela UNESCO, um exemplo em que o conhecimento da estrutura jurídica do intermediário é de extrema relevância para a proteção da pessoa humana são os casos dos serviços de armazenamento de informações em nuvem: "Em relação à vigilância de usuários de serviços baseados em nuvem, em muitos aspectos um usuário não pode se proteger, mas depende do provedor de serviços na nuvem para o exercício dos direitos fundamentais e a proteção contra interferências arbitrárias da segurança nacional" (Schulz e Hoboken, 2016, p. 56). Essa pré-condição de fragilidade envolvendo a tutela dos dados nos serviços de armazenamento em nuvem reforça, pensamos, as problemáticas assimetrias jurisdicionais de acesso aos dados, conforme esboçado na parte final do tópico 3.4 ao dispormos sobre arranjos jurídicos que prestigiam "*a vantagem da equipe de casa."*

[129] No mesmo sentido, na doutrina nacional, Carlos Affonso de Souza: "um aspecto importante no debate sobre segurança é a compreensão do papel que desempenham os agentes de tratamento para garantir a segurança e o sigilo dos dados que estão sob seu controle. Muito se discute sobre como o sistema de proteção de dados deve garantir que o titular tenha controle sobre seus dados. Para além do controle exercido pelo titular, é necessário analisar como os dados são tratados por terceiros e quais são os deveres que precisam ser observados para que a tutela dos dados não seja frustrada." (SOUZA, Carlos Affonso. *Segurança e sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018, in:* TEPEDINO, Gustavo, FRAZÃO, Ana e OLIVA, Milina Donato (coord.) – *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2ª ed. - São Paulo: Thomson Reuters Brasil, 2020. p. 415).

[130] Interessante, ademais, é a sugestão contida em relatório da UNESCO no sentido de que seria útil o emprego de sistemas que reconheçam quando o titular necessita de um nível mais alto de criptografia e, assim, reagiriam automaticamente: "*Developing smart technologies that make encryption as convenient as possible would support privacy and freedom of expression, including special protection measures for journalists, media actors and vulnerable users such as women and girls and minorities. Systems that know when you need a higher level of encryption and automatically react to that demand could be helpful. Users might not want to decide again and again about the security of their communication, but might do it once when opting for a device or a software system*" (Schulz e Hoboken, 2016, p. 63). Nessa linha, pertinente é a Patente US 7602903 B2, concedida à Microsoft já em 2009 a respeito do mapeamento do grau de proteção oferecido por alguns sistemas criptográficos: (CRYPTOGRAPHY correctness detection methods and apparatuses. Depositante: Microsoft Corporation. US 7602903 B2. Depósito: 16 jan. 2004. Concessão: 13 out. 2009). Disponível em:

Passadas essas considerações iniciais, ingressemos no âmbito do subsistema da segurança.

4.2. Segurança e a Proteção Preventiva de Ordem Técnica Pelos Intermediários

No intuito de apresentarmos como criptografia e *backdoors* se articulam com as disposições sobre segurança, primeiramente é importante apontar a base normativa.

A segurança na LGPG[131], é composta pelos princípios setoriais: da segurança propriamente dita, da prevenção e da responsabilização, respectivamente incisos VII, VIII e X do Art. 6º.[132] Por sua vez, essa base principiológica é densificada por meio das regras previstas nos Artigos 46 a 49 da Lei[133], compondo a Seção I do capítulo VI, relativo à segurança e às boas práticas.

<https://ppubs.uspto.gov/pubwebapp/static/pages/landing.html>. Acesso em: 9 jul. 2022. Para vislumbrar outras patentes envolvendo relações com a criptografia, inclusive sob domínio das grandes empresas de tecnologia, ver: <https://patents.justia.com/search?q=cryptography>. Acesso em 09 jul. 2022.

[131] Por sua vez, para uma análise comparativa do tema da segurança entre a LGPD e o GDPR: MORAES PALMEIRA, Mariana. *A segurança e as boas práticas no tratamento de dados pessoais, in:* MULHOLLAND, Caitlin (org.) – *A LGPD e o novo marco normativo no Brasil.* Porto Alegre: Arquipélago, 2020. pp. 319-342.

[132] LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[133] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter

Acrescente-se, ainda, a necessária interface dessa base normativa com as disposições sobre segurança também previstas no Marco Civil da Internet e em seu Regulamento. No caso da Lei (MCI), o Art. 3º, V; o Art. 10, §4º e os Artigos 13, caput e 15, caput.[134] Por sua vez, no que toca ao Regulamento, para os fins aqui propostos, especialmente o Art. 13, IV[135].

Carlos Affonso de Souza (2020) aponta que a segurança e o sigilo são categorias chaves para a instrumentalização da proteção de dados e, nessa linha, reflete sobre a possibilidade da formação de uma consciência social protetiva dos dados, ainda que se dê a partir da visibilidade dos efeitos decorrentes das falhas na segurança, por exemplo, os vazamentos de dados.[136]

Considerando que os *backdoors* podem representar vulnerabilidades na segurança, exploradas por terceiros mal intencionados, o problema se conecta

ou mitigar os efeitos do prejuízo. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

[134] MCI, Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; MCI, 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. § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais; MCI, Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento; MCI, 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.

[135] Decreto 8.771/16, Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

[136] O autor também recorda que a proteção de dados pessoais não é exclusividade da LGPD. Nesse sentido, aponta e comenta outras fontes normativas desse sistema protetivo, tais como os incisos X, XII e LXXII, do Art. 5º, da CF/88; o CC/02; o CDC; o MCI: (SOUZA, Carlos Affonso. *Segurança e sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018*, *in:* TEPEDINO, Gustavo, FRAZÃO, Ana e OLIVA, Milena Donato (coord.) – *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2ª ed. - São Paulo: Thomson Reuters Brasil, 2020. pp. 416-419)

diretamente à disposição do Art. 46 da LGPD, que prevê expressamente o risco do acesso não autorizado.

O dispositivo também arrola as situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Para esse conjunto de situações-problema, entretanto, o Art. 46 prevê como remédios: as medidas de segurança, técnicas e administrativas[137].

Certamente, uma das medidas técnicas que poderia ser adotada pela ação diligente dos intermediários, para fins de proteção do titular/usuário, é a criptografia, justamente porque é uma técnica de cibersegurança que reduz a superfície de ataque de um sistema, dificultando a exploração ilícita de certa vulnerabilidade.

Sucede que não há, ao menos expressamente nas Leis, disposições que obriguem a adoção da criptografia pelos intermediários. O Art. 46 da LGPD apenas afirma que os agentes de tratamento devem adotar as medidas de segurança, sejam elas técnicas ou administrativas.

Ao analisar o emprego do verbo "dever" pela fonte legal, Souza (2020) endossa a interpretação de Márcio Cots e Ricardo Oliveira[138], no sentido da

[137] Apesar de o presente estudo focar em um recorte da relação dos *backdoors* com uma medida técnica de segurança, a criptografia, e não nos aprofundarmos nas medidas administrativas de segurança, alguns pontos são dignos de nota. Em relação às medidas administrativas direcionadas ao setor privado, Carlos Affonso de Souza recomenda que o agente de tratamento desenvolva uma política interna de segurança da informação (PSI), pois funcionaria "*como um código de conduta a ser seguido pelos funcionários e busca impedir o acesso daquelas informações por parte de terceiros não autorizados*" (SOUZA, Carlos Affonso. *Segurança e sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018, in:* TEPEDINO, Gustavo, FRAZÃO, Ana e OLIVA, Milena Donato (coord.) – *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2ª ed. - São Paulo: Thomson Reuters Brasil, 2020. pp. 430-431). Por sua vez, no caso de medidas administrativas a serem adotadas pelo Poder Público, ao menos em nível federal, é importante apontar para o Decreto n.º 9.637/18, que cuida da Política Nacional de Segurança da Informação – PNSI, prevendo expressamente a segurança cibernética como elemento integrante da segurança da informação (Art. 2º, I). Pontue-se que o conceito de informação contido neste Decreto é mais vasto do que o de dados pessoais, na medida em que a PNSI se refere à informação, generalizadamente, ao passo que dados pessoais são informações qualificadas pela possibilidade de identificação de uma pessoa natural (LGPD, Art. 5º, I). Nesse sentido, futuramente será necessário equacionar eventuais conflitos sobre medidas de segurança envolvendo a LGPD, mas também contidas na Lei de Acesso à Informação, no Decreto 7.724/12 e no Decreto da PNSI, caso haja sobreposição de informações públicas protegidas por medidas espraiadas nesses últimos três atos normativos, mas que, eventualmente também contenham dados pessoais. À título de exemplo, o possível conflito entre Incidentes de Segurança da LGPD e os Incidentes Cibernéticos do Poder Público associados à PNSI. Nesse sentido, ver o Decreto n.º 10.748/21, que Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

[138] SOUZA, Carlos Affonso. *Segurança e sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018, in:* TEPEDINO, Gustavo, FRAZÃO, Ana e OLIVA, Milena Donato (coord.) – *Lei*

imperatividade das medidas de segurança por parte dos agentes de tratamento em favor dos titulares como um meio preventivo de tutela de seus direitos, sob pena de sanção. Nessa linha, afasta-se o enquadramento no sentido de ser uma faculdade dos agentes de tratamento para com a adoção da proteção adequada.

Por outro lado, a despeito de a LGPD, por meio da regra de seu art. 46, impor que os agentes de tratamento devem adotar medidas técnicas e administrativas adequadas à segurança dos dados, não há clareza a respeito da específica adoção da encriptação como técnica obrigatória a ser observada pelos agentes de tratamento.

É que o §1º do Art. 46, direcionado exclusivamente às medidas técnicas de segurança, reserva à ANPD a competência material para fixar padrões técnico-protetivos mínimos, obviamente em casos que envolvam o tratamento de dados pessoais. No entanto, emprega-se a expressão "poderá dispor sobre padrões técnicos mínimos".

Entendemos que, ao pertencer a Administração Pública, a expressão "poderá dispor" poderia ser interpretada como um "poder-dever" da ANPD, para aqueles que objetivam construir uma força obrigatória da criptografia, sob pena de contribuir para um quadro de omissão inconstitucional quanto a sua missão protetiva.

Há que se considerar, ainda, que o §3º do Art. 48 da LGPD prevê uma importante consideração a ser feita pela ANPD no que toca a avaliação de um incidente de segurança:

> no juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los (§3º do Art. 48 da LGPD).

Ao prever que a ANPD irá considerar a adoção de medidas técnicas que tornem ininteligíveis os dados, a Lei sinaliza para a criptografia, senão de forma obrigatória e expressa, ao menos como um estímulo à sua adoção, na medida em que essa técnica pode ser elemento atenuante de eventual sanção, por força do inciso

Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 2ª ed. - São Paulo: Thomson Reuters Brasil, 2020. pp. 430-431).

VIII do §1º do Art. 52.[139] Recorde-se, ademais, que encriptar é tornar relativamente ininteligível um objeto, exceto para aqueles que portem as chaves da decriptação, as chaves da inteligibilidade.

Em sede de reforço, é relevante à construção de um adequado grau protetivo tomar-se, como parâmetros suplementares, as disposições dos caputs dos Artigos 13 e 15 do MCI, que dispõem sobre ambiente de controle e segurança no que toca a guarda de registros de conexão e de aplicações, ainda que o MCI reserve esse ambiente controlado e de segurança para a esfera regulamentar:

> MCI, Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> MCI, 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.

Esses marcos legais são desdobrados no Art. 13 do regulamento que, em seu inciso IV, prevê o uso obrigatório de medidas técnicas que garantam a inviolabilidade dos dados, no entanto, aparentemente, apenas recomenda a encriptação ou outra medida equivalente. Salvo melhor juízo, há uma obrigatoriedade da adoção de técnicas que assegurem a inviolabilidade dos dados. Por outro lado, se as eventuais técnicas A, B ou C serão ou não obrigatórias, não parece haver um avanço normativo, apenas a exemplificação de que a encriptação pode ser uma delas. Eis o teor:

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

[139] LGPD, Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

Souza (2020) também apresenta outro parâmetro suplementar a ser utilizado pelos agentes de tratamento em caso de lacuna de normatividade pela ANPD. Trata-se da norma da ABNT ISSO/IEC 27002[140], que institui um Código de práticas para a gestão da informação, conforme mencionada pelo autor.

Avançando sobre o conteúdo da norma técnica, chamamos especial atenção para o seu ponto 15.1.6, "d", pois nela é abordada a regulamentação de controles de criptografia, estabelecendo diretrizes para sua implementação. No caso, a alínea "d" dispõe que as diretrizes para a implementação da criptografia devem considerar o paradigma *backdoors* aplicado por outros países, isto é, o acesso autorizado de outras autoridades[141].

Existiriam outras fontes normativas para fins de reforço à segurança?

Acima, vimos fontes suplementares que poderiam ser utilizadas para balizar a diligência dos agentes de tratamento no que tange a implementação de medidas de segurança, com especial ênfase para a construção de uma possível exigibilidade da criptografia, já que não há em favor da técnica, ao menos expressamente, um efeito vinculante. Entretanto, esse atual quadro de ausência de força vinculante expressa da criptografia pode atrair outro instituto adequado à construção de sua exigibilidade: a boa-fé objetiva.

Souza (2020) adverte que a adoção das medidas de segurança e de sigilo pelos agentes de tratamento não podem ser motivadas unicamente pelo temor das eventuais sanções ou dos danos reputacionais, mas também pelo próprio dever de cuidado, desdobramento da boa-fé objetiva, inerente a toda e qualquer relação que envolva o tratamento de dados.

---

[140] BRASIL. ABNT NBR ISO/IEC 27002:2005. *Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação*. Disponível em: <https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf>. Acesso em: 10 mar. 2022.

[141] Eis o inteiro teor do ponto:15.1.6 Regulamentação de controles de criptografia: Controle – Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos e regulamentações pertinentes. Diretrizes para implementação – Convém que os seguintes itens sejam considerados para conformidade com leis, acordos e regulamentações pertinentes: a) restrições à importação e/ou exportação de hardwares ou softwares de computador para execução de funções criptográficas; b)restrições à importação e/ou exportação de hardwares ou softwares de computador que foi projetado para ter funções criptográficas embutidas; c)restrições no uso de criptografia; d) métodos mandatários ou discricionários de acesso pelas autoridades dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo. Convém que assessoria jurídica seja obtida para garantir a conformidade com as legislações e leis nacionais vigentes. Também convém que seja obtida assessoria jurídica antes de se transferirem informações cifradas ou controles de criptografia para outros países.

Essa sinalização do autor para a boa-fé objetiva como fundamento adicional – além dos textos legais e regulamentares – à construção da exigibilidade de técnicas protetivas adequadas é promissor, pois instaura a ideia de posturas diligentes tomadas de ofício no âmbito da segurança cibernética privada.

Por outro lado, uma questão complexa será quando a ANPD dispuser sobre um conteúdo mínimo protetivo, mas eventualmente insuficiente à substancial segurança dos dados. Isso introduz a pergunta a respeito dos possíveis deveres de segurança a cargo do agente de tratamento, mas para além do mínimo fixado por fontes estatais. Ser ou não ser um agente zeloso?

Parece-nos que a LGPD, ao prever a palavra "mínimo" no §1º[142] do Art. 46, sugere uma postura proativa a cargo do agente de tratamento, recordando que essa premissa dialoga diretamente com as preocupações esboçadas em relatório publicado pela UNESCO (2016), relativas à uniformização da proteção dos dados em nível global, pois considera-se a premissa de que o titular possui, em regra, uma postura resignada, ao passo que os intermediários possuem maior capacidade protetiva.

Nessa linha, por exemplo, apesar de não haver uma obrigatoriedade da adoção de medidas de encriptação, ao menos nos termos do MCI e de seu regulamento, ou de eventual lacuna no que toca a ação da ANPD, conforme exposto outrora, pensamos que a boa-fé objetiva – conforme já apontado pelo professor Carlos Affonso de Souza – possa ser uma via suplementar, apta à construção da exigibilidade dessa e de outras técnicas de cibersegurança, adicionando-se camadas protetivas ao mínimo disposto pelo órgão competente.

