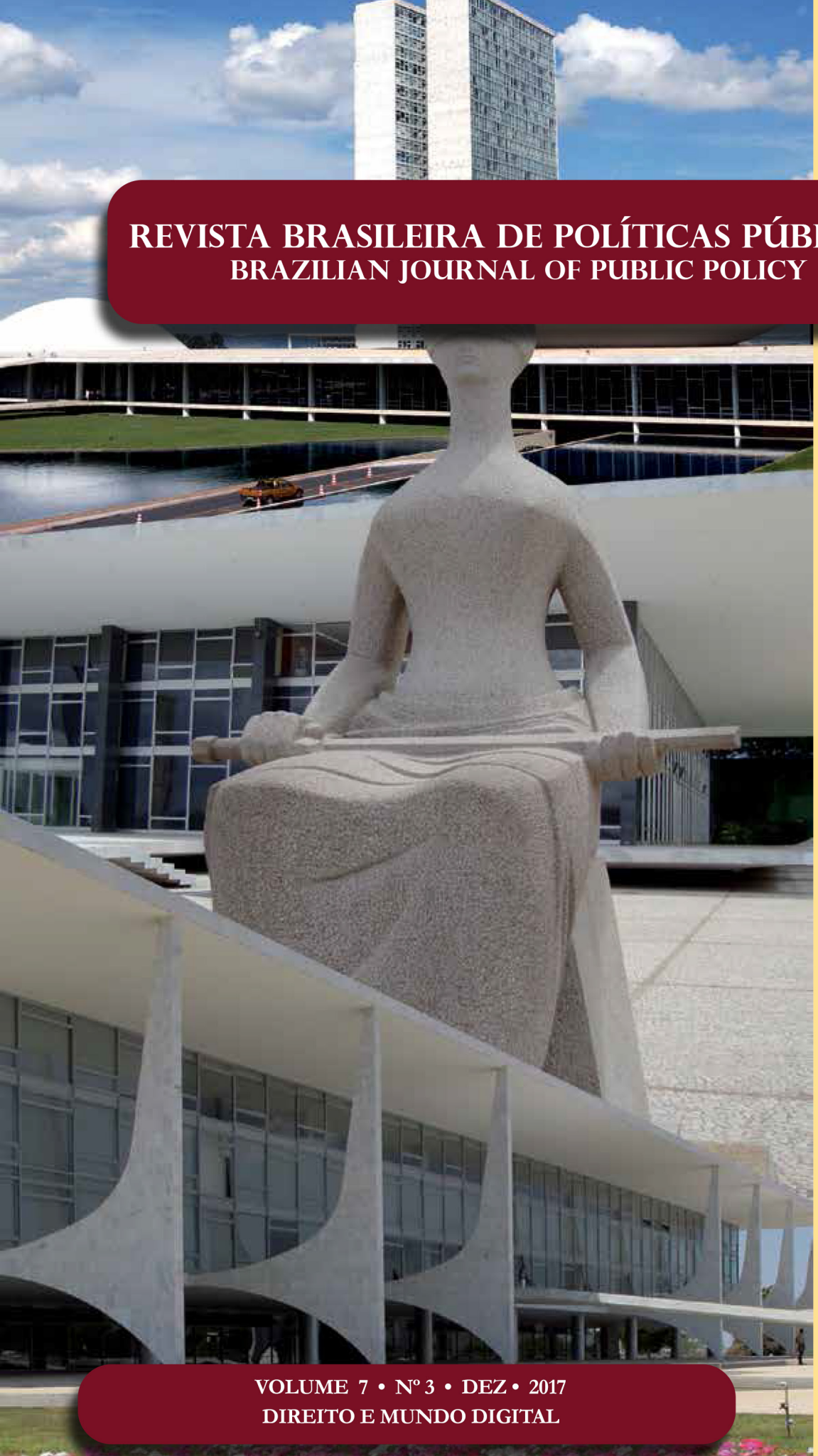

UniCEUB
ISSN 2236-1677

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS
BRAZILIAN JOURNAL OF PUBLIC POLICY

Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação

Past, present, and future of strong encryption: technological development and regulation

Jacqueline de Souza Abreu

VOLUME 7 • Nº 3 • DEZ • 2017
DIREITO E MUNDO DIGITAL

Sumário

I. Introdução I

The Datasphere and the Law: New Space, New Territories III
Jean-Sylvestre Bergé e Stéphane Grumbach

II. Dossiê Especial: Direito e Mundo Digital 22

A. Criptomoedas e tecnologia blockchain 23

Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação 25
Jacqueline de Souza Abreu

Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro 44
Mariana Dionísio de Andrade

Território das criptomoedas: limites à regulamentação estatal quanto à circulação de moedas no ciberespaço e possíveis alternativas 61
Ranidson Gleyck Amâncio Souza

Criptomoedas e competência tributária 80
Guilherme Broto Follador

Bitcoin e a (im)possibilidade de sua proibição: uma violação à soberania do Estado? 106
Rodrigo Valente Giublin Teixeira e Felipe Rangel da Silva

Blockchain e Agenda 2030 122
Danielle Mendes Thame Denny, Roberto Ferreira Paulo e Douglas de Castro

A reconstrução da jurisdição pelo espaço digital: redes sociais, blockchain e criptomoedas como propulsores da mudança 143
Maria Edelvacy Pinto Marinho e Gustavo Ferreira Ribeiro

B. Proteção de dados e provedores de Internet 158

O tempo e o espaço. Fragmentos do marco civil da internet: paradigmas de proteção da dignidade humana 160
Maria Celeste Cordeiro Leite dos Santos e Marilene Araujo

O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos **185**
Elias Jacob de Menezes Neto, Jose Luis Bolzan de Morais e Tiago José de Souza Lima Bezerra

Dignidade humana na webesfera governamental brasileira **200**
Luciana Cristina Souza

Ciberespaço e conteúdo ofensivo gerado por terceiros: a proteção dos direitos de personalidade e a responsabilização civil dos provedores de aplicação, à luz da jurisprudência do Superior Tribunal de Justiça **217**
Cristiano Colombo e Eugênio Facchini Neto

A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu **239**
Thatiane Cristina Fontão Pires

Rafael Peteffi da Silva

Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro **256**
Fernando Büscher von Teschenhausen Eberlin

The dichotomy between smart metering and the protection of consumer's personal data in Brazilian Law **275**
Lucas Noura Guimarães

O cyberbullying e os limites da liberdade de expressão **295**
Janile Lima Viana, Cinthia Meneses Maia e Paulo Germano Barrozo de Albuquerque

O Supremo Tribunal Federal e o discurso de ódio nas redes sociais: exercício de direito versus limites à liberdade de expressão **314**
Carlo José Napolitano e Tatiana Stroppa

Análise comparada de estratégias de enfrentamento a "revenge porn" pelo mundo **334**
Natália Neris, Juliana Pacetta Ruiz e Mariana Giorgetti Valente

Uso indevido de redes sociais e aplicativos de mensagens instantâneas no ambiente laboral **349**
Eloy Pereira Lemos Junior, Edmar Warlisson de Souza Alves e César Augusto de Castro Fiuza

C. Direito ao esquecimento 366

Ensaio sobre a promessa jurídica do esquecimento: uma análise a partir da perspectiva do poder simbólico de Bourdieu 368
Joana Machado e Sergio Negri

Uma agenda para o direito ao esquecimento no Brasil..... 384
Bruno de Lima Acioli e Marcos Augusto de Albuquerque Ehrhardt Júnior