Obviamente, a adequabilidade dessas técnicas deverá considerar os cumulativos parâmetros traçados pela própria LGPD, quais sejam: "a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei" (§1º do Art. 46).

[142] LGPD, Art. 46, § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

Outra questão, variante da anterior, seria quando os agentes de tratamento já tiverem adotado algumas medidas de segurança, mas supervenientemente a ANPD atue fixando padrões mínimos, ou modificando a normatividade previamente existente. Nesses casos, pensamos ser possível tomarmos de empréstimo a mesma lógica que anima o sistema de competências concorrentes existente na Constituição da República[143], mas adaptando-o para uma parametrização no seguinte sentido:

i) No âmbito das medidas técnicas de segurança de dados pessoais, a ANPD possui o poder-dever de estabelecer padrões mínimos;

ii) A competência da ANPD para dispor sobre padrões mínimos não exclui a adoção de medidas técnicas protetivas suplementares pelos próprios agentes de tratamento;

iii) Inexistindo a fixação de padrões mínimos pela ANPD, os agentes de tratamento adotarão, de ofício, medidas técnicas de segurança exigíveis, por força da boa-fé objetiva, consideradas a expectativa de segurança pelo titular, a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º da LGPD;

iv) A superveniência de normatização pela ANPD suspende a eficácia das medidas protetivas, no que lhe for contrário.

No entanto, sobre o último ponto, "iv", recairia uma autocrítica, de modo que não seria prudente a suspensão imediata de medidas de segurança. Tamanha postura poderia ser paradoxal se o objetivo é a continuidade de um pleno ambiente de segurança para os dados.

Nessa ordem de ideias, seria mais adequado estabelecer um regime de transição para que os agentes de tratamento, paulatinamente, possam suspender as medidas que vêm aplicando e passem a adotar os padrões impostos pela ANPD. Assim, a disposição poderia ser remodelada para: *iv)* A superveniência de

[143] Trata-se dos parágrafos do Art. 24 da CF/88: §1º No âmbito da legislação concorrente, a competência da União limitar-se-á a estabelecer normas gerais; §2º A competência da União para legislar sobre normas gerais não exclui a competência suplementar dos Estados; §3º Inexistindo lei federal sobre normas gerais, os Estados exercerão a competência legislativa plena, para atender a suas peculiaridades; §4º A superveniência de lei federal sobre normas gerais suspende a eficácia da lei estadual, no que lhe for contrário.

normatização pela ANPD será regulamentada setorialmente através de regimes de transições que objetivem a modificação dos padrões, observada a continuidade da proteção integral dos dados.

As considerações acima são extremamente criticáveis, uma vez que o presente estudo, focado no problema da relação entre criptografia e *backdoors*, não teve como preocupação central explorar as complexidades da articulação entre boa-fé objetiva e o sistema de segurança da LGPD, especificamente no que toca as inúmeras possibilidades de conflito técnico entre eventuais disposições normativas a serem expedidas pela ANPD e as modelagens de cibersegurança internas dos agentes de tratamento. Trata-se, apenas, de uma tentativa de contribuição, em nada fruto de uma cognição exauriente sobre o ponto.

Avancemos quanto ao ponto das medidas técnicas preventivas.

Souza (2020) chama atenção, por fim, para um importantíssimo ponto quanto à adoção de medidas preventivas de segurança dos dados pessoais e referentes à privacidade desde a concepção do produto. Trata-se da filosofia do *privacy by design* desenvolvida por Ann Cavoukian (2011)[144], recepcionada, segundo o autor, pelo §2º do Art. 46 da LGPD ao dispor expressamente que as medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Há que se acrescentar que os conceitos de *privacy by design* e, por sua vez, de *security by design* representam paradigmas convergentes, contemplando uma ampla interface reconhecida e explorada pela própria Cavoukian e por Mark Dixon desde 2013[145]. Quanto ao *security by design*, consta a premissa de que um produto ou serviço também deve sofrer testes para verificar a existência de vulnerabilidades de segurança desde a sua concepção, possuindo, portanto, perfeita sintonia com o mesmo dispositivo da LGPD (§2º do Art. 46), além de dialogar com as capacidades de ataque da criptoanálise, tal como apontado nos tópicos 2.1.1 e 3.4.

[144] Para maiores detalhes: (CAVOUKIAN, Ann – The 7 Foundational Principles. Privacy by Design. Ontario, Canada - Information and Privacy Commissioner of Ontario, 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso: 1 jun. 2022.

[145] Para maiores detalhes: (CAVOUKIAN, Ann and DIXON, Mark – Privacy and Security by Design: An Enterprise Architecture Approach. Information and Privacy Commissioner Ontario, Canada, 2013. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf>. Acesso em: 1 jun. 2022.

Em linhas sintéticas, esse seria o arcabouço jurídico preventivo, de ordem técnica, focado na criptografia, contra possíveis vulnerabilidades na segurança. Avancemos ainda sobre a proteção pelos intermediários e a sua relação com a criptografia, mas quando situada em fase subsequente, intermediária entre as medidas preventivas e o dano. Trata-se da fase em que se constata a existência de um incidente de segurança passível de desencadear riscos ou danos relevantes.

Passemos ao ponto envolvendo os incidentes de segurança.

4.3. Segurança e Proteção Intermediária: O Incidente de Segurança

Como é possível uma articulação entre vulnerabilidades/*backdoors*, incidente de segurança, o dever de comunicar a ANPD sobre o incidente e a criptografia, tudo à luz da LGPD?

Para respondermos a esta pergunta, antes, devemos conhecer o que é um incidente de segurança e como funciona o dever de o agente de tratamento notificar a ANPD a respeito do incidente. Depois, verificaremos como a criptografia pode afetar essa dinâmica entre o incidente e o dever de notificar.

Com base no Art. 46 da LGPD, Carlos Affonso de Souza define o incidente como:

> a violação das medidas adotadas pelos agentes de tratamento para salvaguardar a integridade e o sigilo dos dados pessoais sob sua administração, resultando em acessos não autorizados e em situações acidentais ou ilícitas de destruição perda alteração comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Souza, 2020, p. 426)

Por sua vez, o *caput* do Art. 48[146] prevê que o controlador deverá comunicar à autoridade nacional[147] e ao titular[148] a ocorrência de incidente de segurança que, frise-se, possa acarretar risco ou dano relevante aos titulares.

Nota-se, pela leitura do caput do Art. 48, que a existência de um incidente de segurança, por si só, não implica, necessariamente, no dever de informar a

[146] LGPD, Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
[147] LGPD, Art. 5º, XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
[148] LGPD, Art. 5º, V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

ANPD. É que um incidente de segurança não tem por efeito necessário o risco ou dano relevante aos titulares, segundo a Lei e sua literalidade, pensamos.

A expressão "que possa acarretar risco ou dano relevante aos titulares" contida na parte final do caput do Art. 48 reflete a abertura para um juízo de possibilidade. Ao que parece, o legislador subordina a notificação a uma avaliação qualitativa da relevância do incidente pelo controlador. É indagar: essa falha na segurança acarretou riscos aos titulares? Ou produziu danos aos titulares? Mas esses riscos e/ou danos foram relevantes? Ou seja, uma coisa é ter ocorrido o incidente, outra é informar sobre ele.

Souza cita, como exemplo, a possibilidade de que haja apenas uma perda temporária de dados, a qual o controlador exitosamente teria recuperado o controle. Nesse sentido, ele afirma que a avaliação do dever de comunicar caberá ao controlador que, por sua vez, deve se guiar pelas razões da indisponibilidade dos dados, pelas possíveis consequências daquele incidente e pelos riscos aos titulares dos dados.

Ponderamos, em acréscimo, que a Lei sinaliza para a atribuição do juízo de relevância do incidente em prol do controlador quase como uma possível avaliação potestativa por parte desse ator, o que poderá produzir opacidades, uma problemática que poderá será melhor enfrentada em futuros estudos.

É que, por outro lado, há de se levar em conta que controlar o espectro cognoscível da segurança sobre uma informação pessoal – um dado pessoal – no caso, "o quem pode saber sobre o que", além de subverter o conceito de Stefano Rodotà[149] (2008) sobre controle das informações pessoais em desfavor do titular e em favor do terceiro intermediário, aquele que usa o conhecimento sobre a pessoa humana como insumo de suas práticas, também pode ter outras finalidades não muito esclarecidas na esfera pública. Como por exemplo: evitar danos reputacionais, garantir uma ação coordenada com os órgãos de espionagem, evitar que o conhecimento do incidente na esfera pública comprometa um acordo informal

[149] Segundo Stefano Rodotà: "*Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. Assim a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações*." (RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje.* Org. Maria Celina Bodin Moraes, Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 92)

existente entre um agente de tratamento e um outro país que tenha o acesso autorizado, entre outras potencialidades que orbitam a relação dos intermediários com outros atores.

No que essa possível captura do juízo da relevância pelos intermediários poderia contribuir para uma história transparente da privacidade?

Recorde-se, ademais, do caso *The Shadow Brokers – Wannacry* descrito no tópico 3.4, pertinente ao que se discute nesse momento.

Passadas as apresentações sobre a definição de incidente de segurança e a notificação da ANPD, indagamos sobre a relação desses institutos com os *backdoors*.

Conforme já exposto, os *backdoors* representam vulnerabilidades da segurança de uma infraestrutura comunicacional apta a ser explorada, ora por terceiros autorizados ao acesso excepcional, no caso aqui estudado, o Estado, ora por terceiros não autorizados.

Nesse sentido, o incidente de segurança e a notificação devem levar em consideração o critério da autorização do acesso, pois os institutos devem ser interpretados sistematicamente com o Art. 46, *caput*, o qual prevê que os agentes de tratamento devem adotar medidas de segurança contra o acesso não autorizado e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Assim, um *backdoor* em que se franqueia o acesso ao Estado é um *backdoor* autorizado, de modo que não poderia ser enquadrado como incidente de segurança a exploração dessa falha pelo órgão público autorizado a tanto, ao menos para os fins da LGPD.

Questão árdua, e que demandaria um exame mais aprofundado, seria verificar se a existência de um *backdoor* autorizado e explorado por um órgão público implicaria no dever de comunicar a ANPD. Essa é a situação pontual sobre vulnerabilidade intencional, para o Estado, mas relevante para este capítulo, hipótese em que advertimos, no bojo do tópico 4.1, sobre a possibilidade de exploração abusiva da vulnerabilidade por um órgão público autorizado.

E assim retomamos: a existência de um *backdoor* autorizado/intencional e explorado por um órgão público implicaria no dever de comunicar a ANPD? Aparentemente, uma primeira impressão poderia ser no sentido de negar a comunicação. Isso porque, além de estarmos diante de um acesso autorizado por força de interpretação do caput do Art. 46, a notificação da ANPD também poderia comprometer a efetividade da exploração pelo órgão público autorizado, na medida em que ampliaria o espectro cognoscível de uma prática necessariamente sigilosa para além dos envolvidos, isto é, para outra instituição: a ANPD.

No entanto, também não é de todo improvável que, apesar de ser franqueável a um órgão público, o acesso a uma determinada infraestrutura seja exercido de modo abusivo ou em desvio de finalidade, para além dos limites constitucionais, o que poderia implicar, eventualmente e concretamente, em situações ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais, conforme previsto na parte final do caput do Art. 46.

E aqui restaura-se a dúvida sobre caber ao intermediário/controlador comunicar ou não comunicar a ANPD, inaugurando uma possível tensão entre diferentes instituições públicas e intermediários franqueadores de infraestrutura com vulnerabilidades exploradas. Um ponto merecedor de exames futuros e mais demorados.

Em relação a interface dos institutos do incidente e do dever de comunicação à ANPD com a criptografia, trazemos a observação do professor Carlos Affonso de Souza no sentido de que “em um cenário de maior segurança digital, no qual as informações estão criptografadas, por exemplo, a perda da chave criptográfica também se enquadra na hipótese de perda de dados” (Souza, 2020, p. 247).

É pertinente, do ponto de vista de uma proteção forte da privacidade e dos dados pessoais, associar a perda das chaves da inteligibilidade de um objeto à perda de um dado pessoal, condição que pode atrair o enquadramento do fato como um incidente de segurança e, observados os termos do Art. 48 da LGPD, também o dever de comunicar a ANPD.

Passadas essas considerações sobre a interface entre institutos que orbitam o tema da cibersegurança, retomamos a pergunta: como é possível uma articulação

entre vulnerabilidades/*backdoors*, incidente de segurança, o dever de comunicar a ANPD e a criptografia, todos à luz da LGPD?

Essa articulação é possível de ser extraída do trabalho de Danilo Doneda e Diego Machado (2019), em que os autores analisam uma interface entre criptografia e anonimato e seus reflexos sobre os limites hermenêuticos da LGPD.

Os autores indagam se a cifragem de dados pessoais – a encriptação de dados pessoais – pode ser enquadrada como técnica de anonimização para fins de afastar a proteção assegurada pela LGPD. Eis o teor:

> Assim, suscita-se a seguinte questão: se a criptografia é apta a tornar informações ininteligíveis, pode a cifragem de dados ser reputada como técnica de anonimização quando o dado tiver caráter pessoal, isentando, por conseguinte, responsáveis pelo tratamento de dados cifrados da observância do regime jurídico da proteção de dados pessoais? Em outras palavras, considerando que a definição de dado pessoal dada pela Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), em seu art. 5º, I, abrange a "informação relacionada a pessoa natural identificada ou identificável", em qual medida os dados pessoais submetidos a procedimento de encriptação serão considerados como tais? (Doneda e Machado, 2019, p. 138).

A resposta a essa indagação produzirá ressonâncias, segundo os autores, no tema da segurança dos dados, notadamente no instituto do incidente de segurança e do correlato dever de comunicação à ANPD, conforme será exposto adiante.

Mas antes, por que poderíamos cogitar que encriptar um dado pessoal implicaria no afastamento do conceito de dado pessoal? Pois quando a criptografia torna um dado pessoal ininteligível, poder-se-ia cogitar, apressadamente, que essa ininteligibilidade teria como corolário a desidentificação do dado, rompendo-se o vínculo associativo entre informação e uma pessoa humana, o que faria com que o dado deixasse de apresentar a qualidade de dado pessoal para, por força da cifragem, apresentar uma nova qualidade: a de *dado anonimizado*[150], uma informação em que não é possível visualizar a identificação de um humano.

Os autores explicam que a operação de cifragem, isto é, de encriptação de um dado pessoal, por si só, não tem por efeito necessário tornar esse dado anônimo ou anonimizado. Isso porque mediante técnicas suplementares é possível a (re)identificação do titular, apontam os autores.

[150] LGPD, Art. 5º, III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

Nesse sentido, sem fazer justiça ao amplo estudo dos autores, isto é, adotando uma perspectiva bastante sintética do estudo, o dado encriptado gozaria de uma terceira qualidade: a de *dado pseudonimizado*, aplicando-se, a partir de então, um regime modulado, afirmam.

E, dentro desse regime modulado, ancorados no GDPR[151], os autores afirmam que poderá ser dispensado o dever de comunicar o incidente de segurança que resulte em altos riscos a direitos dos titulares de dados, se o controlador adotou apropriadas técnicas de segurança, tal como a criptografia.

Focando sempre na análise do caso concreto, eis a conclusão dos autores:

> No caso concreto, deve-se analisar se os dados criptografados, a partir da execução do protocolo criptográfico desenhado, não mais se vinculam a pessoa natural identificada ou identificável, por meios suscetíveis de ser razoavelmente utilizados, de forma permanente e irreversível. Ainda que cifrados, prima facie os dados são de caráter pessoal, pseudonimizados, porém; aplicável, então, o estatuto de proteção de dados pessoais, mesmo que de forma modulada (Machado e Doneda, 2020, p. 160).

Sob essa ordem de ideias, portanto, caso um eventual *backdoor* engendre um incidente de segurança envolvendo dados pessoais, mas que estavam eficientemente encriptados de tal forma que não possam ser (re)identificados por meios razoáveis disponíveis à época, então o controlador não teria a obrigação de comunicar a ANPD e os titulares. Essa seria uma possível articulação entre os institutos.

Pensamos ser pertinente a reflexão sobre o papel da criptografia e das ferramentas técnicas de decriptação e possível re-identificação de um dado a uma pessoa, segundo meios técnicos razoavelmente disponíveis em uma certa época, à luz da experiência histórica de um interessante caso. O caso VENONA.

Em 1943, a Inteligência militar estadunidense, antes mesmo da criação da própria NSA, inaugurou um programa secreto de codinome VENONA, cujo objetivo era desencriptar as mensagens diplomáticas soviéticas.[152]

---

[151] General Data Protection Regulation (GDPR) é o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia. Para análise do texto: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em 16 out. 2021.

[152] Para mais detalhes: <https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/smdsort14707/title/>. Acesso em 05 jun. 2022.

O programa durou anos, de tal modo que informações encriptadas e ininteligíveis à época de sua coleta, isto é, durante a Segunda Guerra Mundial, foram armazenadas em um banco de ininteligíveis para, assim, serem submetidas a um árduo processo histórico de decriptação.

Anos mais tarde, através das novas ferramentas da inteligibilidade, através das supervenientes chaves do acesso ao conteúdo, aquelas informações, antes ininteligíveis e não identificáveis de uma pessoa humana, posteriormente, quando se tornaram inteligíveis, revelaram uma lista de espiões da KGB espraiados por diferentes países, inclusive agentes britânicos, tendo sido "neutralizados"[153]. Entretanto, somente em 1995[154], com a abertura desses arquivos sigilosos à esfera pública é que a maior parte do mundo pôde tomar conhecimento do caso.

Por vezes, o vazamento de informações submetidas à forte encriptação e, à luz da época, qualificadas como ininteligíveis, podem compor um banco de dados muito segmentado e utilitário, sob a gestão reservada àqueles que investem nas supervenientes ferramentas da inteligibilidade, da compreensão. Insumos incompreensíveis, mas acautelados na antessala do inteligível. Na antessala dos seletos sujeitos do conhecimento futuro.

Num mundo composto, de um lado pela ascensão massiva de dados e de comunicações mediadas por infraestruturas cibernéticas, mas, de outro, pela decadência do registro físico e da oralidade, modos de transmissões do conhecimento em sobrevida[155], informar ou não informar, aqui e agora, talvez possa, lá na frente, contribuir para a democratização do acesso a um possível direito à verdade, ou até mesmo para a definição dos legitimados à confrontação dos fatos históricos. Os ininteligíveis de hoje podem ser os insumos à espera dos futuros narradores da História, aqueles que tiverem a guarda das chaves da decifração.

---

[153] Para uma análise resumida sobre o caso: <https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/venona_story.pdf>. Acesso em 05 jun. 2022. Por sua vez, para uma análise completa sobre o programa de espionagem: <https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/smdsort14707/title/>. Acesso em 05 jun. 2022.

[154] Para acessar a documentação antes sigilosa, mas hoje disponibilizada pela própria NSA, ver: <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/venona/declass_materials/doc-14.pdf>. Acesso em: 05 jun. 2022.

[155] Para uma análise da trajetória da memória privada até o legado digital, por exemplo: (BRANCO, Sérgio – *Memória e esquecimento na internet*. Porto Alegre: Arquipélago Editorial, 2017. pp. 17-71).

4.4. A (Des)Confiança em Relação aos Intermediários e Proteção pela Transparência

Procuramos abordar nos últimos tópicos a questão da segurança das informações pessoais através da relevante ação dos intermediários: agentes de tratamento, provedores de conexão e de aplicações. Primeiramente através das medidas técnicas preventivas que podem ser empregadas por esses atores, tal como a criptografia e, depois, apresentando uma segunda fase protetiva, focada na ação que caberia ao controlador quando constatado um incidente de segurança.

O foco nesses agentes é necessário, pois as suas práticas de segurança, sobretudo os padrões criptográficos internamente adotados, modelam o grau de proteção do usuário/titular. Por outro lado, também sabemos que a massiva passagem e armazenamento de dados na infraestrutura desses intermediários é convidativa à ação das comunidades de Inteligência e de atores não estatais sofisticados no que toca ao uso de meios sub-reptícios de acesso aos dados.

Ademais, podemos consultar a História recente e constatar que boa parte dos principais intermediários que operam as TICs possuíram – e não se sabe se ainda possuem – algum acordo informal com as comunidades de Inteligência de seus países, no intuito de facilitar o acesso aos dados. Todavia, ainda assim, a publicidade comercial é no sentido de que seus produtos e serviços gozam de alto grau de segurança.

Considerando que esses acordos informais introduziram uma camada de opacidade colaborativa com esses intermediários, não seria ingênuo apostar na segurança dessa interface? Como enfrentar o ceticismo que decorre dessas considerações?

Ultimamente, aponta-se para a transparência como um possível caminho. Nessa linha, colhe-se do relatório publicado pela UNESCO as recomendações pelo *software* aberto e sujeito ao escrutínio público, além de auditorias técnicas aptas à verificação do grau de segurança praticado pela empresa fornecedora do serviço. Estas abordagens redirecionam o foco diretamente para a indústria, revelando um profundo diálogo com as concepções de *privacy by design* e *security by design.*

Em relatório publicado pela UNESCO (2016), explica-se que o escrutínio público permitiria uma maior detecção de vulnerabilidades, o que produziria maior consciência para investir em auditorias de códigos amplamente usados, provenientes da comunidade de *software* livre e de código aberto. A transparência na realização de testes de segurança dos bens e serviços fortaleceria a qualidade protetiva do objeto.

Sobre a questão do escrutínio público de vulnerabilidades, por exemplo, é digno recordar que no próprio ano de 2013, logo após o escândalo do caso Snowden, o então ministro Paulo Bernardo, ministro das comunicações de Dilma Rousseff, advertiu sobre a necessidade de a ANATEL ampliar as exigências de equipamentos produzidos no Brasil, como forma de driblar a espionagem internacional, admitindo que os equipamentos presentes nas redes brasileiras poderiam conter uma funcionalidade de *backdoor* em cumprimento à legislação americana denominada *Communications Assistance for Law Enforcement Act* (CALEA), de 2004.[156]

Por outro lado, somente no ano de 2020 e, com base no Regulamento de Segurança Cibernética aplicado ao Setor de Telecomunicações (Resolução 740/2020), é que a ANATEL expediu ordens para o recolhimento de produtos no intuito de verificar, mediante amostragem, a existência de *backdoors*.[157]

Esse foi um exemplo direcionado aos *backdoors* no setor de telecomunicações. Mas a questão torna-se mais difícil quando redirecionada aos intermediários que tratam dados pessoais e estão sujeitos à LGPD ou quando direcionada aos grandes provedores de conexão e de aplicações que estão espraiados por toda a internet, sobretudo se recordarmos que paira sobre muitos desses atores uma opacidade quanto a possíveis acordos informais com seus governos sedes.

A verificação de vulnerabilidades em seus bens e serviços, sobretudo a exploração por atores sofisticados e parceiros de parte desses atores privados, poderia ser enfrentada, por exemplo, a partir de auditorias fiscalizatórias,

[156] POSSETI. Helton. Denúncias podem fazer Brasil ampliar exigências de produtos. Exame.com. Disponível em: <https://exame.com/tecnologia/denuncias-podem-fazer-brasil-ampliar-exigencias-de-produtos/>. Acesso em: 13 dez. 2020

[157] AQUINO, Mirian. Anatel Começa A Verificar Se Tem Backdoor Em Produtos De Telecom No Brasil No Segundo Semestre. Disponível em: <https://www.telesintese.com.br/anatel-comeca-a-verificar-se-tem-backdoor-em-produtos-de-telecom-no-brasil-no-segundo-semestre/>. Acesso em: 07 jul. 2021.

concretizando o princípio da transparência[158]. Mas esse é um tema que pode atrair fortes oposições.

No MCI, por exemplo, não consta, ao menos expressamente, qualquer previsão de auditoria nas pessoas jurídicas provedoras de conexão e de aplicações. Por sua vez, a LGPD prevê o termo "auditoria", mas apenas em dois dispositivos, o §2º do Art. 20[159] e o inciso XVI do Art. 55-J, este último exposto adiante.

Na primeira hipótese, §2º do Art. 20, a auditoria é uma possível ação a ser adotada pela ANPD em casos de decisões automatizadas discriminatórias. Trata-se de uma auditoria específica e associada ao campo da automatização de decisões odiosas, prevendo, já no próprio marco legal, a possível tensão dessa análise com o segredo comercial e industrial do agente de tratamento. Eventual análise sobre as decisões automatizadas e a sua relação com as possíveis auditorias qualificadas escaparia ao escopo desse trabalho[160].

Por outro lado, há também a previsão de auditorias fiscalizatórias através do inciso XVI do Art. 55-J, uma das mais relevantes competências da ANPD. O referido inciso deve ser interpretado sistematicamente com os incisos II e IV. Eis a transcrição de todos eles:

> Art. 55-J. Compete à ANPD:
> II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

[158] A LGPD prevê a transparência como um de seus princípios: Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

[159] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. § 3º (VETADO).

[160] Para um estudo sobre as opacidades ao redor das decisões automatizadas e a necessidade de fortalecimento da transparência quanto ao ponto: (FRAZÃO, Ana. *Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados, in:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato – (coord.) *Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro*. 2ª ed. - São Paulo: Thomson Reuters Brasil, 2020. pp. 23-52).

> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

Percebe-se pela leitura dos três incisos que a possibilidade da auditoria entra em possível fricção com os segredos comercial e industrial. É digno, para tanto, pontuarmos o histórico dessas previsões.

Na redação originária da LGPD, as atribuições da ANPD eram dispostas em seu Art. 56, de modo que o seu originário inciso XVI contemplava a hipótese de auditoria, mas nos seguintes termos:

> Art. 56. A ANPD terá as seguintes atribuições:
> XVI - realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o Poder Público.

Nota-se que a modelagem originária das auditorias sobre os agentes de tratamento pela ANPD não sofria tantas limitações materiais e procedimentais. Tratava-se de puro exercício fiscalizatório – obviamente respeitado o devido processo legal – atividade típica de órgão ou entidade Estatal. Tanto era assim, que a previsão originária das atribuições da ANPD, notadamente a do inciso II do Art. 56, reforçava tamanha prerrogativa ao dispor sobre a possibilidade de ponderação entre valores:

> Art. 56. A ANPD terá as seguintes atribuições:
> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
> II - zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

É possível perceber que além da disposição originária do inciso XVI não conter, em seu próprio texto, a referência aos segredos, a redação originária do inciso II, por sua vez, previa a expressão "em ponderação", inaugurando, a cargo da ANPD, um possível juízo de proporcionalidade envolvendo os segredos, o zelo pelos dados pessoais e os próprios fundamentos da Lei.

Não custa acrescentar que o primeiro fundamento da Lei é o respeito à privacidade (Art. 2º, I[161]). E, considerando tratar-se de uma Lei que se enuncia formalmente como protetiva de dados pessoais, e que esse conceito, por sua vez, versa sobre informação capaz de identificar um ser humano[162], não seria redundante sempre recordar que a privacidade é funcionalizada à pessoa humana, ainda que outros interesses, em nada humanos, possam pegar carona na sua elasticidade conceitual.

Retomando. O grande problema é que aqueles dispositivos foram vetados, assim como todo o Art. 56, que previa as atribuições da ANPD. O veto foi em razão da inconstitucionalidade formal dos dispositivos por vício de iniciativa, acertadamente, pois na medida em que dispunham sobre entidade integrante da Administração Pública a iniciativa deve ser reservada ao Chefe do Executivo[163].

Por outro lado, os aspetos formais poderiam ter sido corrigidos por nova Lei, dessa vez deflagrada pelo Executivo, mas mantidos o conteúdo material dos dispositivos. Mas isso não ocorreu.

Em seguida, em 27 de dezembro de 2018 foi editada a Medida Provisória 869, contemplando novas atribuições para a ANPD, dessa vez no Art. 55-J. Nessa etapa regulatória, não apenas as auditorias fiscalizatórias foram suprimidas, não constando em quaisquer dos incisos do Art. 55-J, como, por outro lado, também foi inserido um novo parágrafo após as competências da ANPD prevendo o fortalecimento do zelo pelos segredos sob pena, frise-se, de uma possível responsabilização institucional:

> MP 869/2018, Art. 55-J, § 4º No exercício das competências de que trata o caput, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade.

Prosseguindo com o processo histórico-formal da LGPD e a questão das auditorias em tensão com os segredos. Passada a redação original, o seu respectivo veto e, posteriormente, as disposições da Medida Provisória 869/2018, uma terceira

[161] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade;

[162] Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

[163] Para maiores detalhes sobre o veto presidencial: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em 15 mar. 2022.

etapa regulatória sobre os poderes da ANPD foi disposta através da Lei n.º 13.853 de 08 de julho de 2019, produto da conversão da referida Medida, e que hoje contempla a redação vigente da LGPD.

Nessa ocasião, conversão da Medida em Lei, foram retomadas as disposições sobre as auditorias fiscalizatórias, mas sob novos termos, e, por outro lado, foram mantidas as disposições sobre o zelo pelos segredos, mas com pequenas alterações, dentre as quais a retirada da responsabilização institucional da ANPD introduzida pela medida provisória. Eis um quadro comparativo:

Redação originária da LGPD e vetada por inconstitucionalidade formal	**Redação dada pela MP 869 de 27 de dezembro de 2018 - Suprimida a previsão sobre auditorias fiscalizatórias e acrescentado o seguinte parágrafo às atribuições da ANPD:**	**Redação dada pela Lei n.º 13.853 de 8 de julho de 2019 – Conversão da MP 869 – atual redação vigente da LGPD**
Art. 56. A ANPD terá as seguintes atribuições: II - zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; XVI - realizar ou determinar a realização de auditorias, no	Art. 55-J. Compete à ANPD: (...)	Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019) II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019) XVI - realizar auditorias, ou determinar sua

âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o Poder Público.	§ 4º No exercício das competências de que trata o caput , a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade.	realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019) § 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

Verifica-se, portanto, que a redação final, hoje atual, retomou a possibilidade das auditorias, no entanto, não empregou, ao menos expressamente, a possibilidade de ponderação entre a proteção dos dados e os segredos, conforme era previsto na redação original. Ademais, reforçou o zelo institucional pelos segredos.

Essas pequenas sutilezas históricas revelam, a nosso ver, indícios da luta pelo direito, se nos é permitida tomar de empréstimo a famosa expressão de Rudolf von Ihering[164]. Vontades políticas muito bem organizadas que orientam, através de suas criptas, o produto final: um texto ao qual os futuros intérpretes limitar-se-ão.

[164] IHERING, Rudolf von – *A luta pelo Direito.* Tradução Edson Bini. 2ª ed., Edipro, 2019.

Daí a importância da historicidade e de que o debate não se restrinja aos supostos valores colidentes segundo a narrativa do momento, mas também inclua a dinâmica do xadrez entre os atores que condicionam e recondicionam esses valores.

A supressão das auditorias e a ascensão dos segredos dentro da evolução formal da regulação é historicamente simbólica. Ela ilumina indícios a serem colhidos pelo ceticismo moderado, essencial ao estudo jurídico. No caso da proteção de dados e da privacidade, são indícios que podem permitir uma nova ótica sobre textos que se enunciam formalmente como cartilha de direitos voltados à pessoa humana, mas que em sua materialidade se inclinam muito mais à estabilização das relações patrimoniais. Afinal, não é interessante que um concorrente trate dados à sombra a Lei.

Nesse estudo, vimos, de um lado, a propagada ideia de segurança cibernética e reverência à privacidade dos titulares pelo setor privado, sobretudo após o marco histórico Snowden. Por outro lado, esse mesmo marco introduziu uma saudável (des)confiança na consciência social a respeito de quem possui a gestão e, portanto, o controle de nossas informações pessoais, sobretudo porque as colaborações opacas não foram devidamente desvendadas.

Some-se a esse quadro a pouco explorada consciência de que existem meios sub-reptícios de acessar os dados à sombra da criptografia. E que esses meios estão, sobretudo, sob a expertise técnica de pouquíssimos atores, muito deles com um braço em outros Estados.

Por sua vez, as medidas que poderiam avançar sobre essas opacidades ou não estão previstas nas Leis supostamente protetivas, ou quando estão, sofrem sérias dificuldades de efetivação. Contra elas se apõe uma nova camada de opacidade: os segredos.