Não adianta nem tentar esquecer: um estudo sobre o direito ao esquecimento..... 412
José Augusto Fontoura Costa e Geraldo Miniuci

A aplicação do direito ao esquecimento aos agentes delitivos: uma análise acerca da ponderação entre o direito à imagem e as liberdades de expressão e de informação437
Paulo Afonso Cavichioli Carmona e Flávia Nunes de Carvalho Cavichioli Carmona

Direito ao esquecimento: na sociedade informacional há espaço para o epílogo da máquina de tortura kafkiana? 454
Alexandre Antonio Bruno da Silva e Marlea Nobre da Costa Maciel

Esquecimento, internet e "preferência" da informação: possibilidades de aplicação da doutrina dos preferred rights da jurisprudência norte-americana ao caso brasileiro 484
Maria Vital da Rocha, Isaac Rodrigues Cunha e Karin de Fátima Rodrigues Oliveira

D. Propriedade intelectual 510

Direitos autorais e música: tecnologia, direito e regulação 512
Marcia Carla Pereira Ribeiro, Cinthia Obladen de Almendra Freitas e Rubia Carneiro Neves

Direito autoral na cibercultura: uma análise do acesso aos bens imateriais a partir das licenças creative commons 4.0..... 539
Gabriela Maia Rebouças e Fernanda Oliveira Santos

E. Políticas públicas e novas tecnologias..... 559

Salto digital nas políticas públicas: oportunidades e desafios..... 561
Marcelo D. Varella, Clarice G. Oliveira e Frederico Moesch

Fostering e-government in Brazil: a case study of digital certification adoption.585
Lamartine Vieira Braga

Democratização na era digital: desafios para um diálogo consciente e igualitário.602
Raquel Cavalcanti Ramos Machado e Laura Nathalie Hernandez Rivera

Redes sociais e crowdsourcing constitucional: a influência da ciberdemocracia sobre a gênese e a interpretação de normas constitucionais 618
Igor Ajouz

Marco civil da internet e política pública de transparência: uma análise da e-democracia e do compliance público 634
Juliana Costa Zaganelli e Wallace Vieira de Miranda

Políticas públicas brasileiras de computação em nuvem: análise documental dos relatórios do global cloud computing scorecard 648
Lucas dos Santos Costa e Marcos Fernando Machado de Medeiros

O uso monopolista do Big Data por empresas de aplicativos: políticas públicas para um desenvolvimento sustentável em cidades inteligentes em um cenário de economia criativa e de livre concorrência 672
José Antonio Remedio e Marcelo Rodrigues da Silva

1. Introdução 673

2. A urbanização das cidades e a sociedade em rede: economia criativa, colaborativa e compartilhada como formas de concretização de funções sociais da cidade 674

4. Concorrência e Big Data Business relevantes às Smart Cities: estudo de caso envolvendo a aquisição do Waze pelo Google 686

5. Considerações finais 689

Referências 690

III. Outros temas 694

Como salvar o sistema de repercussão geral: transparência, eficiência e realismo na escolha do que o Supremo Tribunal Federal vai julgar 696
Luís Roberto Barroso e Frederico Montedonio Rego

Precariedade do sistema penitenciário brasileiro como base temática para a proibição ou legalização das drogas 715
Lilian Rose Lemos Rocha e José Eduardo Cardozo

A terceira margem do constitucionalismo republicano: uma crítica a Frank Michelman 732
Daniel Barcelos Vargas

Medida provisória e controle de constitucionalidade: relevância, urgência e pertinência temática 749
Clarice G. Oliveira e José Levi Mello do Amaral Júnior

Objeto e conceito do direito administrativo: revisão crítica **765**
Carlos Bastide Horbach

Avaliação de políticas públicas versus avaliação de impacto legislativo: uma visão dicotômica de um fenômeno singular **782**
Aparecida de Moura Andrade e Héctor Valverde Santana

Los avatares del interés definido en términos de poder en la formulación de las políticas públicas **800**
Louis Valentin Mballa

Consequencialismo judicial na modulação de efeitos das decisões declaratórias de inconstitucionalidade nos julgamentos de direito tributário **819**
Fernando Leal e Daniela Gueiros Dias

Judicialização da saúde: a dignidade da pessoa humana e a atuação do Supremo Tribunal Federal no caso dos medicamentos de alto custo **845**
Fabricio Veiga Costa, Ivan Dias da Motta e Dalvaney Aparecida de Araújo

doi: 10.5102/rbpp.v7i3.4869

Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação*

Past, present, and future of strong encryption: technological development and regulation

Jacqueline de Souza Abreu**

Resumo

Os episódios recentes de bloqueio do WhatsApp no Brasil e de confronto entre Apple e FBI nos Estados Unidos retratam um cenário de embate entre Estados-nações e empresas que usam, em seus produtos e serviços, tecnologias de "criptografia *forte*" — do tipo que não oferece um mecanismo de acesso nem quando o devido processo legal foi observado. A partir de análise da literatura especializada, este artigo investiga como se chegou a esse ponto e quais as questões regulatórias em jogo. Primeiramente, mapeia o histórico das chamadas "guerras de criptografia" nos Estados Unidos e no Brasil. A seguir, analisa se e quando existe um dever jurídico aplicável a empresas de construir sistemas de comunicação e armazenamento de dados que sejam passíveis de realizar quebras de sigilo sempre que seguido o devido processo legal. Por fim, discute questões de política pública em pauta nos debates sobre criptografia forte: os potenciais efeitos para segurança pública e a proposta de "acesso excepcional". O artigo conclui que, no quadro jurídico em vigor, não é evidente a existência de dever jurídico de ter habilidade de quebrar sigilo para empresas de tecnologia e internet e que, no atual estado da técnica, o balanço de riscos, custos e benefícios da criptografia forte recomenda a preservação incólume dessa tecnologia.

Palavras-chave: Criptografia. Whatsapp. Apple. Privacidade. Segurança.

Abstract

Recent episodes of WhatsApp blocking in Brazil and the standoff between Apple and the FBI in the United States portray a scenario of clash between nation-states and private companies that use "*strong* encryption" – encryption that does not provide a mechanism for law enforcement access even when due legal process was observed. Based on an analysis of the specialized literature, this article shows how it came to this point and what regulatory issues are at stake. First, it maps the history of the so-called "crypto wars" in the United States and in Brazil. Next, it analyzes if and when there is a legal duty applicable to private entities to build communication and data storage systems that are susceptible to breaches of confidentiality, whenever

* Recebido em 27/10/2017
Aprovado em 09/12/2017

** Doutoranda em Direito na Universidade de São Paulo. Mestra em Direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais. Coordenadora da área "Privacidade e Vigilância" no InternetLab, centro independente de pesquisa em direito e tecnologia. Email: jacqueline.abreu@usp.br

due process is followed. Finally, it discusses policy issues at the heart of the debates on strong encryption: the potential effects on public safety and the 'exceptional access' proposal. The article presents two conclusions. First, that the putative legal duty applicable to technology and internet companies of having the ability to breach secrecy is not evident in the current legal framework. Second, that, in the current state of the art, the balance of risks, costs and benefits of strong encryption recommend the unimpeded preservation of this technology.

Keywords: Encryption. Whatsapp. Apple. Privacy. Security. Brazil.

1. Introdução

O aplicativo de mensagens instantâneas WhatsApp foi alvo de quatro decisões de bloqueio no Brasil, três delas que foram levadas a cabo, por não entregar conteúdo de comunicações de investigados em inquéritos e processos penais.[1] Desde o momento em que implementou a chamada "criptografia de ponta a ponta"[2], a empresa responsável pelo aplicativo tem reiterado a impossibilidade técnica de cumprir ordens judiciais de interceptação.[3] Diante disso, o então Ministro da Justiça Alexandre de Moraes declarou intenções[4] de trazer um projeto de lei que regularia aplicativos de mensagens que utilizam criptografia e o Supremo Tribunal Federal convocou audiência pública[5] para entender as complexidades técnicas dessa tecnologia.

No plano internacional, em 2015, a Apple desafiou judicialmente um pedido de acesso a informações contidas em um iPhone com "criptografia completa de disco"[6] feito pelo *Federal Bureau of Investigations* (FBI) no âmbito de investigações de atentado terrorista em San Bernardino, na Califórnia.[7] Basicamente, o FBI buscava a determinação judicial de que a Apple desenvolvesse uma nova versão do software do iPhone que fosse capaz de burlar medidas de segurança que a própria Apple criou para impedir o acesso não autorizado ao iPhone, o qual automaticamente encripta as informações nele armazenadas quando está no modo de repouso (bloqueado por senha). O FBI acabou abrindo mão desse pedido depois que conseguiu desbloquear o iPhone através de uma "solução" comprada de um terceiro.[8]

Esses dois episódios recentes, nacional e internacional, retratam um cenário de embate entre Estados-nações e empresas que implementam tecnologias de "criptografia *forte*" — o adjetivo decorre do fato de que

1 Tais ordens de bloqueio, e as respectivas decisões de suspensão do bloqueio, podem ser consultadas na plataforma <http://bloqueios.info>.

2 Tipo de criptografia que converte mensagens (texto, voz e vídeo) em dados cifrados, de tal modo que apenas os participantes da comunicação (as 'pontas') podem decifrá-las. Nenhum terceiro — nem mesmo o criador do software (no caso, WhatsApp) — é capaz de fazer a transformação de texto cifrado para texto legível.

3 Há um conflito acerca dos limites da jurisdição brasileira sobre o aplicativo, para além questão da criptografia, apesar de esse não ser o foco deste trabalho. Ver ABREU, Jacqueline de Souza. From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp. *Columbia Journal of Transnational Law Online Edition*, 17 out. 2016. Disponível em: <http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/>. Acesso em: 28 set. 2017.

4 PASSARINHO, Nathalia. Governo elabora projeto para regular acesso a informações do WhatsApp. *G1*, 19 jul. 2016. Disponível em: <http://g1.globo.com/politica/noticia/2016/07/governo-elabora-projeto-para-regular-acesso-informacoes-do-whatsapp.html>. Acesso em: 28 set. 2017.

5 SUPREMO TRIBUNAL FEDERAL. Ministro Fachin convoca audiência pública para discutir bloqueios judiciais do WhatsApp. *Notícias STF*, Brasília, 3 nov. 2016. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=328600&caixaBusca=N>. Acesso em: 28 set. 2017.

6 Tipo de criptografia que converte todas as informações armazenadas em um aparelho em texto cifrado; a transformação que só pode ser revertida se inserida a chave correta (no caso, senha do usuário de desbloqueio do celular, desconhecido pela Apple, criadora do software).

7 COOK, Tim. A Message to Our Customers. *Apple*, 16 fev. 2016. Disponível em: <https://www.apple.com/customer-letter/>. Acesso em: 28 set. 2017.

8 BANNER, Katie; LICHTBLAU, Eric. U.S. Says It Has Unlocked iPhone Without Apple. *New York Times*, 28 mar. 2016. Disponível em: <https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?mcubz=3>. Acesso em: 27 set. 2017.

não oferece um mecanismo de acesso nem quando o devido processo legal foi observado. Trata-se de um conflito entre poderes tradicionais do Estado, de investigar e punir por meio do processo penal, e os crescentes poderes informacionais, de criar e facilitar espaços de comunicação e exercício de liberdades, de grandes corporações.[9] Diante disso, colocam-se as seguintes indagações: como se chegou a este ponto? Quais as questões regulatórias em jogo? A partir de análise da literatura especializada, este artigo faz uma investigação dessas questões. Primeiro, mapeia o histórico das chamadas "guerras de criptografia" nos Estados Unidos e no Brasil (Parte 2). A seguir, com base na apresentação do quadro jurídico em vigor nesses países, analisa se existe um dever jurídico aplicável a empresas de construir sistemas de comunicação e armazenamento de dados que sejam passíveis de quebras de sigilo, sempre que seguido o devido processo legal (Parte 3). Por fim, discute o impacto da criptografia forte na segurança pública e a proposta de 'acesso excepcional' como estratégia regulatória (Parte 4).

Estudos sobre criptografia fora das faculdades de matemática, ciência da computação e engenharia são ainda incipientes no Brasil. Há pouca produção acadêmica sobre tratamento e implicações jurídicas dessa tecnologia fora de temas como certificação digital, por exemplo.[10] Isso significa que os embates de autoridades com grandes empresas que implementam a tecnologia da criptografia forte em seus serviços ainda não foram objeto de estudo aprofundado no Brasil; apesar de ter sido tema de alguns artigos jornalísticos e textos de opinião[11]. Este artigo pretende contribuir para o preenchimento dessa lacuna na literatura jurídica acadêmica nacional. Ao mesmo tempo, o leitor não deve esperar uma explicação aprofundada sobre o funcionamento técnico da criptografia. Apresentam-se noções básicas se e quando forem relevantes para o debate de direito e política pública, uma vez que o público desse texto é a comunidade jurídica.

2. Passado: o histórico das 'crypto wars'

A criptografia foi criada para proteger informações sensíveis do acesso não autorizado de terceiros, isto é, de pessoas que não são o remetente nem o destinatário dessas informações e dados.[12] No jargão da segurança da informação, ela se presta não somente a assegurar a *confidencialidade* de conteúdo de mensagens, dados e informações, mas também a *integridade* (contra alterações do conteúdo) e *autenticidade* (das partes). Trata-se de uma tecnologia que remonta à Antiguidade, quando já era utilizada na transmissão de mensagens que precisavam ser asseguradas da descoberta de inimigos.[13] Nos tipos mais simples de criptografia, rearranjava-se o alfabeto e quem tinha conhecimento da ordem de reorganização do alfabeto — a "chave" — era capaz de decodificar o conteúdo da mensagem. Quem quisesse "quebrar" a criptografia, isto é, decifrar a

9 Sobre políticas de informação, a atuação do e o impacto no Estado, ver BRAMAN, Sandra. *Change of State:* Information, Policy, and Power. Cambridge: The MIT Press, 2007. p. 24-27. Agradeço ao Avaliador B por esta indicação de bibliografia.

10 Tocam o tema MARCACINI, Augusto. *Direito e Informática:* uma abordagem jurídica sobre a criptografia. São Paulo: edição eletrônica, 2010; e SILVA, Alexandre Assunção e. *Sigilo das Comunicações na Internet*. Curitiba: Juruá, 2017, mas não tratam do debate na perspectiva tomada aqui.