Se, de um lado, a coleta de dados do humano por empresas que tomam essa informação como insumo à prestação de seus serviços é facilitada através de contratos de adesão cuja escolha do titular é consentir ou ficar obsoleto, de outro, o conhecimento das "informações pessoais" desse segmento empresarial é desestimulado/dificultado através de categorias jurídicas que operam sob a função-matriz da propriedade: o poder de exclusão. Por exemplo, através dos segredos e da propriedade intelectual.

Essa assimetria epistemológica é denunciada por Frank Pasquale (2015), para quem estaríamos diante de cidadãos transparentes vs. um aparato corporativo-governamental opaco. Pasquale acrescenta que há uma maior facilidade em se inspecionar o próprio aparato público de Inteligência do que o segmento empresarial que com ele dialoga opacamente.

Essa família de ideias sobre facilitações, para uns, e complexificações, para outros, nos desperta, também, os ensinamentos de Norberto Bobbio (2006) sobre a própria função promocional do Direito[165]. No caso, estruturas jurídicas que, de um lado, facilitam o conhecimento de atributos humanos e, de outro, estruturas, também jurídicas, mas que dificultam o conhecimento corporativo patrimonial, ainda que esse segmento se alimente daquele.

Shoshana Zuboff (2015) recorda que a interface entre titulares de dados, pessoas humanas, e os intermediários é regida pela lógica da extração, consistindo em um processo unidirecional, e não num relacionamento. Para a autora, essa dinâmica espelha uma ausência de reciprocidades estruturais entre a empresa suas populações de usuários.

Nesse sentido, a ausência de uma estrutura normativa densificada e direcionada à ação Estatal voltada para a inspeção das infraestruturas dos intermediários engendra um maior grau de liberdade desses atores. Ao comentar essas liberdades concedidas para alguns, Zuboff[166] afirma que arranjo estrutural além de proteger o segmento corporativo das consequências da desconfiança, também introduz assimetrias substanciais de conhecimento e poder.

Acrescentamos: quando o horizonte aponta para uma possível colisão entre, de um lado, a proteção da pessoa humana através da transparência e, de outro, a preservação da opacidade corporativa, rapidamente os bastidores se movem para atualizar o quadro normativo de modo a amoldar as formas jurídicas ao zelo pelas categorias fortes e tradicionais do Direito, como o contrato (no caso, de adesão) e a propriedade (dessa vez, a intelectual, em sua forte tutela via segredo).

[165] Nesse sentido, ver: BOBBIO, Norberto – *Da estrutura à função: novos estudos da teoria do direito*. Tradução Daniela Versiani. Barueri, SP: Manoele, 2007. pp. 01-21.
[166] No caso, a autora toma como exemplo concreto a falta de amarras jurídicas sobre o Google.

É sintomático desse quadro, ademais, a própria incipiência[167] da pesquisa jurídica quanto ao ponto da eventual superação dos segredos, sobretudo quando a recente experiência histórica nos adverte sobre a legítima desconfiança e a necessária busca por ferramentas de transparência[168] mais efetivas, tais como a inspeção direta através de auditorias.

Digno pontuar as lições de Stefano Rodotà (2008), segundo as quais o fortalecimento da privacidade pressupõe maior transparência e controle das esferas de outros sujeitos, não sendo por acaso que o desenvolvimento de uma tutela dos dados também pressuponha uma evolução recíproca de disposições normativas que prestigiem o acesso às informações de *como* operam aqueles sujeitos. Não apenas o "para que" se tratam dados, mas o "como" se tratam. Esse "como" é legítimo? Se não for, seria um enriquecimento sem causa? Muitas perguntas poderiam ser colocadas.

Seria necessário, portanto, avançar na tutela da privacidade e da proteção de dados através de novos estudos que mirem as opacidades que orbitam os intermediários dos dados.

Passemos, por fim, a um interessante caso em que se consolidam diversos aspectos tratados ao longo desse estudo.

4.5. Um Caso para Reflexão – Convergência dos Institutos Discutidos

Susan Landau (2017) recorda que, até não muito tempo atrás, havia a assunção de que um terceiro mal intencionado e explorador de uma vulnerabilidade, por exemplo, um hacker, poderia esconder sua origem se direcionasse o seu ataque por meio dos dispositivos e sistemas de terceiros, escondendo a sua rota, seus

[167] Para uma interessante metáfora sobre o que interessa e o que não interessa ser dito, ver as camadas piramidais de obscurecimento e censura apresentadas por Julian Assange: (ASSANGE, Julian et al. *Cypherpunks: liberdade e o futuro da internet*. Tradução Cristina Yamagami, São Paulo: Boitempo, 2013. p. 128). Na mesma linha, sobre o controle do ingresso de importantes informações na esfera pública, ver também a sua conversa com Hans-Ulrich Obrich em: (ARANDA, Julieta; WOOD, Brian Kuan; VIDOKLE, Anton – *The Internet Does Not Exist*. E-journal: Sternberg Press, 2015. pp. 208-244).

[168] Para um mapeamento da transparência já em Louis Brandeis, em 1913, até sua recepção institucional e conversão em Lei em 1966 através do Freedom of Information Act (FOIA), passando, antes, pelas fracassadas tentativas transnacionais de transparência na Liga das Nações em 1918, ver: (METAHAVEN. *Black Transparency*: The Right to Know in the Age of Mass Surveillance, Editora: Sternberg Press, 2014, pp.60-62). Por sua vez, o ato normativo FOIA pode ser acessado em: <https://www.foia.gov/foia-statute.html>. Acesso em: 18 dez. 2020.

rastros, dispersando sua trajetória por infraestruturas alheias. Mas esse método decaiu, diz Landau.

Segundo a autora, em 2013, a empresa de cibersegurança *Mandiant*[169] expôs hackers chineses, sob a acusação de que pertenceriam ao exército chinês e que teriam atacado indústrias estadunidenses e do Ocidente.

No caso, Landau afirma que o governo dos EUA estava disposto a indiciar, formalmente, cinco hackers chineses, no entanto, tendo individualizado os supostos agressores através do auxílio corporativo, o governo estadunidense sequer tentou removê-los da China. Segundo a autora, essa inércia é avalizada pelo ponto de vista da comunidade de Inteligência. Mas por quê?

Porque, segundo Landau, do ponto de vista da Inteligência, não promover um julgamento desses atores afasta a necessidade de demonstrar os métodos pelos quais esses acusados foram identificados.

Por outro lado, reputamos surpreendente essa constatação. Isso porque o caso EUA-*Mandiant*-China[170] pode ser paradigmático sobre o que orbita não só os *backdoors*, vulnerabilidades infraestruturais passíveis de exploração, mas também toda a discussão sobre os arredores sombrios dos arranjos de cibersegurança.

Aqui estão em jogo diversos elementos: *i)* a colaboração entre empresas e governos na arena cibernética; *ii)* saberes opacos; *iii)* como as vulnerabilidades/*backdoors* foram exploradas? *iv)* os meios de rastreamento cibernético do ataque; *v)* os meios de identificação de uma pessoa humana supostamente atacante; *vi)* a possibilidade de extradição dessa pessoa humana; *vii)*

[169] Quase dez anos após esse caso, a mesma gigante da cibersegurança, *Mandiant*, é comprada pelo Google por 5,4 bilhões de dólares, no que seria a segunda maior aquisição de sua história, no intuito de lançar a Big Tech no mercado sobre armazenamento em nuvem e, assim, rivalizar com as empresas dominantes na área: Amazon e Microsoft.: <https://www.nytimes.com/2022/03/08/business/google-mandiant-cybersecurity.html>. Acesso em 20 abr. 2022. A aquisição é anunciada em 8 de março de 2022, logo após a recém deflagrada guerra entre Rússia e Ucrânia. Em 24 de março, no entanto, a *Mandiant* anuncia em seu próprio site a criação de uma força tarefa global para rastrear ameaças cibernéticas aos seus clientes decorrentes da invasão russa: <https://www.mandiant.com/resources/insights/ukraine-crisis-resource-center>. Acesso em 20 abr. 2022. Digno mencionar, ademais, que o fundador da *Mandiant*, Kevin Mandia, é egresso das forças armadas estadunidenses, tendo servido, inclusive, dentro do Pentágono. O tradicional clientelismo entre militarismo, Inteligência e setor privado: <https://www.mandiant.com/company/leadership/kevin-mandia>. Acesso em: 20 abr. 2022.

[170] Para maiores detalhes: <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>. Acesso em: 15 jun. 2022. Ou através das próprias informações disponibilizadas pela própria empresa *Mandiant*: <https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units>. Acesso em 15 jun. 2022.

a cláusula do devido processo legal – julgamento justo com ampla defesa e contraditório; mas, sobretudo; *viii)* os meios de obtenção da prova e de formação de uma verdade jurídica. Lícitos ou ilícitos? As formas de se produzir a verdade, uma verdade, mas possivelmente não mais iluminista.

Nesse caso, o ônus democrático do *devido processo legal* através do dever de a acusação expor os meios de obtenção da prova esbarraria nas sombras dos segredos da Inteligência pública e dos segredos corporativos. Esbarraria em seus métodos sub-reptícios e colaborativos de se obter uma informação extraterritorialmente.

Assim, a solução é: melhor não ir pela porta aberta do devido processo legal.

Sob este pilar paira uma transparência inconveniente que fere outros interesses.

Melhor adicionar mais uma camada de opacidade ao debate.

Negligenciemos. Tranquemos algumas portas.

“Panos quentes” – (com a licença do prosaísmo).

Discricionariedades persecutórias utilitárias?

Alguém sugere alguma saída alternativa? Que tal soluções retaliatórias de ordem comercial via órgãos internacionais? Por que não, amigos úteis?

Quando o ônus democrático pode demonstrar, talvez, que não haja tanta democracia assim.

5. CONCLUSÃO

Nos últimos anos, o emprego de fortes padrões criptográficos em bens e serviços utilizados massivamente na sociedade atual, notadamente o uso da criptografia ponta a ponta, introduziu, de largada, dificuldades à efetividade de práticas persecutórias estatais tradicionais, como a interceptação ou a entrega do conteúdo de comunicações privadas (armazenadas ou em fluxo).

Na perspectiva das forças de segurança, endossa-se a narrativa segundo a qual o aparato persecutório estatal estaria "indo às escuras" – *going dark* – em razão da criptografia e que o debate seria representativo de um embate - *trade-off* - entre, de um lado, privacidade e, de outro lado, a segurança pública.

Como efeito desse suposto antagonismo de valores – privacidade vs. segurança - proliferam-se pedidos de autoridades públicas para a introdução de *backdoors*/vulnerabilidade nas infraestruturas comunicativas, sobretudo as novas comunicações digitais, de modo a franquear ao Estado o acesso excepcional aos dispositivos para fins de interceptação, ou mesmo que sejam adotados outros meios de enfraquecimento e/ou contorno do espectro protetivo da criptografia presente nesses suportes. Esse tipo de reação estatal em face da criptografia não é novo.

Diferentemente do argumento das forças de segurança e seus pedidos pela introdução de *backdoors* nas infraestruturas TICs, é o argumento dos especialistas em cibersegurança ao analisarem, tecnicamente, as referidas pretensões estatais. Em síntese, a comunidade técnica adota o argumento da unidade da insegurança trazida pela introdução dos *backdoors*: adverte-se que as vulnerabilidades criadas para o acesso excepcional em favor do Poder Público trariam o risco de, igualmente, franquear essas falhas à exploração por terceiros mal-intencionados.

Afirma-se que as infraestruturas comunicativas teriam a sua integridade abalada, engendrando-se, em razão dos *backdoors*, um estado de insegurança generalizado. Nessa linha, argumenta-se que o dilema cripto não seria representativo de um conflito - *trade-off* - entre privacidade vs. segurança, mas um sopesamento entre segurança vs. segurança. A comunidade técnica vale-se do argumento consequencialista: o de que os *backdoors* estatais ampliariam a superfície de ataque das infraestruturas e, assim, suscitam um juízo de

possibilidade: terceiros mal intencionados se sentirão atraídos por essas falhas e poderão explorá-las. Logo, é a segurança quem perderá.

Por outro lado, há de se reconhecer que a criptografia em alguns suportes comunicativos, sobretudo digitais e que operam através da internet, introduz, inflexivelmente, um escudo difuso sobre as trocas e armazenamentos informativos privados, impedindo o acesso ao conteúdo inteligível pelo Estado, ao menos, por meio de suas práticas *tradicionais* de formação da prova – v.g. interceptação -, ainda que sejam adotados os mecanismos de freios e contrapesos, isto é, os corolários do devido processo legal: supervisão judicial por mandado, ordem específica, proporcionalidade, interceptação controlada para fins específicos, etc.

Há de se reconhecer que a criptografia, ao menos de imediato, dificulta algumas práticas tradicionais de formação da prova, de formação de uma verdade jurídica e, consequentemente, da duração razoável de um sistema doméstico de distribuição de responsabilizações, sejam elas penais ou até mesmo civis.

Contudo, narra-se que o enfraquecimento ou mesmo a extinção de práticas fiscalizatórias públicas tradicionais pela criptografia não seria necessariamente ruim. Por que? Porque outros valores, dito humanos, serão prestigiados e porque o Estado poderia evoluir e, assim, desempenhar seus poderes investigativos e fiscalizadores para além da flexibilização da criptografia.

Pede-se que o Estado busque outros meios alternativos de acesso aos dados sem que as medidas de segurança aplicadas sobre as TICs sejam enfraquecidas. Para tanto, recomenda-se a adoção de outros sucedâneos investigativos forenses encontráveis na Era de Ouro da Vigilância em que nos encontramos. Investigações através de: i) metadados; ii) localização via GPS; iii) monitoramento de redes sociais; iv) acesso a dados armazenados em nuvem; v) acesso à informação em dispositivos *smarts* caseiros, como a *smart* TV da *Samsung* ou o sistema *Alexa* da *Amazon*; vi) compartilhamento e integração de bancos de dados, entre outros meios.

A saída para o *going dark* será a Era de Ouro da Vigilância? Parece-nos assustador o fato de abraçar-se tamanha virada para os novos meios de formação de uma verdade jurídica, para esses novos meios de formação probatória, sem que se indague a legitimidade desses meios, quem fornecerá esses meios ao Estado e, tampouco se valore, historicamente, qual ou quais Estados estão ancorados em

práticas probatórias tradicionais e quais Estados já podem descartá-las, pois a seu serviço estão os novos métodos. Parece haver uma valoração, de antemão, desses novos meios em relação aos meios tradicionais e que se encontram atenuados ou suprimidos pela criptografia utilizada massivamente em infraestruturas digitais.

Seria prudente tecer algumas perguntas para futuras explorações dessa saída apontada para o Estado: os mercadores de infraestrutura blindados pela criptografia irão produzir alguma regra de transição para países calcados em métodos persecutórios tradicionais atingirem uma efetividade adequada dos novos meios persecutórios? E mais, uma efetividade balanceada o suficiente para que não sejam erodidos os direitos fundamentais que serão ameaçados por esses meios? Ou outra: quais condutas reprováveis possuem apuração inexoravelmente dependente do conhecimento do conteúdo trocado? Do ponto de vista social, a apuração da criminalidade do colarinho branco será mais fácil ou mais difícil de se apurar sem que se acesse rapidamente o conteúdo, tal como ocorre na interceptação? A jornada em busca dos novos métodos forenses não teria a aptidão de enviar algumas polícias judiciárias, Ministérios Públicos e Sistemas Judiciais de volta ao ensino fundamental da investigação, cujos novos professores são os especialistas em cibersegurança e os grandes armazenadores de dados? Parece-nos que essas preocupações poderiam ser mais bem consideradas no debate.

Em rigor, as considerações acima seriam um breve resumo do atual debate envolvendo a criptografia e os *backdoors*. Elas espelham um grupo de valorações positivas e um grupo de valorações negativas. Valora-se negativamente a introdução de *backdoors* nas infraestruturas digitais, sobretudo através do argumento técnico de que a introdução de vulnerabilidades para e em razão do Estado engendraria um quadro de insegurança e potencial captura dessas falhas por terceiros, além de que seria demasiadamente custosa, reverteria algumas boas práticas da internet e poderia introduzir um conflito geopolítico sobre quem armazenaria as chaves da decriptação.