11 Por exemplo, FERRAZ JUNIOR, Tercio Sampaio; MARANHÃO, Juliano; FINGER, Marcelo. O desafio do WhatsApp ao Leviatã. *Folha de S. Paulo*, São Paulo, 16 ago. 2016. Opinião. Disponível em: <http://www1.folha.uol.com.br/opiniao/2016/08/1803323-o-desafio-do-whatsapp-ao-leviata.shtml>; ANTONIALLI, Dennys et al. Especial: o que dizem especialistas em criptografia sobre bloqueio do WhatsApp. *Deu nos Autos*, 21 jul. 2016. Disponível em: <http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/>. Acesso em: 27 set. 2017; DONEDA, Danilo. A regulação da criptografia e o bloqueio do WhatsApp. *Consultor Jurídico*, 30 maio 2017. Disponível em: <https://www.conjur.com.br/2017-mai-30/danilo-doneda-regulacao-criptografia-bloqueio-whatsapp>; LIMA, Caio César Carvalho. Criptografia e (ou?) interceptação das comunicações. *Jota*, 31 maio 2017. Disponível em <https://jota.info/colunas/direito-digital/criptografia-e-ou-interceptacao-das-comunicacoes-31052017>. Acesso em: 27 set. 2017.

12 SINGH, Simon. *The Code Book:* The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 1999. p. xiii.

13 SINGH, Simon. *The Code Book:* The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 1999. p. 3-14; MARCACINI, Augusto. *Direito e Informática:* uma abordagem jurídica sobre a criptografia. São Paulo: edição eletrônica, 2010. p. 19.

mensagem ou descobrir a lógica da encriptação, teria de analisar padrões de repetição de letras, conforme a frequência delas na mensagem e compará-los com a frequência em palavras de uma certa língua.

A essência da criptografia hoje ainda é a mesma, com a diferença de que é muito mais complexa. Como resultado do avanço da tecnologia computacional, técnicas de criptografia foram sofisticadas: hoje o alfabeto não é simplesmente reordenado, mas fórmulas complexas de matemática — algoritmos — são aplicadas para cifrar mensagens. Já quem se engaja na tarefa rival de "quebrar" criptografia (*criptoanálise*) hoje também não consegue fazê-lo apenas "humanamente", simplesmente observando padrões de repetição de letras: depende-se igualmente de "supercomputadores". Em outras palavras, praticamente não é possível desenvolver códigos e sistemas seguros ou quebrar criptografia sem um conhecimento avançado em matemática, um enorme poder computacional e um enorme orçamento.

Não é à toa que a pesquisa científica sobre criptografia se deu por muito tempo por financiamento de Estados, dentro de entidades estatais, como órgãos militares e serviços secretos.[14] Esses órgãos tinham tanto os incentivos quanto os recursos necessários para isso. Afinal, criptografia é uma técnica crucial para *proteger* informações sensíveis. Assim, quando o Estado quer garantir a privacidade e a segurança de suas próprias comunicações e dados, a implementação de técnicas de criptografia é imprescindível. Por outro lado, quando um Estado quer *produzir* informações sobre outros Estados ou indivíduos (os "inimigos"), em operações de contrainteligência, por exemplo, precisam tentar quebrar a criptografia utilizada por eles.

Esse cenário expõe a tensão que mora no seio da relação de Estados com a criptografia: Estados usam criptografia; mas não celebram o fato de que outros — principalmente inimigos — também a usem. Como em outros lugares no mundo, essa tensão veio à tona no Brasil. Subjacente aos casos de bloqueio do WhatsApp, encontra-se o descontentamento de autoridades estatais com a impossibilidade técnica de interceptação em tempo real de conversas de suspeitos investigados, em razão da criptografia utilizada pela empresa. Entretanto, o Estado brasileiro endossa e emprega a criptografia para uso próprio, isto é, para proteger suas próprias comunicações e dados. Após as revelações de Edward Snowden em 2013, por exemplo, quando foi revelado que a *National Security Agency* (NSA) havia influenciado o órgão de padronização de sistemas criptográficos americano (*National Institute of Standards and Technology* – NIST), o governo brasileiro mudou o padrão criptográfico de certificação digital que era o americano para um alemão numa medida evidente de reação contra à vigilância estrangeira.[15] A Agência Brasileira de Inteligência também desenvolveu sistemas próprios de criptografia para proteger as comunicações do governo, diante das alegações de que a própria presidência da República vinha sendo objeto de vigilância da NSA.[16]

Essa tensão histórica hoje vai além das disputas geopolíticas entre Estados. Quando a criptografia de chave pública foi desenvolvida ao final dos anos 1970 por pesquisadores da Universidade de Stanford nos Estados Unidos,[17] um método que o jornal O Estado de São Paulo chamou de "técnica contra ouvintes clandestinos"[18], a NSA tentou abafar o desenvolvimento de pesquisa acadêmica na área, e, principalmente,

14 LEVY, Steven. *Crypto:* how the code rebels beat the government saving privacy in the digital age. New York: Penguin Books, 2001. p. 13-36 (sobre como a *National Security Agency* estadunidense desenvolvia secretamente criptografia); LEVY, Steven. *Crypto:* how the code rebels beat the government saving privacy in the digital age. New York: Penguin Books, 2001. p. 313-330 (sobre o papel da *Government Communication Headquarters* inglesa no avanço de padrões criptográficos).

15 GROSSMANN, Luís Osvaldo. Brasil abandona padrão de criptografia maculado pela NSA. *Convergência Digital*, 27 maio 2014. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=36860>. Acesso em: 25 set. 2017.

16 Ver PARAGUASSU, Lisandra. Abin cria sistema de criptografia para proteger dados do governo. *O Estado de São Paulo*, São Paulo, 7 set. 2013. Disponível em: <http://politica.estadao.com.br/noticias/geral,abin-cria-sistemas-de-criptografia-para-proteger-dados-do-governo,1072368>. Acesso: 25 set. 2017; MATAIS, Andreza; MORAES, Marcelo de. Temer recebe telefone criptografado projetado pela ABIN. *O Estado de São Paulo*, São Paulo, 22 maio 2017. Disponível em: <http://politica.estadao.com.br/blogs/coluna-do-estadao/temer-recebe-telefone-criptografado-projetado-pela-abin/>. Acesso: 25 set. 2017.

17 Trabalho seminal foi DIFFIE, Whitfield; HELLMAN, Martin. New directions in cryptography. *IEEE transactions on Information Theory*, v. 22, n. 6, p. 644-654, 1976. Disponível em: <https://www-ee.stanford.edu/~hellman/publications/24.pdf>. Acesso: 25 set. 2017.

18 O ESTADO DE SÃO PAULO. Nova técnica contra ouvintes clandestinos, p. 25, 5 jul. 1978.

impedir que produtos que adotassem esse modelo de criptografia fossem amplamente comercializados.[19] A preocupação da agência consistia, fundamentalmente, na perda do "monopólio tecnológico" que tinha sobre a criptografia e na emergência de forças independentes que dominassem o uso dessa técnica, tornando a possibilidade de se proteger informações e dados sensíveis de maneira segura contra terceiros disponível para o grande público — não somente Estados-inimigos, mas grupos terroristas e criminosos.[20]

Autoridades estatais estadunidenses lutaram bravamente. Dois episódios — ou batalhas — sintetizam os anos marcados pelas primeiras "guerras de criptografia" (*crypto wars*) entre os setores público e privado naquele país. Primeiro, a utilização de leis de exportação contra empresas que queriam implementar criptografia forte em seus produtos. Considerada, desde o pós II Guerra Mundial, como munição militar pelo Departamento de Estado, responsável pela lista de itens submetidos às *International Traffic in Arms Regulations21* e ao *Arms Export Control Act22,* a criptografia estava sujeita a procedimentos estritos de obtenção de licença para exportação.[23] Esse regime apenas se afrouxou, ao longo dos anos 1990, com pressão da indústria temendo danos à competitividade de produtos estadunidenses no mercado global, e com as demonstrações de ineficácia da restrição na era da Internet[24] e de derrota no Judiciário.[25]

O segundo episódio marcante consistiu na proposta do *Escrowed Encryption Standard* como novo padrão nacional de algoritmo criptográfico. Encampada pelo Governo Clinton em 1993, a iniciativa propunha que produtos incorporassem o "Clipper chip", dispositivo que criptografava comunicações, mas guardava uma cópia das chaves em depósito (*in escrow*) juntamente a um "terceiro confiado", para que agentes de investigação pudessem decifrar as informações buscadas quando amparados por ordem judicial autorizadora.[26] Em outras palavras, tratava-se de um protocolo de criptografia que continha um *backdoor* (porta dos fundos) para autoridades. A proposta encontrou objeções juntamente à indústria (preocupada com a concorrência internacional), aos especialistas em segurança da informação (convencidos das fragilidades do esquema)[27], e membros da sociedade civil organizada (aflitos com as ameaças às liberdades civis). Foi abandonada.

Ao fim da década de 1990, as guerras de criptografia se enfraqueceram nos EUA, com claros vencedores. Os avanços consolidados da pesquisa acadêmica sobre o assunto e o emprego de criptografia em diversos produtos no comércio são evidência de que o poder público efetivamente perdeu seu monopólio tecnológi-

19 LEVY, Steven. *Crypto:* how the code rebels beat the government saving privacy in the digital age. New York: Penguin Books, 2001. p. 114-124 (sobre pesquisa) e LEVY, Steven. *Crypto:* how the code rebels beat the government saving privacy in the digital age. New York: Penguin Books, 2001. p. 125-155 (sobre comércio).

20 Nota-se na tentativa de barrar a disseminação desse conhecimento a manifestação dos Estados Unidos como "Estado informacional", na forma de Estado que controla informações para exercício de poder. Ver BRAMAN, Sandra. *Change of State:* Information, Policy, and Power. Cambridge: The MIT Press, 2007. p. 34;244-245.

21 ESTADOS UNIDOS DA AMÉRICA. 22 C.F.R. §§ 120-130.

22 ESTADOS UNIDOS DA AMÉRICA. *22 U.S.C. §§ 2751-2799aa-2*. Disponível em: <https://www.law.cornell.edu/uscode/text/22/chapter-39:>. Acesso em: 10 set. 2017

23 RICE, Eric. The Second Amendment and the Struggle Over Cryptography. *Hastings Science and Technology Law Journal*, v. 9, p. 32-37, 2017; MARCACINI, Augusto. *Direito e Informática:* uma abordagem jurídica sobre a criptografia. São Paulo: edição eletrônica, 2010. p. 22.

24 Em 1991, Paul Zimmerman, que desenvolveu o programa de encriptação de mensagens Pretty Good Privacy (PGP) postou seu software na Internet, desafiando as restrições de exportação, já que agora poderia ser baixado em outros lugares do mundo. Ver RICE, Eric. The Second Amendment and the Struggle Over Cryptography. *Hastings Science and Technology Law Journal*, v. 9, p. 31, 2017; MARCACINI, Augusto. *Direito e Informática: uma abordagem jurídica sobre a criptografia*. São Paulo: edição eletrônica, 2010, pp. 23-25.

25 Em 1996, Daniel Bernstein, que desenvolveu um novo protocolo criptográfico, processou o Departamento de Estado, argumentando que incluir criptografia no regime de controle de exportações de munições militares era inconstitucional pois violaria a Primeira Emenda. A District Court de Northern California acolheu o pedido e declarou que códigos de criptografia eram discursos protegidos pela Constituição. Ver ESTADOS UNIDOS AMÉRICA. District Court de Northern California. *Bernstein v. U.S. Dept. of State*, 9 dez. 1996, 945 F. Supp. 1279; RICE, Eric. The Second Amendment and the Struggle Over Cryptography. *Hastings Science and Technology Law Journal*, v. 9, p. 36, 2017.

26 LEVY, Steven. *Crypto:* how the code rebels beat the government saving privacy in the digital age. New York: Penguin Books, 2001. p. 226-268.

27 ABELSON, Hal et al. The risks of key recovery, key escrow, and trusted third-party encryption. *Columbia University Academic Commons*, 1997. Disponível em: <http://academiccommons.columbia.edu/catalog/ac:127127>. Acesso em: 23 out. 2017.

co. Com uma derrota tão contundente naquele momento, a pergunta que se coloca é o que levou aos mais novos episódios de guerra entre poderes público e privado sobre criptografia, isto é, aos episódios com que se abriu esse artigo: os bloqueios do WhatsApp no Brasil e o caso Apple vs. FBI nos Estados Unidos. A resposta é: a disseminação do uso de criptografia para proteção de comunicações para o público em massa.

Para entender a mudança crucial, é preciso lembrar que o uso da criptografia nasceu da e se difundiu pela necessidade de confidencialidade, integridade e autenticidade de informações e comunicações *sensíveis* (como a localização de tropas em uma guerra, números de cartão de crédito numa transação pela internet e denúncias em regimes autoritários), o que a relegou por muito tempo a usos por atores específicos em situações em que a quebra de sigilo de comunicações é vinculada a grandes riscos. Em outras circunstâncias, a disseminação dessa tecnologia entre cidadãos comuns sempre esbarrou na falta de conhecimento sobre a existência dessa tecnologia, na necessidade de escolha consciente de se empregar tal técnica, e na dificuldade de implementação correta pelo público leigo em segurança da informação. Evidência disso é como o software de criptografia *Pretty Good Privacy*, apesar de disponibilizado ao público gratuitamente na internet em 1991, se mantém relativamente restrito a pessoas e grupos que buscam privacidade, principalmente para proteção de comunicações de alto risco.[28]

O cenário já não é mais esse, entretanto. Em setembro de 2014, a empresa de tecnologia mais valiosa do mundo — Apple Inc. — passa a aplicar criptografia como configuração padrão do sistema operacional de um dos celulares mais vendidos do mundo (iOS 8 para iPhones), no caso dos Estados Unidos, com 90,1 milhões de usuários;[29] e , em abril de 2016, a empresa por trás do aplicativo de mensagens mais popular do mundo — WhatsApp — implementa um tipo de criptografia a ser empregado por mais de um bilhão de pessoas no mundo, e, no caso do Brasil, por 92% dos usuários de *smartphones*,[30] essa última fronteira que separava a criptografia do público em massa foi em grande parte superada.[31] Diante disso, reacenderam os alertas de entidades estatais. Se o desenvolvimento independente de criptografia (fora das entidades estatais) já havia levado a oportunidade de acesso à criptografia ao público em geral, ela se limitou por muito tempo a aplicações específicas e a usuários (inclusive criminosos) sofisticados. Essas novas iniciativas de empresas levam a criptografia, finalmente, para as massas — inclusive aos criminosos mais comuns.

Esse quadro chama atenção para o fato de que o tipo de criptografia empregado em um serviço é uma opção da própria empresa. Para entender esse ponto, é importante voltar por um instante ao funcionamento de sistemas de criptografia. Para que as partes envolvidas em uma *comunicação* à distância possam se comunicar de forma segura é, em geral, necessário que tenham previamente "combinado" uma chave que decifre as mensagens que querem trocar; como esse processo de estabelecer uma chave é por vezes inconveniente e inseguro, muitos sistemas modernos de criptografia operam automaticamente a troca de chaves sem que as partes nem se deem conta.[32] Por sua vez, para que uma pessoa possa *armazenar* dados de forma segura em algum aparelho, é necessário que crie uma chave secreta que apenas ela saiba; o sistema de criptografia então combinará essa chave com outra chave única do próprio aparelho, junção a partir da qual ocorre processos de cifragem e decifragem.