Sob essa perspectiva, as vulnerabilidades propositais – para o Estado – não são vistas como bons olhos. São vistas como possíveis riscos à segurança. Longe de querer contestar essas colocações, buscamos, ao longo desse estudo, demonstrar que também é necessário levar em conta os possíveis movimentos dos variados atores envolvidos no debate, de modo que a discussão sobre criptografia e

backdoors também possa considerar algumas peculiaridades, espinhosas, capazes de introduzir algumas considerações sobre aqueles enquadramentos de valores em conflito: privacidade vs. segurança ou segurança vs. segurança.

É além dessa perspectiva que buscamos demonstrar que as vulnerabilidades são inerentes às comunicações interconectadas. Que os *backdoors* são inerentes às TICs, suas fontes decorrem de uma relação entre as novas tecnologias e as técnicas de defesa autofágicas dessas tecnologias. Buscamos demonstrar que existem muitos *backdoors*, que suas fontes não são necessariamente os *backdoors* estatais. Mas, sobretudo, demonstrar a relação entre essas outras espécies e os sujeitos de conhecimento dessas falhas. Que essas outras fontes de vulnerabilidades, acidentais, são de conhecimento de poucos atores, que esses atores operam à sombra do debate, que possuem meios sub-reptícios de acesso aos dados à revelia da criptografia e que, não raro, na perspectiva transnacional do debate, há um horizonte de acordos informais entre setor privado e seus governos sedes para colaboração quanto ao acesso aos dados.

As políticas da criptografia, portanto, políticas do seletivamente ininteligível, nunca estão reduzidas ao prisma vertical e interno de um ou outro Estado. Não se encerram na adoção de uma regulação A ou B. Necessárias são as considerações sobre os fatores que moldam o arranjo sociotécnico dos envolvidos. O debate, em geral, costuma apontar para os malefícios do Estado A ou do Estado B em se adotar a política criptográfica com intensidades X ou os *backdoors* com intensidades Y. No entanto, a arena é transnacional.

O argumento e as preocupações da comunidade técnica são louváveis, mas eles devem ser contextualizados com o arranjo de atores que dominam os saberes sobre as vulnerabilidades e a arena transnacional de acesso aos dados. É nesse sentido que no capítulo 2 buscamos enfatizar que o debate está ancorado num possível acordo extremamente frágil: a de que a cada ator envolvido irá renunciar a sua possibilidade de explorar alguma vulnerabilidade acidental para que a infraestrutura informativa e comunicacional reste íntegra. O acesso dar-se-á por outros meios.

Poder-se-ia argumentar que todo o argumento dos técnicos é contrário a toda e qualquer vulnerabilidade, e que o objetivo central é não haver a exploração de

qualquer vulnerabilidade, seja ela acidental ou intencional. Mas isso é realista? A NSA deixaria de explorar essas falhas? Os imperativos de defesa seriam renunciados? Seria como esperar que todos votem nulo.

Os conhecimentos sobre as vulnerabilidades e os saberes de sua defesa e de seu ataque são incessantes, eles se renovam a cada nova invenção, a cada nova interação em rede. As ofertas da cibersegurança também se renovam, autofagicamente. E isso nos empurra ao solucionismo tecnológico da cibersegurança e seu clientelismo cruzado com as Inteligências.

O ponto é: como fica a relação entre países que introduziram fortes padrões criptográficos e países que podem contornar esses padrões, mas ambos operando na mesma arena transnacional? O padrão de segurança produz efeitos impeditivos de acesso ao inteligível à quais sujeitos, mas produz efeitos acessíveis à quais outros?

Não se diz muito sobre quem tem e quem não tem a *expertise* dos meios sub-reptícios de acesso aos dados. Há uma opacidade imensa sobre os sujeitos de conhecimento desses meios. Tampouco se compara a blindagem do acesso ao conteúdo pelas jurisdições locais, seja pela política pública criptográfica interna, seja, na ausência dessa, pela própria política criptográfica da empresa de plantão, com outros meios sub-reptícios de acesso aos dados, independentemente da criptografia, e que estão sob domínio de atores muitas vezes externos. Ou tampouco é apresentado como se formam as vulnerabilidades/*backdoors* nas infraestruturas e quais atores possuem os segmentados domínios de saberes aptos a exploração utilitária dessas falhas.

As condições de acesso parecem ser historicamente, tecnologicamente e financeiramente assimétricas entre os diversos atores envolvidos. Se considerarmos, por benefício da dúvida, que existe uma forte assimetria de acesso por diferentes atores, considerada uma infraestrutura comum, qual seria a função da criptografia para esses atores que não podem superá-la? A criptografia estaria funcionalizada ao ordenamento ou seria o ordenamento que estaria funcionalizado à criptografia? Criptografia de quem? De quem pode superá-la?

Assimetrias Criptográficas Engendram Soberanias Soprepostas Opacamente – A.C.E.S.S.O? Aparentemente, o *trade-off* que envolve a criptografia também possui uma série de fatores que operam para fragilizar e/ou fortalecer uma

jurisdição em face da outra. A discussão sobre os *backdoors* voluntários, para o Estado, corre o risco de ser convertida em um espúrio meio de *acesso mutuamente assegurado*, haja vista a existência de outros meios de contorno da criptografia à cargo de colaborações opacas entre empresas e seus governos. Pior do que o acesso de todos os países seriam os privilégios de acesso de uns, mas não de outros.

Quando há muitas variáveis, o terreno da discussão não pode partir de cada uma dessas especificidades regulatórias locais. O limbo e a confusão devem ser enfrentados, como qualquer discordância, pelas premissas compartilhadas, os elemento comuns que fundem esse fenômeno e que descem deus tentáculos para cada jurisdição local. Um desses elementos é a própria natureza transfronteiriça da rede e, assim, toda discussão poderia levar em conta a infraestrutura (sobretudo a sua base física) e como se engendram suas vulnerabilidades. Outro elemento comum são justamente os atores que operam transnacionalmente, os intermediários de dados e informações ininteligíveis/encriptadas.

Intermediários comuns para diferentes jurisdições e diferentes usuários. E isso atrai a pergunta sobre como eles operam: acordos informais? A criptografia é um custo de produção para a proteção de suas infraestruturas ou um instrumento de proteção humana? Eles são o compartilhamento de premissas dentro desse quebra – cabeça. E não compreendemos, pois não possuímos as ferramentas epistemológicas para tanto. A opacidade é a característica desse elemento comum e as ferramentas da transparência se encontram em tensão direta com os seus segredos corporativos.

As considerações sobre as pré-condições dos meios de acesso aos dados/informações encriptadas podem introduzir uma hierarquia de acessos à sombra das soberanias, facilitadas para uns, dificultadas para outros, problematizada, ainda mais, se considerarmos os acordos informais que a grande caixa preta da espionagem jamais vai, de boa vontade, abrir.

Ora, argumentar contra os *backdoors*, apesar de nobre, pressupõe, no mínimo, o fim das comunidades de Inteligência, que são constituídas justamente para, dentro de suas competências, explorar essas falhas tecnológicas acidentais. Pressupõe, igualmente, que exista um padrão técnico universal e inviolável. Pressupõe que o mercado exerça sua liberdade de design de modo a ser superior aos

poderes das Inteligências, que sejam superadas as razões de Estado. Parece utópico, infelizmente. Logo, se pode ser utopia, talvez seja prudente enxergar nesse debate um mecanismo de seletividade de jurisdições quanto ao conhecimento do ininteligível, mas, advirtamos: provisoriamente ininteligível. Os insumos à espera das chaves da compreensão.

Veda-se a captura do conteúdo em trânsito às jurisdições locais sob o argumento de proteção da privacidade, muito embora esse conteúdo em trânsito não seja apenas conversas, trocas de figurinhas, vídeos ou áudios ou qualquer outra expressão da liberdade dos comuns, mas também cifras, e símbolos de 1 ou 0, códigos de energia elétrica, propriedade intelectual, segredos de Estado, as informações realmente relevantes que governam o mundo, mas agora convertidas em *bits*. Não seriam apenas dados pessoais sensíveis, mas informações sensíveis. Objetos sensíveis. Segredos sensíveis.

No entanto, na ADPF 403, por ora, o Ministro Fachin avançou e optou por uma decisão que, de antemão, afasta qualquer possibilidade de ação estatal persecutória-judicial nacional sobre tecnologias com recursos criptográficos, o que é problemático, pois numa arena transnacional de fluxos informativos, o conteúdo que é inacessível para uns, por força de certos padrões criptográficos, não o é para outros, que podem driblar esses padrões e capturar o mesmo conteúdo. Nessa linha, a decisão do Ministro tem a potência de dificultar as práticas do aparato persecutório-judicial nacional, facilitando, indiretamente, a ação de outros poderes, não raro, externos, mais opacos e que não precisam da criptografia. Almeja-se proteger o humano, mas opera-se como uma linha auxiliar involuntária de outros interesses, em nada humanos.

Quando posicionamentos jurídicos sinalizam para a introdução da criptografia como elemento de blindagem da infraestrutura digital geralmente o fazem em prestígio da proteção humana, mas podem desconsiderar os atores e arranjos que se acoplam nas bordas desse debate e que, salvo melhor juízo, poderiam ser mais bem iluminados. Nessa linha, a criptografia pode desempenhar uma função diversa. Domesticamente, prestigiar, narrativamente, a proteção das comunicações privadas, mas no plano externo, decotar a própria efetividade do aparato persecutório-judicial nacional em detrimento de outros ordenamentos mais

fortes e dotados de outros saberes de acesso aos mesmos dados, mas à revelia da criptografia.

Talvez seja melhor esperar um amadurecimento do problema, sem que se dê o primeiro passo à frente. Podemos nos moldar pela realidade das dificuldades externamente impostas e intransponíveis, e não pelos sonhos do *dever ser* internos.

Podemos correr o risco de, ao adotarmos um política criptográfica em descompasso com as opacas políticas de seu contorno, introduzirmos um Cavalo de Tróia no ordenamento nacional. Uma intensidade criptográfica X implica uma intensidade de acesso sub-reptício Y > X. A arena comum: a rede interconectada. Quais atores possuem os seletivos acessos ao inteligível? Qual a relação de proximidade desses atores com outros ordenamentos? Um brasileiro, agora, poderá invocar a Quinta Emenda?

Se as modelagens de segurança cibernética amputam braços domésticos de acesso aos dados ou criam próteses de acesso extraterritorial aos mesmos dados por força da arena transnacional interconectada e das colaborações opacas dos intermediários, esse é um ponto espinhoso, mas que pode ser o coração do problema.

Não podemos nos esquecer, por fim, da própria estrutura da criptografia. Sua função primordial e interna é tornar um objeto ininteligível e, subsequentemente e externamente, introduzir um espectro de circulação desse objeto entre aqueles que possuem as condições materiais da decifração, as chaves.

Uma informação somente circula se é compreendida. A circulação da informação pressupõe o compartilhamento de premissas, o compartilhamento da inteligibilidade de algo, das condições de acesso. Cifrar, tornar ininteligível, é controlar os domínios da circulação da informação. É inviabilizar que terceiros indesejados, desprovidos do aparato técnico da decriptação, compreendam o conteúdo da informação que se circula no mundo e que se armazena. Produz uma seletividade utilitária aos detentores das chaves. Não nos parece prudente haver posicionamentos de antemão em que se valore um fenômeno somente pelo fato de que paira, sobre ele, a criptografia. A legitimidade da criptografia não estaria na análise concreta de quem são os terceiros indesejados excluídos da inteligibilidade? Sobretudo, se forem terceiros humanos?

Compreender é o resultado de um regime de interações. Selecionar os sujeitos da compreensão é um ato político. Por outro lado, existem inúmeros modos de interagir e de se comunicar no mundo. Modos sob o domínio de diferentes sujeitos, diferentes comunidades, diferentes tribos, diferentes culturas. E a infraestrutura que dá suporte a esses modos? Cada um desses modos deve possuir um tipo de infraestrutura que lhe dá suporte. Mas as perguntas seriam: esses outros modos e a base física que materializa esses modos também são extensões da liberdade de expressão desses sujeitos? Suas infraestruturas são intocáveis? Seus direitos foram encriptados?

Reservamo-nos, com a devida licença, se possível, concluir esse estudo através do recorte de uma passagem aparentemente sem sentido com o contexto aqui discutido. No entanto, conforme avisado no início dessa estrada, falar sobre criptografia é, também, falar nas entrelinhas. Portanto, considerando que, no fundo, estamos falando sobre comunicações, sobre QUEM pode compreender O QUE, sobre quem pode transmitir o que, entre outras ideias associadas às infraestruturas comunicativas, eu novamente peço a condescendência do(a) leitor(a) para que busque colher as diferentes sensibilidades interativas de cada um desses modos comunicativos que habitam o nosso tempo, mas, sobretudo, a diferença entre os sujeitos da compreensão e da materialização desses modos e a luta, encriptada, pela coexistência desses sujeitos.

Assim sendo, tomo de empréstimo uma passagem não de juristas, mas da própria arte, sobretudo daquele tipo de arte que opera através da grafia e cuja tradicional infraestrutura que lhe dá suporte pode ter as suas medidas de segurança do conteúdo violadas por um gesto simples e universal a cargo dos dedos da mão humana: girar a capa protetiva num movimento de 180 graus da direita para a esquerda:

> Eu estava dirigindo meu Lexus, contra o vento. Esse carro é montado numa área de trabalho completamente isenta de presenças humanas. Sem uma gota de suor mortal, com exceção, vá lá, dos sujeitos que saem da fábrica dirigindo o produto - eles devem deixar um pouco de umidade no volante. O sistema flui ininterrupto, automatizado, com uma perfeição sacerdotal, cada movimento suave devidamente registrado para garantir um desempenho perfeito. Carrocerias ocas sendo produzidas numa sequência infindável. Ninguém na linha de montagem que sofra de nervos cafeinados ou tenha histórico de depressão clínica. Apenas a tessitura sinistra de ligas de cromo transportadas em arcos entrelaçantes, blocos de ferro e folhas de asfalto, cromados suspensos descendo para serem encaixados e soldados.

> Robôs apertando porcas, máquinas programadas que não sonham com familiares falecidos.[171]

24/7 x (0.0; 0.1; 1.0; 1.1; .....“.”)

Polegares, polegares, polegares...

[171] DELILLO, Don. Submundo, 1999, p.57.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABELSON, Harold et al. ***Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*.** MIT Press. Cambridge, 2015. Disponível em: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>. Acesso em: 10 abr. 2022.

ADITYA, J., SHANKAR RAO, P. - ***Quantum Cryptography.*** Computer Science Engineering at Andhra University. Disponível em: <https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf>. Acesso em: 10 abr. 2022.

ALIMONTI, Veridiana – ***Criptografia, direitos e a problemática polarização entre "privacidade individual" e "segurança coletiva"***, *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

AMADEU, Sérgio – ***Brasil, colônia digital***. Instituto Humanista UNISINOS, 2020. Disponível em: <http://www.ihu.unisinos.br/600360-brasil-colonia-digital-artigo-de-sergio-amadeu>. Acesso em: 10 abr. 2022.

AMNESTY INTERNATIONAL – ***Spain: EU must act to end spyware abuse after prominent Catalans targeted with Pegasus***. 18 April, 2022. Disponível em: <https://www.amnesty.org/en/latest/news/2022/04/spain-pegasus-spyware-catalans-targeted/>. Acesso em: 10 abr. 2022.

AMNESTY INTERNATIONAL - ***The Pegasus Project: How Amnesty Tech uncovered the spyware scandal***. 23 March, 2022. Disponível em: <https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/>. Acesso em: 10 abr. 2022.

ANONYMOUS And Secure Network-based Interaction. Depositante: Microsoft Corporation. US 8458349 B2. Depósito: 6 jun. 2011. Concessão: 4 jun. 2013.

AQUINO, Mirian. ***Anatel Começa A Verificar Se Tem Backdoor Em Produtos De Telecom No Brasil No Segundo Semestre***. **TELE SÍNTESE**, [*S. l.*], p. 1-1, 25 mar. 2021. Disponível em: <https://www.telesintese.com.br/anatel-comeca-a-verificar-se-tem-backdoor-em-produtos-de-telecom-no-brasil-no-segundo-semestre/>. Acesso em: 10 abr. 2022.