Além de operar troca de chaves e processos de cifragem e decifragem, muitas empresas mantêm, também, uma cópia delas, guardando para si o poder de decifrar as mensagens. [33] A grande discussão desen-

28 Ver também MARCACINI, Augusto. *Direito e Informática:* uma abordagem jurídica sobre a criptografia. São Paulo: edição eletrônica, 2010. p. 26 (afirmando haver certo exagero no lema de "massificação" da PGP).

29 STATISTA. *Number of iPhone users in the United States from 2012-2016*. 2017. Disponível em: <https://www.statista.com/statistics/232790/forecast-of-apple-users-in-the-us/>. Acesso em: 28 set. 2017.

30 DATAFOLHA. *Hábitos de uso de aplicativos*: população brasileira – 13 anos ou mais, dez. 2016. Disponível em: <http://media.folha.uol.com.br/datafolha/2017/01/27/da39a3ee5e6b4b0d3255bfef95601890afd80709.pdf>. Acesso em: 10 out. 2017.

31 Nesse sentido, ver PFEFFERKORN, Riana. *Apple vs. FBI*: Where did it come from? What Is It? Where Is It Going? Palestra realizada na Universidade da Califórnia, Berkeley, 7 mar. 2016. p. 5-6. Disponível em: <https://cyberlaw.stanford.edu/files/blogs/Riana%20BIPLA%20talk%203-7-16.pdf>. Acesso em: 10 out. 2017.

32 ROZENSHTEIN, Alan Z. Surveillance Intermediaries. *Stanford Law Review*, v. 70, p. 29, 2018. Disponível em: <https://ssrn.com/abstract=2935321>. Acesso em: 10 out. 2017.

33 Segundo Alan Rozenshtein, a razão principal por que algumas empresas de internet assim o fazem é econômica: seu modelo

cadeada hoje se dá em torno da "criptografia de ponta-a-ponta" e da "criptografia completa de disco", implementadas pelo WhatsApp no aplicativo de mesmo nome e pela Apple nos novos iPhones, em que o software desenvolvido pelas empresas se encarrega da troca de chaves, mas não as retêm. Isso significa que essas empresas não são capazes de decifrar mensagens e dados; é impossível tecnicamente — a criptografia é por isso *forte*. Há algumas razões por que fariam isso: (i) o consenso público de que esse modelo é mais seguro do que outros métodos; (ii) a demonstração de boa fé ao público em geral e de compromisso com privacidade, trazendo vantagens comerciais; (iii) os ganhos do argumento da "impossibilidade técnica" de cooperar com autoridades, desobrigando empresas dos custos de atender, responder e contestar pedidos de interceptação e quebras de sigilo.[34]

Diante dessas escolhas, colocam-se questões sobre o que o direito do país em questão proíbe ou autoriza que essas empresas façam em termos de utilização de criptografia forte, bem como sobre riscos e benefícios de modelos regulatórios que pretendam interferir nessa técnica. Nas próximas duas seções, organizo os argumentos que aparecem nessas discussões.

3. Presente: o quadro normativo

No Brasil, estatísticas oficiais do Conselho Nacional de Justiça apontam que, só em 2015, juízes criminais brasileiros expediram 100.568 ofícios de interceptação telefônica e telemática.[35] A maior empresa do setor de telecomunicações no país diz ter recebido muito mais que isso: segundo o relatório de transparência da Telefónica (Vivo), 326.811 pedidos de interceptação foram dirigidos à empresa.[36] Esses números reforçam uma impressão sobre autoridades envolvidas em investigações: o disseminado uso (e, possivelmente, dependência) de medidas de quebra de sigilo de comunicações.

Nesse contexto, a emergência de empresas que escolhem construir seus sistemas de forma tão segura que impossibilita substancialmente sua cooperação com autoridades estatais é vista como ameaça a seus poderes de investigação.

> A disponibilidade de escutas — legais ou não — por mais de uma vida nos deu gerações de policiais que não podem imaginar um mundo sem elas. Confrontados com a sugestão de perder essa ferramenta, eles respondem do mesmo modo que seria de esperar um médico moderno confrontado com a perspectiva de retornar a um mundo sem ressonância magnética, tomografia computadorizada, painéis sanguíneos e os inúmeros outros testes diagnósticos que caracterizam a medicina moderna.[37]

Do ponto de vista do direito em vigor, empresas privadas possuem a faculdade de construir sistemas de criptografia que impossibilitam, tecnicamente, a colaboração com autoridades investigativas na realização de interceptações em tempo real e quebras de sigilo de dados armazenados? Ou elas estão proibidas pelo direito (do país em questão)? É para essas questões que esta seção olha.

---

de negócio se baseia na análise de dados de usuários para oferecimento de publicidade direcionada. É o caso de Google e Facebook, por exemplo. Por essa mesma razão, tais empresas são capazes de atender a pedidos de interceptação e quebras de sigilo. ROZENSHTEIN, Alan Z. Surveillance Intermediaries. *Stanford Law Review*, v. 70, p. 27, 2018. Disponível em: <https://ssrn.com/abstract=2935321>. Acesso em: 10 out. 2017. No caso de empresas de tecnologia como a Apple, é mais difícil dizer onde restaria o interesse econômico em reter o acesso.

34 ROZENSHTEIN, Alan Z. Surveillance Intermediaries. *Stanford Law Review*, v. 70, p. 29, 2018. Disponível em: <https://ssrn.com/abstract=2935321>. Acesso em: 10 out. 2017.

35 Ver CONSELHO NACIONAL DE JUSTIÇA. *Sistema Nacional de Controle de Interceptações*. Disponível em: <http://www.cnj.jus.br/interceptacoes_tel/relatorio_quantitativos.php>. Acesso em: 15 out. 2017. Estatísticas dos totais 2 e 8.

36 TELEFÓNICA. Informe de Transparencia en las Comunicaciones. 2016. p. 11. Disponível em: <https://www.telefonica.com/documents/364672/127737347/Telefonica_Transparencia_ESP_interactivo_22B.pdf/e39832d1-0622-4d1b-bbfd-510af449de86>. Acesso em: 15 out. 2017.

37 DIFFIE, Whitfield; LANDAU; Susan. *Privacy on the Line:* The Politics of Wiretapping and Encryption. Cambridge: The MIT Press, 2007. p. 7. (tradução livre)

3.1. O caso (fácil) das empresas de telecomunicações

A Lei das Interceptações[38], aprovada em 1996, preencheu de sentido referência que existe no texto da Constituição Federal brasileira de 1988: "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," diz o art. 5º, inciso XII (grifo adicionado). Nela estão, portanto, regulamentadas as condições e circunstâncias que tornam a realização de monitoramento em tempo real de comunicações admissível no direito brasileiro. Estabeleceu-se o *procedimento* para tal.

O próprio texto da lei também já antecipou o papel fundamental que certas empresas provedoras de serviços de comunicação à distância teriam na assistência para realização de interceptações: diz o art. 7 que "Para os procedimentos de interceptação de que trata essa Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público". A expressão "concessionárias de serviço público" revela o que estava na mente do legislador: empresas que oferecem serviços de telefonia e, que pouco tempo depois, passaram também a ofertar conexão à Internet — ou seja, aquelas que compõem o *setor de telecomunicações*.

Altamente reguladas, tais empresas estão sob a supervisão da Agência Nacional de Telecomunicações (ANATEL) e devem obedecer às suas resoluções. Entre elas, estão as Resoluções nº 73/1998 (Regulamento dos Serviços de Telecomunicações), nº 426/2005 (Regulamento do Serviço Telefônico Fixo Comutado), nº 477/2007 (Regulamento do Serviço Móvel Pessoal) e nº 614/2013 (Regulamento do Serviço de Comunicação Multimídia) que, entre muitas obrigações, determinam que prestadoras mantenham disponíveis recursos tecnológicos e facilidades necessárias para a suspensão de sigilo das telecomunicações determinada por autoridade judiciária ou legalmente investida desses poderes, com algumas pequenas variações de linguagem.[39] As *prestadoras de telecomunicações* estão sob a obrigação, portanto, de construir seus sistemas de forma que as comunicações à distância facilitadas por elas sejam "grampeáveis". Elas devem possuir tal *habilidade*.

O quadro regulatório nos Estados Unidos guarda semelhanças. Não há direito ao sigilo das comunicações previsto na Constituição dos Estados Unidos — a Quarta Emenda apenas estabelece um direito contra buscas e apreensões arbitrárias —, sendo esse direito resguardado, explicitamente, apenas em leis. No nível infraconstitucional, o *Wiretap Act*[40] e o *Pen Register Act*[41] estabelecem as hipóteses e a forma como podem ocorrer interceptações em tempo real de *conteúdo* e de *metadados*[42] de comunicações no país, respectivamente;

38 BRASIL. *Lei n. 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: out. 2017.

39 Art. 26, parágrafo único do Regulamento dos Serviços de Telecomunicações: "A Prestadora tornará disponíveis os recursos tecnológicos necessários à suspensão de sigilo de telecomunicações determinada por autoridade judiciária ou legalmente investida desses poderes e manterá controle permanente de todos os casos, acompanhando a efetivação dessas determinações e zelando para que elas sejam cumpridas dentro dos estritos limites autorizados". Art. 24 do Regulamento de Serviço Telefônico Fixo Comutado e art. 90 Regulamento do Serviço Móvel Pessoal: "A prestadora deve tornar disponíveis os recursos tecnológicos e facilidades necessários à suspensão de sigilo de telecomunicações, determinada por autoridade judiciária ou legalmente investida desses poderes, e manter controle permanente de todos os casos, acompanhando a efetivação dessas determinações, e zelando para que elas sejam cumpridas, dentro dos estritos limites autorizados". Art. 52, parágrafo único, do Regulamento do Serviço de Comunicação Multimídia: "A Prestadora deve tornar disponíveis os dados referentes à suspensão de sigilo de telecomunicações às autoridades que, na forma da lei, tenham competência para requisitar essas informações".

40 ESTADOS UNIDOS DA AMÉRICA. *18 U.S.C. §§ 2510-2522*. Disponível em: <https://www.law.cornell.edu/uscode/text/18/2511>. Acesso em: 15 set. 2017.

41 ESTADOS UNIDOS DA AMÉRICA. *18 U.S.C. §§ 3121-3121*. Disponível em: <https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206>. Acesso em: 15 set. 2017.

42 Metadados são, a rigor, "dados sobre dados". Aqui, diz respeito a registros gerados sobre uma comunicação: data, hora, identificadores (da linha, da conexão, do aparelho), origem, destino e duração de uma comunicação, por exemplo.

o *Stored Communications Act43* regula pedidos que quebras de sigilo de dados armazenados.[44] Por outro lado, o *Communications Assistance for Law Enforcement Act45* (CALEA) requer que provedores de telecomunicações sejam capazes de isolar e interceptar comunicações e fornecê-las a autoridades, observado o devido processo legal.[46]

3.2. O caso (difícil) das empresas de tecnologia e de internet

Esse cenário regulatório das telecomunicações ajuda a explicar por que as autoridades brasileiras e americanas se acostumaram ao longo dos anos a terem a capacidade e o poder de realizarem interceptações e quebras de sigilo de comunicações de pessoas investigadas com o auxílio do setor privado. O costume, fundado em lei, de poder contar com empresas de telecomunicações na condução de vigilância gerou uma certa expectativa que se traduz hoje na postulação de que essa prerrogativa também se estende a *empresas de tecnologia* (como a Apple) e *aplicações de internet* (como o WhatsApp). Observado o devido processo legal que até hoje foi o suficiente para conseguir a cooperação de empresas de telecomunicações, autoridades esperam que o mesmo ocorra com esses novos grandes atores.

No caso brasileiro, isso aparece em manifestações de autoridades que alegam que a impossibilidade técnica de o WhatsApp atender a ordens judiciais de interceptação de mensagens contrariaria a legislação brasileira.[47] Eis o que afirma a juíza Daniela Souza, envolvida no último bloqueio do aplicativo, por exemplo:

> Qualquer empresa que se instale no País fornecendo determinado serviço, deverá estar apta a cumprir as decisões judiciais que, porventura, recaiam sobre esta, sob pena de cancelamento do próprio serviço, […]. A falta ou a negativa de informação por parte da empresa, deixando de atender a uma determinação judicial, impede aos órgãos de persecução de apurarem os ilícitos e alcançarem os autores dos crimes praticados, constituindo-se a recusa no fornecimento dos dados mera estratégia da empresa a fim de procrastinar e até descumprir a ordem judicial, sob o pálio de impossibilidades técnicas.[48]

O problema é que não é tão evidente assim que a impossibilidade técnica de realizar interceptações em tempo real no WhatsApp, criada pelo uso de criptografia de ponta a ponta, contrarie a legislação brasileira. Na verdade, raciocínios como o da magistrada parecem querer extrair da própria previsão legal no direito brasileiro de *procedimentos de quebra de sigilo* o dever de que a *habilidade de quebra de sigilo* sempre exista.[49] Esse salto, entretanto, não é simples quando estamos falando de empresas de internet — e não mais de prestadoras de telecomunicações.

Por um lado, permanece o texto da Constituição Federal sobre o direito ao sigilo das comunicações ("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

43 ESTADOS UNIDOS DA AMÉRICA. *18 U.S.C. §§ 2701-2711*. Disponível em: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>. Acesso em: 15 set. 2017.

44 SOLOVE, Daniel; SCHWARTZ, Paul. *Information Privacy Law*. 4. ed. New York: Wolters Kluver, 2015. p. 353;358-359.

45 ESTADOS UNIDOS DA AMÉRICA. *47 U.S.C. §§ 1000-1010*. Disponível em: <https://www.law.cornell.edu/uscode/text/47/chapter-9/subchapter-I>. Acesso em: 15 set. 2017.

46 SOLOVE, Daniel; SCHWARTZ, Paul. *Information Privacy Law*. 4. ed. New York: Wolters Kluver, 2015. p. 359.

47 Ver ROSA, João Luiz Moraes. Sigilo e persecução penal. *Justiça do Direito*, v. 31, n. 1, p. 138, jan./abr. 2017; BARRETO, Alesandro Gonçalves; CASELLI, Guilherme. WhatsApp: é possível cumprir decisões judiciais? *Direito & TI,* 10 abr. 2016. Disponível em: <http://direitoeti.com.br/artigos/whatsapp-e-possivel-cumprir-decisoes-judiciais/>. Acesso em: 23 out. 2017; SOBRAL, Carlos Eduardo. Por que a Justiça deve bloquear o WhatsApp. *Jota*, 4 jul. 2016. Disponível em: <https://jota.info/artigos/por-que-justica-deve-bloquear-o-whatsapp-quando-nao-ha-colaboracao-04072016>. Acesso em: 15 set. 2017.