ARANDA, Julieta; WOOD, Brian Kuan; VIDOKLE, Anton – ***The Internet Does Not Exist***. E-journal: Sternberg Press, 2015.

ARANHA, Diego F. - ***O que é a criptografia fim a fim e o que devemos fazer a respeito?*** *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

ARTICLE 29 DATA PROTECTION WORKING PARTY. ***Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU***. Bruxelas, 2018. Disponível em: <https://www.aepd.es/sites/default/files/2019-09/art29-statement.pdf>. Acesso em: 10 abr. 2022.

ASSANGE, Julian, APPELBAUM, Jacob, MULLER-MAGUHN, Andy, ZIMMERMANN, Jeremy – ***Cypherpunks: liberdade e o futuro da internet***. Tradução Cristina Yamagami, São Paulo: Boitempo, 2013.

BALL, James; BORGER, Julian; GREENWALD, Glenn. ***Revealed: how US and UK spy agencies defeat internet privacy and security***. The Guardian, [S. l.], p. 1-1, 6 set. 2013. Disponível em: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 10 abr. 2022.

BENSON, Robert L. NSA/CSS – ***THE VENONA STORY***. Disponível em: <https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/venona_story.pdf>. Acesso em: 10 abr. 2022.

BIDDLE, Sam. ***How Peter Thiels's Palantir Helped the NSA spy on the whole world: Documents provided by NSA whistleblower Edward Snowden reveal Palantir role in creating the U.S. governments international spy machine***. The Intercept, [*S. l.*], p. 1-1, 22 fev. 2017. Disponível em:

<https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/>. Acesso em: 10 abr. 2022.

BITANSKY, Nir, CANETTI, Ran, GARG, Sanjam, HOLMGREN, Justin, JAIN, Abhishek et al. ***Indistinguishability Obfuscation for RAM Programs and Succinct Randomized Encodings.*** Vol. 47, No. 3, pp. 1123–1210, MIT, 2018. Disponível em: <https://dspace.mit.edu/bitstream/handle/1721.1/137817/15m1050963.pdf?sequence=2>. Acesso em: 10 abr. 2022.

BOBBIO, Norberto – ***Da estrutura à função: novos estudos da teoria do direito***. Tradução Daniela Versiani. Barueri, SP: Manoele, 2007.

BODRIAGOV, Oleksandr e BUCHEGGER, Sonja - ***Encryption for Peer-to-Peer Social Networks.*** School of Computer Science and Communication KTH - The Royal Institute of Technology Stockholm, Sweden. 2011. Disponível em: <http://www.peerson.net/papers/spsn2011.pdf>. Acesso em: 10 abr. 2022.

BOROWSKA, Anna and RZESZUTKO, Elżbieta – ***The cryptanalysis of the enigma cipher. The plugboard and the cryptologic bomb***. Computer Science. Vol. 15, nº 4, 2014. Disponível em: <https://doi.org/10.7494/csci.2014.15.4.365>. Acesso em: 10 abr. 2022.

BRANCO, Sérgio – ***Memória e esquecimento na internet***. Porto Alegre: Arquipélago Editorial, 2017.

BRASIL. ABNT NBR ISO/IEC 27002:2005. ***Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação***. Disponível em: <https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf >. Acesso em: 10 abr. 2022.

BRASIL. ANATEL. Análise nº 178/2020/VA. Processo Administrativo Processo nº 53500.060032/2017-46. ***Reavaliação da regulamentação visando diminuir barreiras regulatórias à expansão das comunicações Máquina-a-Máquina e da Internet das Coisas***. Conselheiro: Vicente Bandeira de Aquino Neto. Boletim de Serviço Eletrônico em 03/11/2020. Disponível em: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_ex

terna.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO6yRUAVOQVFdXLPeDggveAxcE4-tlqW-MeX1k1TbwBPtMONOL6_rN0i1fibBRqmPQdArtM-hTvIvm0w5MrjUv00>. Acesso em: 10 abr. 2022.

BRASIL. ***Ato n.º 77 de 5 de janeiro de 2021 da ANATEL***. Disponível em: <https://www.in.gov.br/en/web/dou/-/ato-n-77-de-5-de-janeiro-de-2021-297933302>. Acesso em: 10 abr. 2022.

BRASIL. ***Constituição da República Federativa do Brasil de 1988***. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 10.024, de 20 de setembro de 2019. ***Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10024.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 10.046, de 9 de outubro de 2019. ***Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 10.748, de 16 de julho de 2021. ***Institui a Rede Federal de Gestão de Incidentes Cibernéticos***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 10.777, de 24 de agosto de 2021. ***Institui a Política Nacional de Inteligência de Segurança Pública.*** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10777.htm.

BRASIL. Decreto n.º 10.778, de 24 de agosto de 2021. ***Aprova a Estratégia Nacional de Inteligência de Segurança Pública***. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10778.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 10.822, de 28 de setembro de 2021. ***Institui o Plano Nacional de Segurança Pública e Defesa Social 2021-2030***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10822.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 5.450, de 31 de maio de 2005. ***Regulamentava o pregão, na forma eletrônica, para aquisição de bens e serviços comuns***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5450.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 592, de 6 de julho de 1992. ***Pacto Internacional sobre Direitos Civis e Políticos – PIDCP.*** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 678, de 6 de novembro de 1992. ***Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica).*** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 7.724, de 16 de maio de 2012. ***Regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI).*** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 7.845, de 14 de novembro de 2012. ***Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 8.771, de 11 de maio de 2016. ***Regulamenta a Lei n.º 12.965/2014 (Marco Civil da Internet – MCI)***. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 9.489, de 30 de agosto de 2018. ***Regulamenta, no âmbito da União, a Política Nacional de Segurança Pública e Defesa Social*.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9489.htm>. Acesso em: 10 abr. 2022.

BRASIL. Decreto n.º 9.637, de 26 de dezembro de 2018. ***Institui a Política Nacional de Segurança da Informação*.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 10.176, de 11 de janeiro de 2001. ***Altera a Lei no 8.248/1991***. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/LEIS/LEIS_2001/L10176.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 12.527 de 18 de novembro de 2011. ***Lei de Acesso à Informação (LAI)***. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/Lei/L12527.htm#art37>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 12.654, de 28 de maio de 2012. ***Dispõe sobre a coleta de perfil genético como forma de identificação criminal***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. ***Marco Civil da Internet***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 13.506, de 13 de novembro de 2017. ***Altera a Lei n.º 6.385 de 7 de dezembro de 1976.*** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13506.htm#art35 >. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 13.674, de 11 de junho de 2018. ***Altera a Lei nº 8.248, de 23 de outubro de 1991***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13674.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 13.675, de 11 de junho de 2018. ***Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp)***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. ***Lei Geral de Proteção de Dados Pessoais (LGPD)***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 13.853 de 08 de julho de 2019. ***Altera a Lei nº 13.709/2018***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 14.069/2020, de 1 de outubro de 2020. ***Cria o Cadastro Nacional de Pessoas Condenadas por Crime de Estupro.*** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14069.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 14.232, de 28 de outubro de 2021. ***Institui a Política Nacional de Dados e Informações relacionadas à Violência contra as Mulheres (PNAINFO)***. Disponível em: <https://www.in.gov.br/en/web/dou/-/lei-n-14.232-de-28-de-outubro-de-2021-355729305>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 6.385, de 7 de dezembro de 1976. ***Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários.*** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l6385.htm >. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 8.248, de 23 de outubro de 1991. ***Dispõe sobre a capacitação e competitividade do setor de informática e automação*.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8248.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei n.º 9.296/96 de 24 de julho de 1996. ***Lei das Interceptações*.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 10 abr. 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. ***Institui o Código Civil*****.** Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

BRASIL. Medida Provisória n.º 810, de 8 de dezembro de 2017. ***Altera a Lei nº 8.248, de 23 de outubro de 1991***. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Mpv/mpv810.htm>. Acesso em: 10 abr. 2022.

BRASIL. Medida Provisória n.º 869, de 27 de dezembro de 2018. ***Altera a Lei nº 13.709/2018.*** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 10 abr. 2022.

BRASIL. Mensagem n.º 451, de 14 de agosto de 2018. ***Veto Presidencial*****.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em: 10 abr. 2022.

BRASIL. Mensagem n.º 574, de 23 de outubro de 1991. ***Veto presidencial.*** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/Mensagem_Veto/anterior_98/VEP-LEI-8248-1991.pdf>. Acesso em: 10 abr. 2022.

BRASIL. Resolução n.º 740 de 21 de dezembro de 2020. ***Aprova o Regulamento de Segurança Cibernética Aplicado ao Setor de Telecomunicações*****.** Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776>. Acesso em: 10 abr. 2022.

BRASIL. STF, **ADC 51 DF**. Relator: Ministro Gilmar Mendes. 28/11/2017. JusBrasil. 2017. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>. Acesso em: 10 abr. 2022.

BRASIL. STF, **ADI 4.829 DF**. Relatora: Ministra Rosa Weber. 09/08/2012. JusBrasil. 2012. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>. Acesso em: 10 abr. 2022.

BRASIL. STF, **ADI 5.527 DF**. Relatora: Ministra Rosa Weber. 13/05/2016. JusBrasil. 2016. Disponível em: <

https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282 >. Acesso em: 10 abr. 2022.

BRASIL. STF, **ADI 6.529 DF**. Relatora: Ministra Carmén Lúcia. 04/08/2020. JusBrasil. 2020. Disponível em: < https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238 >. Acesso em: 10 abr. 2022.

BRASIL. STF, **ADI 6.649 DF**. Relator: Ministro Gilmar Mendes. 18/12/2020. JusBrasil. 2020. Disponível em: < https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238 >. Acesso em: 10 abr. 2022.

BRASIL. STF, **ADPF 403 SE**. Relator: Ministro Edson Fachin. 03/05/2016. JusBrasil. 2016. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500>. Acesso em: 10 abr. 2022.

BRASIL. STF, **ADPF 695 DF**. Relator: Ministro Gilmar Mendes. 15/06/2020. JusBrasil. 2020. Disponível em: < https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693 >. Acesso em: 10 abr. 2022.

BRASIL. STF, **PETIÇÃO n. 9.935/DF.** Relator: Ministro Alexandre de Moraes. 20/03/2022. Disponível em: < https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/DecisaoTelegram20mar.pdf >. Acesso em: 10 abr. 2022.

BRASIL. STJ – **MS 26.627/DF**, Rel. Ministro SÉRGIO KUKINA, Primeira Seção, julgado em 09/03/2022, - DJe 27/04/2022.

BRASIL. STJ - **REsp 1.885.201/SP**, Rel. Ministra NANCY ANDRIGHI, Terceira Turma, julgado em 23/11/2021, DJe 25/11/2021.

BRASIL. STJ - **RMS 60.531-RO**, Rel. Ministro NEFI CORDEIRO, Rel. Acordão Ministro RIBEIRO DANTAS, Terceira Seção, julgado em 09/12/2020, DJe 17/12/2020.

BRITISH – U.S. COMMUNICATION INTELLIGENCE AGREEMENT. 1946. Disponível em: <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/ukusa/agreement_outline_5mar46.pdf>. Acesso em: 10 abr. 2022.

BROOKE-HOLLAND, Louisa, CURTIS, John and MILLS, Claire – ***The AUKUS agreement.*** House of Commons, Library. 11 October 2021. Disponível em: https://researchbriefings.files.parliament.uk/documents/CBP-9335/CBP-9335.pdf

BRUNTON, Finn e NISSENBAUM, Helen – ***Obfuscation: a user's guide for privacy and protest.*** 1ª ed. - United States: MIT Press paperback edition, 2016.

BURNS, Thomas L. - ***The Quest for Cryptologie Centralization and the Estabelishment os NSA: 1940 – 1952***. Series V: The Early Postwar Period, vol. VI. Center for Cryptologic History, 2005.

CARTA CAPITAL. ***Procuradores da Lava Jato tentaram comprar programa espião israelense Pegasus: Documentos protocolados pela defesa do ex-presidente Lula comprovam negociações entre Operação e empresa dona do programa desde 2018***. BRASIL, 26 jul. 2021. Política, p. 1-1. Disponível em: <https://www.cartacapital.com.br/politica/procuradores-da-lava-jato-tentaram-comprar-programa-espiao-israelense-pegasus/>. Acesso em: 10 abr. 2022.

CASTELVECCHI, Davide – ***This Is the Fastest Random-Number Generator Ever Built: A laser generates quantum randomness at a rate of 250 trillion bits per second and could lead to devices small enough to fit on a single chip***. Scientific American – Nature magazine. On March 3, 2021. Disponível em: <https://www.scientificamerican.com/article/this-is-the-fastest-random-number-generator-ever-built/>. Acesso em: 10 abr. 2022.

CASTRO, Daniel, BANKSTON, Kevin, DAVIDSON, Alan, e STEPANOVICH, Amie – ***Has the NSA Won The Crypto Wars?*** - Clipper Chip debate of the 1990s. 2013. Disponível em: <https://www.youtube.com/watch?v=_Qh7jRKn7wI>. Acesso em: 10 abr. 2022.

CAVOUKIAN, Ann – ***The 7 Foundational Principles.*** Privacy by Design. Ontario, Canada - Information and Privacy Commissioner of Ontario, 2011. Disponível em:

<https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 10 abr. 2022.

CAVOUKIAN, Ann; DIXON, Mark – Privacy and Security by Design: ***An Enterprise Architecture Approach.*** Information and Privacy Commissioner Ontario, Canada, 2013. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf. Acesso em: 10 abr. 2022.

CHAMAYOU, Grégoire – ***Oceanic enemy: A brief philosophical history of the NSA***, *Radical Philosophy*, 191, May/Jun 2015 Disponível em: <https://www.radicalphilosophy.com/commentary/oceanic-enemy. Acesso em: 10 abr. 2022.

CHAMAYOU, Grégoire. ***Patterns of life: a very short history of schematic bodies***. The Funambulist, [*S. l.*], v. 57, p. 1-1, 4 nov. 2014. Disponível em: <https://thefunambulist.net/editorials/the-funambulist-papers-57-schematic-bodies-notes-on-a-patterns-genealogy-by-gregoire-chamayou>. Acesso em: 10 abr. 2022.

CHAOS COMPUTER CLUB (CCC). ***Signed the open letter against backdoors*** - ***Planned encroachment on encryption of messenger services would have fatal consequences*****. IT security: CCC against weakening of encryption by law, 2019.** Disponível em**:** https://www.ccc.de/en/updates/2019/encrypted-messengers

CIPHERING Device. Depositante: Arthur Scherbius. US 1584660 A. Concessão: 11 maio 1926. Disponível em: <https://patentimages.storage.googleapis.com/41/1e/93/ea39ef52bf95db/US1556964.pdf>.
<https://patentimages.storage.googleapis.com/cb/ca/ff/d4d2e2e9adc7db/US1657411.pdf>.
<https://patentimages.storage.googleapis.com/e2/82/35/6e8429192f63ae/US1584660.pdf>. Acesso em: 10 abr. 2022.

CIPHERING Machine. Depositante: Arthur Scherbius. US 1657411 A. Concessão: 24 jan. 1928.

CLAUSEWITZ, Carl von – ***Da Guerra***. Tradução Maria Teresa Ramos. 3ª ed. - São Paulo: WMF Martins Fontes, 2010.

Coalition of the Gulf War. In: WIKIPÉDIA, a enciclopédia livre. Under United Nations Security Council Resolution 678, a coalition of 35 countries, led by the United States, fought Iraq in the Gulf War from 1990–1991. Disponível em: <https://en.wikipedia.org/w/index.php?title=Coalition_of_the_Gulf_War&oldid=1100511272>. Acesso em: 10 abr. 2022.

COLLBERG, Christian e NAGRA, Jasvir – ***Surreptitious Software: obfuscation, watermarking, and tamperproofing for Software Protection.*** Boston: Pearson Education, 2010.

COMPTROLLER and ADUTIOR GENERAL – National Audit Office – Department of Health Investigation: ***WannaCry cyber attack and the NHS***. HC/414 Session 2017-2019, 25 apr. 2018. Disponível em: <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>. Acesso em: 10 abr. 2022.

COOK, Tim – ***A Message to Our Customers. The Need for Encryption*** – Apple. February 16, 2016. Disponível em: <https://www.apple.com/customer-letter/>. Acesso em: 10 abr. 2022.

CRYPTOGRAPHY correctness detection methods and apparatuses. Depositante: Microsoft Corporation. US 7602903 B2. Depósito: 16 jan. 2004. Concessão: 13 out. 2009.

CUNHA E MELO, Mariana – ***Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças ao direito à privacidade no Brasil***. 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf>. Acesso em: 10 abr. 2022.

DANG, Nhan Tam, TRAN, Ha Manh, NGUYEN, Sinh Van, MALESZKA, Marcin & LE, Hai-Duong – ***Sharing secured data on peer-to-peer applications using attribute-based encryption.***

DARPA - Department of Defense Fiscal Year (FY) 2023 Budget Estimates April 2022. ***Defense Advanced Research Projects Agency Defense-Wide Justification***

Book Vol. 1 of 5 Research, Development, Test & Evaluation, Defense-Wide. Disponível em: <https://www.darpa.mil/attachments/U_RDTE_MJB_DARPA_PB_2023_APR_2022_FINAL.pdf>. Acesso em: 10 abr. 2022.

DATA anonymity and separation for user computation. Depositante: Amazon Technologies, Inc. US 9710671 B1. Depósito: 2 jan. 2015. Concessão: 18 jul. 2017.)

DEIBERT, Ronald J. - ***Shutting the backdoor: The perfils os National Security and Digital Surveillance Programs***. Canadian Defence e Foreign Affairs Intitute (CDFAI), 2013. Disponível em: <https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/377/attachments/original/1414207665/Shutting_the_Backdoor.pdf?1414207665>. Acesso em: 10 abr. 2022.

DENNING, Dorothy E**. – Interview, Oral History 424 -** Conducted by Jeffrey R. Yost on 11 April 2013. Computer Security History Project Naval Postgraduate School, Monterey, CA. 2013. Disponível em: <https://conservancy.umn.edu/bitstream/handle/11299/156519/oh424ded.pdf?sequence=1&isAllowed=y>. Acesso em: 10 abr. 2022.

DEPARTMENT OF JUSTICE – ***Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide: Defendants' Separate Campaigns Both Targeted Software and Hardware for Operational Technology Systems***, 24 março 2022. Disponível em: <https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical>. Acesso em: 10 abr. 2022.

DEPARTMENT OF JUSTICE – ***Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Defendants' Malware Attacks Caused Nearly One Billion USD in Losses to Three Victims Alone; Also Sought to Disrupt the 2017 French Elections and the 2018 Winter Olympic Games***. Monday, 19 out. 2020. Disponível em: <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>. Acesso em: 10 abr. 2022.

DELILLO, Don – ***Submundo.*** Companhia das Letras; 1ª edição. 1999.

DONEDA, Danilo e MACHADO, Diego – (coordenadores) – ***A Criptografia no Direito Brasileiro.*** São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo; ARANHA, Estela. ***O debate sobre o anonimato no caso do Sleeping Giants no Brasil***. ESTADÃO, [*S. l.*], p. 1-1, 15 dez. 2020. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/o-debate-sobre-o-anonimato-no-caso-do-sleep-giants-brasil/>. Acesso em: 10 abr. 2022.

DUDH - ***Declaração Universal de Direitos Humanos de 10 de dezembro de 1948***. Disponível em: < https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf >. Acesso em: 10 abr. 2022.

ELETRIC Ciphering Apparatus. Depositante: Arthur Scherbius. US 1556964 A. Concessão: 13 out. 1925.

ELETRONIC FRONTIER FOUNDATION (EFF) – ***Surveillance Self-defense. Metadata***. disponível em: <https://ssd.eff.org/pt-br/glossary/metadados>. Acesso em: 10 abr. 2022.

ESTADÃO. ***Caso Petrobras: Crime de "insider trading" teve só uma condenação penal em 20 anos: A comprovação dos casos é complexa, principalmente quando quem lucra com a informação vazada não é diretamente ligado à companhia***. [*S. l.*], 4 mar. 2021. InfoMoney, p. 1-1. Disponível em: <https://www.infomoney.com.br/mercados/crime-de-insider-trading-teve-so-uma-condenacao-penal-em-20-anos/>. Acesso em: 10 abr. 2022.

EUCLIDES – ***Os elementos***. Editora Unesp; 1ª edição. 2009.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) – ***Privacy by Default***. Disponível em: <https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en>. Acesso em: 10 abr. 2022.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. ***Regulation (EU) 2016/679. General Data Protection Regulation***. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 10 abr. 2022.

EVANINA, William R. ***National Counterintelligence Strategy of the United States of America 2020-2022***. 2020. Disponível em: <https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf>. Acesso em: 10 abr. 2022.

FEDERAL REGISTER. Presidencial documents. ***Administration of Export Controls on Encryption Products.*** Vol. 61, No. 224. Disponível em: <https://www.federalregister.gov/documents/1996/11/19/96-29692/administration-of-export-controls-on-encryption-products>. Acesso em: 10 abr. 2022.

FISHMAN, Andrew; VIANA, Natalia; SALEH, Maryam. ***EUA estão com a faca e o queijo na mão: Lava Jato faz de tudo para ajudar a justiça americana, inclusive blindar o governo brasileiro***. The Intercept BRASIL, p. 1-1, 12 mar. 2020. Disponível em: <https://theintercept.com/2020/03/12/lava-jato-driblou-governo-ajudar-americanos-doj/>. Acesso em: 17 fev. 2022.

FONNER, Kathryn L.; ROLOFF, Michael E. ***Testing the Connectivity Paradox: Linking Teleworkers? Communication Media Use to Social Presence, Stress from Interruptions, and Organizational Identification***. **Journal of Applied Communication Research**, [*S. l.*], v. 79, n. 2, p. 205-231, 2 jun. 2012. Disponível em: <https://www.researchgate.net/publication/263347954_Testing_the_Connectivity_Paradox_Linking_Teleworkers'_Communication_Media_Use_to_Social_Presence_Stress_from_Interruptions_and_Organizational_Identification>. Acesso em: 10 abr. 2022.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato – (coordenadores) – ***Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro***. 2ª ed. - São Paulo: Thomson Reuters Brasil, 2020.

FREEDOM OF INFORMATION ACT (FOIA). Disponível em: <https://www.foia.gov/foia-statute.html>. Acesso em: 18 dez. 2020.

GACEK, Cristina, LAWRIE, Tony, and ARIEF, Budi - ***The many meanings of Open Source***. Centre for Software Reliability Department of Computing Science University of Newcastle Newcastle upon Tyne NE1 7RU United Kingdom, 2014.

Disponível em: <https://www.researchgate.net/profile/Cristina-Gacek/publication/3248083_The_Many_Meanings_of_Open_Source/links/53d6a0ac0cf228d363ea77c9/The-Many-Meanings-of-Open-Source.pdf>. Acesso em: 10 abr. 2022.

GELLES, David; GOEL, Vindu. ***Facebook Enters $16 Billion Deal for WhatsApp***. **The** New York Times, [*S. l.*], p. 1-1, 19 fev. 2014. Disponível em: <https://archive.nytimes.com/dealbook.nytimes.com/2014/02/19/facebook-to-buy-messaging-start-up/>. Acesso em: 26 jan. 2022.

GELLES, David; GOEL, Vindu. ***WhatsApp rolls out full encryption to a billion messenger users.*** The Guardian, [*S. l.*], p. 1-1, 5 abr. 2016. Disponível em: <https://www.theguardian.com/technology/2016/apr/05/whatsapp-rolls-out-full-encryption-to-a-billion-messenger-users>. Acesso em: 12 jan. 2022.

GOLDSMITH, JACK e WU, Tim – ***Who Controls the internet?: illusions of a Borderless World.*** New York: Oxford University Press, 2006.

GROSSETTI, Michel – ***Les limites de la symétrie. À propos de l'ouvrage de Bruno Latour Changer de société. Refaire de la Sociologie***, Paris, La Découverte, 2006. Sociologies, Journal Open Edition, 2007. Disponível em: <https://doi.org/10.4000/sociologies.712>. Acesso em: 10 abr. 2022.

GUEDES, Gisela Sampaio da Cruz e MEIRELES, Rose Melo Vencelau. ***Término do tratamento de dados***. In: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro. 2ª Ed., São Paulo: Thomson Reuters Brasil, 2020.

GYAWALI, Yashant B. - ***ENCRYPTION ALGORITHM Advanced Encryption Standard.*** Caldwell University Caldwell, NJ, US. 2020. Disponível em: <https://www.researchgate.net/profile/Yashant-Gyawali/publication/345684900_ENCRYPTION_ALGORITHM_Advanced_Encryption_Standard/links/5faaba17299bf15bae065499/ENCRYPTION-ALGORITHM-Advanced-Encryption-Standard.pdf?origin=publication_detail>. Acesso em: 10 abr. 2022.

H.R.4922 - ***Communications Assistance for Law Enforcement Act***. Disponível em: <https://www.congress.gov/bill/103rd-congress/house-bill/4922/text>. Acesso em: 18 dez. 2020.

IHERING, Rudolf von – ***A luta pelo Direito.*** Tradução Edson Bini. 2ª ed., Edipro, 2019.

JAAP-KOOPS, Bert. ***Crypto Law Survey Version 27.0***. 2013. Disponível em: <http://www.cryptolaw.org/>. Acesso em: 10 abr. 2022.

JAFFE, Adam - ***The CEO of Cellebrite, the firm famous for helping the FBI crack into locked iPhones, says 'there is a race' to beat Apple from patching vulnerabilities it exploits.*** Cllebrite. June 16, 2021. Disponível em: <https://cellebrite.com/en/the-ceo-of-cellebrite-the-firm-famous-for-helping-the-fbi/>. Acesso em: 10 abr. 2022.

JOURNAL OF INFORMATION AND TELECOMMUNICATION, 2021. Disponível em: <https://doi.org/10.1080/24751839.2021.1941574>. Acesso em: 10 abr. 2022.

KELLER, Clara Iglesias; DONEDA, Danilo. ***Mirando em fakenews e acertando em vigilância: A identificação de usuários como estratégia falida de combate à desinformação***. PORTAL JOTA, [*S. l.*], p. 1-1, 24 jun. 2020. Disponível em: <https://www.jota.info/coberturas-especiais/liberdade-de-expressao/mirando-em-fake-news-e-acertando-em-vigilancia-24062020>. Acesso em: 10 abr. 2022.

KRUH, Louis; DEAVOURS, Cipher – ***The Commercial Enigma: Beginnings of machine cryptography***. Vol. XXVI, nº 1 – Cryptologia, 2022. Disponível em: <https://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/KruhDeavours.pdf>. Acesso em: 10 abr. 2022.

LANDAU, Susan – ***Listening In: Cybersecurity in an Insecure Age.*** Michigan: Grand Rapids, 2017.

LATOUR, Bruno – ***Reagregando o social: uma introdução à Teoria do Ator-Rede***. Tradução Gilson César Cardoso de Sousa. Salvador: EDUFBA – EDUSC, 2012.

LEONARDI, Paul M.; TREEM, Jeffrey W.; JACKSON, Michele H. ***The Connectivity Paradox: Using Technology to Both Decrease and Increase Perceptions of Distance in Distributed Work Arrangements***. Journal of Applied Communication Research, [*S. l.*], v. 38, p.85-105, 1 fev. 2010. Disponível em: <https://www.researchgate.net/publication/228296495_The_Connectivity_Paradox_Using_Technology_to_Both_Decrease_and_Increase_Perceptions_of_Distance_in_Distributed_Work_Arrangements>. Acesso em: 10 abr. 2022.

LEVY, Steven. ***Battle of the Clipper Chip***. June 12, 1994, Section 6, Page 46. Disponível em: <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>. Acesso em: 10 abr. 2022.

LIGUORI FILHO, Carlos Augusto – ***Criptografia em debate: modelos regulatórios ao redor do mundo***, *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

LOW entropy browsing history for content quasi-personalization. Depositante: Google LLC. US 11194866 B2. Depósito: 8 ago. 2019. Concessão: 7 dez. 2021.

MACASKILL, Ewen. ***NSA paid millions to cover Prism compliance costs for tech companies.*** The Guardian, [S.l.], p. 1-1, 23 ago. 2013. Disponível em: <https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid>. Acesso em: 8 mar. 2022.

MACASKILL, Ewen; DANCE, Gabriel. ***NSA FILES: DECODED: What the revelations mean for you***. The Guardian, [*S. l.*], p. 1-1, 1 nov. 2013. Disponível em: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>. Acesso em: 10 abr. 2022.

MACHADO, Diego e DONEDA, Danilo – ***Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no Direito Brasileir***o. Revista de direito civil contemporâneo, v. 7, n. 23, p. 95-140, abr./jun. 2020. Revista dos Tribunais, 2020. Disponível em: <https://dspace.mj.gov.br/handle/1/3317>. Acesso em: 10 abr. 2022.

MACHADO, Diego e DONEDA, Danilo – ***Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização***

de dados, *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

MAGRANI, Eduardo J. G., e ABRAHÃO, Luiz – ***Internet das Coisas Anônimas (AnIoT): Considerações Preliminares***, *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

MANSON, Katrina. ***NSA Says "No Backdoor" for Spies in New US Encryption Scheme***. BLOOMBERG, [*S. l.*], p. 1-1, 13 maio 2022. Disponível em: <https://www.bloomberg.com/news/articles/2022-05-13/nsa-says-no-backdoor-in-new-encryption-scheme-for-us-tech>. Acesso em: 10 abr. 2022.

MARTINS, Guilherme Magalhães; Longhi, João Victor Rozatti; Faleiros Junior, José Luiz de Moura (coordenaodres) – ***Comentários à Lei Geral de Proteção de Dados: LEI 13.709/2018.*** São Paulo: Editora Foco, 2022.

MCWHORTER, Dan. ***APT1: Exposing One of China's Cyber Espionage Units***. MANDIANT, [*S. l.*], p. 1-1, 25 nov. 2021. Disponível em: <https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units>. Acesso em: 10 abr. 2022.

MEDON, Filipe – ***A criptografia na Era dos Bloqueios do WhatsApp – análise segundo a metodologia constitucional***, *in*: Anais do VI Congresso do Instituto Brasileiro de Direito Civil, 2019. Disponível em: <https://www.academia.edu/38974981/>. Acesso em: 10 abr. 2022.

MERCADO ESPIÃO – Espionagem (***PODEROSO COLETOR PORTÁTIL DE IMSI / IMEI / TMSI COM INTERCEPTAÇÃO CELULAR***). Disponível em: <https://mercadoespiao.com.br/poderoso-coletor-portatil-de-imsi-imei-tmsi-com-interceptacao-celular.html>. Acesso em: 10 abr. 2022.

METAHAVEN. ***Black Transparency: The Right to Know in the Age of Mass Surveillance***, Editora: Sternberg Press, 2014.

METAHAVEN. ***Captives of the Cloud, Part III: All Tomorrow's Clouds***, in: ARANDA, Julieta; WOOD, Brian Kuan; VIDOKLE, Anton. ***The Internet Does Not Exist***. E-journal: Sternberg Press, 2015.

MILLER, A. Ray – ***The Cryptographic Mathematics of Enigma.*** Center for Cryptologic History National Security Agency Revised edition, 2019. Disponível em: <https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/CryptoMathEnigma_Miller.pdf>. Acesso em: 10 abr. 2022.

MORAES, Maria Celina Bodin de. ***LGPD: um novo regime de responsabilização civil dito proativo***. Editorial. Civilística.com, a. 8. n. 3. 2019.

MULHOLLAND, Caitlin - ***Responsabilidade civil por danos causados pela violação de dados sensíveis e a lei geral de proteção de dados pessoais***. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). Responsabilidade civil e novas tecnologias. Indaiatuba: Foco, 2020.

MULHOLLAND, Caitlin (org.) – ***A LGPD e o novo marco normativo no Brasil.*** Porto Alegre: Arquipélago, 2020.

MULHOLLAND, Caitlin et. al. ***RESPONSABILIDADE civil na LGPD***. - Produção: Comissão de Proteção de Dados e Privacidade da OABRJ. Roteiro: Debate sobre a responsabilidade civil na Lei Geral de Proteção de Dados. Gravação de youtube. 2021. Disponível em: <https://www.youtube.com/watch?v=obJEro6QjRA>. Acesso em: 17 mar. 2022.

NATIONAL INSITUTE OF STANDARDS AND TECHNOLOGY, U.S. Department of Commerce, ***About NIST***. January 11, 2022. Disponível em: <https://www.nist.gov/about-nist>. Acesso em: 10 abr. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. Department of Commerce – ***Cryptographic Standards and Guidelines Development Process Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology***. 2014. Disponível em: <https://www.nist.gov/system/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf>. Acesso em: 10 abr. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. U.S. Department of Commerce, ***Cryptographic Standards Statement***. September 10, 2013. Disponível em <https://www.nist.gov/news-events/news/2013/09/cryptographic-standards-statement>. Acesso em: 10 abr. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. U.S. Department of Commerce, ***Glossary. Backdoor***. 2022. Disponível em: <https://csrc.nist.gov/glossary/term/backdoor>. Acesso em: 10 abr. 2022.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE – ***Signals Intelligence (SIGINT) Overview.*** Disponível em: <https://www.nsa.gov/Signals-Intelligence/Overview/>. Acesso em: 10 abr. 2022.

New UFEI Rootkit. ***Schneier on Security***, [*S. l.*], p. 1-1, 28 jul. 2022. Disponível em: <https://www.schneier.com/>. Acesso em: 29 jul. 2022.

NIETZSCHE, Friedrich Wilhelm – ***A gaia ciência***. São Paulo, Campanhia das letras, 2012.

NSA – ***IC OFF THE RECORD – Truth is coming, and it cannot be stopped***. Disponível em: <https://nsa.gov1.info/dni/prism.html>. Acesso em: 10 abr. 2022.

NSA/CSS - ***Second Venona Release – Chief Office Policy***, 1995. Disponível em: <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/venona/declass_materials/doc-14.pdf>. Acesso em: 10 abr. 2022.

NSA/CSS – ***Venona***. Disponível em: <https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/smdsort14707/title/>. Acesso em: 10 abr. 2022.

PASQUALE, Frank – ***The Black Box Society: the secret algorithms that control money and information.*** Havard University Press, 2015.

PATENT PUBLIC SEARCH, in: ***USPTO - United States Patent and Trademark Office***. Disponível em: <https://ppubs.uspto.gov/pubwebapp/static/pages/landing.html>. Acesso em: 10 abr. 2022.

PERLINGIERI, Pietro – ***O Direito Civil na Legalidade Constitucional.*** 1ª ed., Editora: Renovar, 2008.

PERLROTH, Nicole; LARSON, Jeff; SHANE, Scott. ***N.S.A. Able to Foil Basic Safeguards of Privacy on Web***. The New York Times, [*S. l.*], p. 1-1, 5 set. 2013. Disponível em: <https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>. Acesso em: 10 abr. 2022.

PFEFFERKORN, Riana – ***O debate americano sobre vigilância e criptografia***, Mesa 5, in: Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital. By InternetLab em parceria com a Faculdade de Direito da Universidade de São Paulo. 2017. Disponível em: <https://www.youtube.com/watch?v=NuszpDZ69qw>. Acesso em: 10 abr. 2022.

PIMENTA, Guilherme. ***Apenas 8% dos casos de insider tranding vão ao judiciário***. AMEC, [*S. l.*], p. 1-1, 12 abr. 2017. Disponível em: <https://amecbrasil.org.br/noticia-publicada-pelo-portal-jota-apenas-8-dos-casos-de-insider-trading-vao-ao-judiciario/>. Acesso em: 26 jan. 2022.

POSSETI, Helton. ***Denúncias podem fazer Brasil ampliar exigências de produtos***. Revista EXAME, [*S. l.*], p. 1-1, 12 jul. 2013. Disponível em: <https://exame.com/tecnologia/denuncias-podem-fazer-brasil-ampliar-exigencias-de-produtos/>. Acesso em: 10 abr. 2022.

PRESIDENTIAL LIBRARY AND MUSEUM – JOHN F. KENNEDY. ***The President and the press: address before the american newspaper publishers association***, april 27, 1961. Disponível em: <https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-newspaper-publishers-association-19610427>. Acesso em: 10 abr. 2022.

PRESTO, Christian – ***Illegal Insider Trading.*** (2017). La Salle University. Economic Crime Forensics Capstones. 2017. Disponível em: <https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1022&context=ecf_capstones>. Acesso em: 10 abr. 2022.

PUBLIC LAW 100-235. ***Computer Security Act of 1987***. Disponível em: <https://www.congress.gov/100/statute/STATUTE-101/STATUTE-101-Pg1724.pdf>. Acesso em 20 abr. 2022.

PUBLIC LAW 107-56. ***US Patriot Act***. Disponível em: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acesso em: 18 dez. 2020.

QUEIROZ, Rafael Mafei Rabelo – ***Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de troca de mensagens***, *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

RAMIREZ, Luis***. London's Spy Industry Thrives in Private Sector.*** VOA NEWS, [*S. l.*], p. 1-1, 10 fev. 2017. Disponível em: <https://www.voanews.com/a/london-spy-industry-private-sector/3718445.html>. Acesso em: 10 abr. 2022.

RANDHAWA, Sukhwinder – ***Open Source Software and Libraries***. 2018. Disponível em: <https://www.researchgate.net/profile/Sukhwinder-Randhawa/publication/28810296_Open_Source_Software_and_Libraries/links/5acaebf3aca272abdc625901/Open-Source-Software-and-Libraries.pdf. Acesso em: 10 abr. 2022.

REDUCED resolution location determination for improved anonymity of user location. Depositante: Apple Inc. US 10743178 B2. Depósito: 28 set. 2018. Concessão: 11 ago. 2020.

RID, Thomas – ***Active measures: the secret history of disinformation and political warfare.*** New York: Farrar, Straus and Giroux, 2020.

RILEY, Jenn - ***Understanding metadata what is metadata, and what is it for?***. NISO Primer, National Information Standards Organization, 2017. Disponível em: <https://groups.niso.org/higherlogic/ws/public/download/17446/Understanding%20Metadata.pdf>. Acesso em: 10 abr. 2022.

RIVEST, Ronald L. - ***Chaffing and Winnowing: Confidentiality without Encryption***. MIT Laboratory for Computer Science – Technology Square Cambridge. Cryptobytes, 1998. Disponível em: <https://people.csail.mit.edu/rivest/pubs/Riv98a.pdf>. Acesso em: 10 abr. 2022.

RODOTÀ, Stefano – ***A vida na sociedade da vigilância: a privacidade hoje.*** Org. Maria Celina Bodin Moraes, Tradução Danilo Doneda w Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano – ***La vida y las reglas. Entre el Derecho y el no Derecho***. trad. Andrea Greppi, Trotta, Madrid, 2010.

SALVADOR, J. P. et al. - ***Criptografia e Direito: uma perspectiva comparada***, *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

SANDLE, Paul. ***Huawei willing to sign "no-spy" pacts with governments: chairman***. REUTERS, LONDON, 14 maio 2019. BANKS, p. 1-1. Disponível em: <https://www.reuters.com/article/us-huawei-security-britain-chairman-idUSKCN1SK1HL>. Acesso em: 10 abr. 2022.

SANGER, David; BARBOZA, David; PERLROTH, Nicole. ***Chinese Army Unit Is Seen as Tied to Hacking Against U.S***. The New York Times, [*S. l.*], p. 1-1, 18 fev. 2013. Disponível em: <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>. Acesso em: 10 abr. 2022.

SATARIANO, Adam. ***Google is buying Mandiant, a cybersecurity firm, for $5.4 billion: The deal is intended to help Google differentiate its cloud business from that of its rivals Amazon and Microsoft***. The New York Times, [*S. l.*], p. 1-1, 8 mar. 2022. Disponível em: <https://www.nytimes.com/2022/03/08/business/google-mandiant-cybersecurity.html>. Acesso em: 10 abr. 2022.

SCHNEIER, Bruce. ***Data and Goliath***. London: W.W. Norton & Company, 2015.

SCHULZ, Wolfgang e HOBOKEN, Joris van - ***Human rights and encryption***. UNESCO - Paris 07 SP, France, 2016. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000246527?1=null&queryId=e05fdd78-68b9-4ff3-b7ce-b998b0c0cf01>. Acesso em: 10 abr. 2022.

SMITH, Michael - ***Private Intelligence Companies, How the Spooks Moved in on Big Business.*** Disponível em:

<https://web.archive.org/web/20090205143528/http://michaelsmithwriter.com/pdf/intelligence_companies.pdf>. Acesso em: 10 abr. 2022.

SNOWDEN, Edward J. – ***Eterna Vigilância.*** Tradução Sandra Dolinsky. São Paulo: Planeta do Brasil, 2019.

SOLOVE, Daniel J. – ***Understanding Privacy.*** Havard University Press, 2009.

SOUZA, Carlos Affonso e MANGETH, Ana Lara – ***A criptografia entre Flexibilização e Bloqueio de Aplicações: lições internacionais e a experiência brasileira,*** *in*: DONEDA, Danilo e MACHADO, Diego. - *A Criptografia no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

STAROBIN, Paul. ***Private Espionage Is Booming: The US Needs a Spy Registry***. WIRED, [*S. l.*], p. 1-1, 17 jul. 2021. Disponível em: <https://www.wired.com/story/the-murky-merits-of-a-private-spy-registry/>. Acesso em: 13 jan. 2022.

STJ TEM CONDENAÇÃO INÉDITA POR INSIDER TRADING. **VBSO ADVOGADOS**, [*S. l.*], 14 mar. 2016. Equipe de Mercado de Capitais - VBSO Advogados, p. 1-1. Disponível em: <https://www.vbso.com.br/stj-tem-condenacao-inedita-por-insider-trading/>. Acesso em: 24 fev. 2022.

STRAUSS, Leo. - ***Reflexões sobre Maquiavel***. Tradução e apresentação à edição brasileira Élcio Verçosa. 1ª.ed. São Paulo: É Realizações 2015.

SYSTEM and method for detecting trading opportunities in financial markets. Depositante: Codestreet, LLC. US 10743178 B2. Depósito: 3 jul. 2007. Concessão: 27 jul. 2010.

TECNOLOGIA DE DUPLA UTILIZAÇÃO. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2022. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Tecnologia_de_dupla_utiliza%C3%A7%C3%A3o&oldid=63671246>. Acesso em: 10 abr. 2022.

TEODORO, Plínio. Darkmatter: ***Software espião negociado pelo Gabinete do Ódio é usado por ditaduras***. Revista Forum, [*S. l.*], 18 jan. 2022. Política, p. 1-1. Disponível em: <https://revistaforum.com.br/politica/governo-

bolsonaro/2022/1/18/darkmatter-software-espio-negociado-pelo-gabinete-do-odio-usado-por-ditaduras-108884.html>. Acesso em: 17 mar. 2022.

TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de; MENDES, Vanessa Correia; LINS, Ana Paola de Castro e – (coordenadores) - ***Anais do VI Congresso do Instituto Brasileiro de Direito Civil.*** Belo Horizonte: Fórum, 2019.

THE INTERCEPT – ***Is NSA Going Deaf? What is 'Golf Cart Reporting'?*** - An Interview With REDACTED, on Oct. 19, 2055, in: The Intercept, Mar. 1, 2018. Disponível em: <https://theintercept.com/snowden-sidtoday/4389809-is-nsa-going-deaf-what-is-golf-cart-reporting-an/>. Acesso em: 10 abr. 2022.

The NSA'S Cryptographic Capabilities. **Schneier on Security**, [*S. l.*], p. 1-1, 6 set. 2013. Disponível em: <https://www.schneier.com/blog/archives/2013/09/the_nsas_crypto_1.html>. Acesso em: 28 jul. 2022.

TIBBETTS, Jake. **- *Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers*.** Center for Global Security Research LAWRENCE LIVERMORE NATIONAL LABORATORY. September 20, 2019. Disponível em: <https://cgsr.llnl.gov/content/assets/docs/QuantumComputingandCryptography-20190920.pdf. Acesso em: 10 abr. 2022.

TRADEWEB Markets LLC Acquires CodeStreet LLC. **Tradeweb**, [*S. l.*], 2 mar. 2016. Workflows/Technology, p. 1-1. Disponível em: <https://www.tradeweb.com/newsroom/media-center/news-releases/tradeweb-markets-llc-acquires-codestreet-llc/>. Acesso em: 31 mar. 2022.

TRUSTWAVE – SPIDERLABS BLOG - ***The Golden Tax Department and the Emergence of GoldenSpy Malware***. June 25, 2020, Brian Hussey. Disponível em: <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/>. Acesso em: 10 abr. 2022.

TZU, Sun – ***A arte da guerra.*** Tradução Neury Lima. São Paulo: Hunter Books, 2011.

U.S. DEPARTAMENT Of STATE – ***U.S. Support for Connectivity and Cybersecurity in Ukraine***. May 10, 2022. Disponível em: <https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/>. Acesso em: 10 abr. 2022.

US Cloud Act. ***Clarifying Lawful Overseas Use of Data Act***. Disponível em: < https://www.justsecurity.org/wp-content/uploads/2018/02/Cloud-Act.pdf>. Acesso em: 18 dez. 2021.

VÉLIZ, Carissa – ***Privacidade é poder: por que e como você deveria retomar o controle de seus dados.*** São Paulo: Editora Contracorrente, 2021.

VERSTEIN, Andrew – ***Crypto Assets and Insider Trading Law's Domain***. 105 Iowa L.Rev 1, 2019. Disponível em: <https://ilr.law.uiowa.edu/print/volume-105-issue-1/crypto-assets-and-insider-trading-laws-domain/>. Acesso em: 10 abr. 2022.

VILANOVA, Felipe Jung – **Uma ferramenta *Peer-to-Peer* para gerenciamento cooperativo de Redes. Porto Alegre: Programa de Pós-Graduação em Computação**, Universidade Federal do Rio Grande do Sul 2006. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/8496/000577921.pdf?sequence=1>. Acesso em: 10 abr. 2022.

WASHINGTON, D.C. - FISACOURT OPINION EWITH EXEMPTIONS. disponível em: <https://pt.scribd.com/document/162016974/fisa-court-opinion-with-exemptions>. Acesso em: 10 abr. 2022.

Wassenaar Arragement Secretariat Vienna, Austria. Disponível em: <https://www.wassenaar.org/>. Acesso em: 10 abr. 2022.

WEINREB, Lloyd L. – ***A Razão Jurídica: o uso da analogia no argumento jurídico.*** São Paulo: WMF Martins Fontes, 2008.

WESTIN, Alan – ***Privacy and Freedom***. New York: Ig Publishing, 1967.

WHATSAPP. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2022. Disponível em: <https://pt.wikipedia.org/w/index.php?title=WhatsApp&oldid=63902777>. Acesso em: 10 abr. 2022.

WILSON, Duane C. – ***Cybersecurity.*** Cambridge, Massachusets: The MIT Press, 2021.

WINSTEIN'S, Keith – ***Lexical Steganography Through Adaptive Modulation of the Word Choice Hash***. *MIT*, 1998. Disponível em: <http://web.mit.edu/keithw/tlex/lsteg.pdf>. Acesso em: 10 abr. 2022.

WU, Tim – ***Império da Comunicação: do telefone à internet, da AT&T ao Google***. Tradução Claudio Carina. Rio de Janeiro: Zahar, 2012.

ZHANG, K.A., VEERAMACHANENI, K. - ***Enhancing Image Steganalysis with Adversarially Generated Examples.*** *In:* DOLEY, S., HENDLER, D., LODHA, S., YUNG, M. (eds) ***Cyber Security Cryptography and Machine Learning***. CSCML, 2019. Lecture Notes in Computer Science, vol 11527, 2019. Disponível em: <https://doi.org/10.1007/978-3-030-20951-3_15>. Acesso em: 10 abr. 2022.

ZUBOFF, Shoshana – ***Big Other: surveillance capitalismo and the prospects of na information civilization***. Journal of Information Technology, v.30, 2015.