48 BRASIL. Poder Judiciário do Rio de Janeiro. 2ª Vara Criminal de Duque de Caxias. Inquérito Policial 062-00164/2016. Juíza Daniela Barbosa Assumpção de Souza, julg. 19 jul. 2016 (determinando bloqueio do aplicativo).

49 Encontrei essa distinção em PFEFFERKORN, Riana. Apple vs. FBI: Where did it come from? What Is It? Where Is It Going? Palestra realizada na Universidade da Califórnia, Berkeley, em 7 mar. 2016 organizada pela Berkeley Information Privacy Law Association. Disponível em: https://cyberlaw.stanford.edu/files/blogs/Riana%20BIPLA%20talk%203-7-16.pdf. Acesso em: 15 set. 2017.

investigação criminal ou instrução processual penal") e a Lei das Interceptações, cuja aplicação se estende à "interceptação do fluxo de comunicações em sistemas de informática e telemática" (art. 1, parágrafo único). Os textos dos art. 7, II e III[50] e do art. 10, §2º[51] do Marco Civil da Internet[52], lei aplicável a *aplicações de internet* como o WhatsApp, também são claros em prever que o conteúdo de comunicações eletrônicas pode ser disponibilizado (apenas) mediante ordem judicial. É inegável, portanto, que exista em lei um *procedimento* regulando a disponibilização de conteúdo de conversas e dados.

Por outro, como empresas de internet não são 'concessionárias de serviço público' e estão fora do escopo da ANATEL, não recaem sobre elas as expressas exigências técnicas de suas resoluções. O Marco Civil da Internet também não institui, explicitamente, a obrigação de que aplicações de internet tenham *habilidade* de quebrar sigilo.[53] Quando obriga que empresas retenham informações, o dever se estende apenas a *registros* (IP, data e hora de acesso), o que as obriga a, necessariamente, ser capazes de atender a pedidos de quebra de sigilo apenas desses metadados (art. 15).[54] Portanto, o dever jurídico, extraído do direito brasileiro vigente, de que aplicações de internet sejam capazes de quebrar sigilo de conteúdo de comunicações não é evidente; carece de fundamentação — e pode muito bem ser que a conclusão seja de que não exista.

Essa fundamentação teria de necessariamente enfrentar também o próprio art. 5, inciso XII da Constituição Federal. O texto revela o compromisso de se garantir certo nível de proteção de privacidade a comunicações à distância, sobre o qual é recorrente a interpretação jurisprudencial de que protegeria a inviolabilidade do *fluxo* de comunicações enquanto ocorrem.[55] O legislador, entretanto, teria se preocupado em admitir ao menos uma hipótese de interceptação legítima desse fluxo, para comunicações *telefônicas,* porque, ao contrário das demais — que ganham alguma dimensão física (perenidade) e podem ser objeto de busca e apreensão posteriormente —, aquelas podem se perder na oralidade se não grampeadas em tempo real.[56]

Nessa linha de raciocínio, parece forçoso admitir que comunicações eletrônicas como as do WhatsApp são muito mais semelhantes a cartas, telegrafias e, especialmente, dados (informáticos), por deixarem dimensão física de registro em celulares dos participantes das comunicações, inexistindo a imprescindibilidade de que o *fluxo* de tais comunicações deva ser grampeável.[57] Nesse contexto, também a admissão de interceptações 'telemáticas' no parágrafo único do art. 1 da Lei de Interceptações somente pode ser coerente com a Constituição se impuser, no máximo, a "grampeabilidade" de *fluxo* de *conexão à internet* — por *empresas de telecomunicações*, em geral —, uma vez que esse tipo de comunicação também não se pereniza.[58] Outra vez,

50 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;

51 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.

52 BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 15 out. 2017.

53 Mesmo o Decreto nº 8.771 de 2016, que regulamentou o Marco Civil da Internet, quando estabelece que dados pessoais, registros e comunicações privadas "deverão ser mantidos em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto", institui mais uma obrigação aplicável *caso dados sejam mantidos*.

54 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.

55 Ver, por exemplo, BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 418.416-8/SC, Min. Rel. Sepúlveda Pertence, julg. 10 mai. 2006; e BRASIL. Supremo Tribunal Federal. Habeas Corpus 91.867/SP, Min. Rel. Gilmar Mendes, julg. 24 abr. 2012.

56 Nesse sentido, paradigmaticamente, FERRAZ JUNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, p. 447, 1993.

57 Quanto ao risco de que esses vestígios se percam — sejam "deletados" por criminosos —, não há nenhuma novidade tecnológica relevante: afinal, sempre foi possível queimar evidências em papel.

58 Nesse sentido, ver BADARÓ, Gustavo Henrique Righi Ivahy. Interceptação de comunicações telefônicas e telemáticas: limites

portanto, essas breves considerações apontam que justificar a existência do dever de ser capaz de realizar interceptações em tempo real a essas aplicações de internet é bem mais complexo do que parece e, ao que foi sugerido aqui, não se sustenta.

No âmbito da Ação Direta de Inconstitucionalidade nº 5.527 e da Arguição de Descumprimento de Preceito Fundamental nº 403, originadas pelos incidentes de bloqueio do WhatsApp no Brasil, é possível que o Supremo Tribunal Federal (STF) se manifeste quanto a essas questões. Apesar de os objetos das ações se relacionarem, respectivamente, à (in-) constitucionalidade da previsão de 'suspensão temporária' e 'proibição de exercício das atividades' como sanção no Marco Civil da Internet e à (in-)compatibilidade de ordens judiciais de bloqueio do aplicativo com a liberdade de comunicação, elas estão essencialmente relacionadas à criptografia forte do WhatsApp: foi a impossibilidade técnica de se quebrar sigilo de investigados (sem alterar o atual sistema operacional do WhatsApp) que levou aos bloqueios — medidas de constrangimento e punição. Mas se não há dever jurídico de ter a habilidade de quebrar sigilo, não há qualquer base jurídica para se falar em qualquer sanção. Por isso, espera-se do STF uma análise sofisticada, tal como o tema merece.

Nos Estados Unidos, a lei é clara no sentido de que aplicações de internet não precisam ter a *habilidade* de monitorar comunicações em tempo real; tais obrigações se restringem a provedores de telecomunicações nos termos da CALEA. Lá não há dúvidas, portanto, que o direito americano permite que o WhatsApp empregue criptografia de ponta a ponta. Igualmente, não há dúvidas de que a Apple, como empresa de tecnologia, pode implementar a configuração padrão de criptografia completa de disco nos aparelhos que vende.

A questão que se colocou no caso Apple vs. FBI foi, na verdade, se autoridades judiciais podem obrigar a empresa a elaborar um software customizado — uma versão especial do iOS — que pudesse ser instalada num iPhone bloqueado por senha (e, por isso, encriptado) e que desabilitasse as configurações de segurança que frustrariam a realização, pelo FBI, de um "ataque de força bruta" que tentaria adivinhar a senha do celular (e assim desbloqueá-lo e, como consequência, decifrá-lo). Como visto anteriormente, a "senha" selecionada pelo usuário é crucial nesse modelo de criptografia; para que essa chave não seja facilmente adivinhada por terceiros, empresas criam outros elementos de segurança (por exemplo, restrições de número de tentativas e de tempo entre elas). Foi contra esse tipo de medida que o FBI se insurgiu.

O debate girou em torno de dois materiais principais.[59] Primeiramente, o *All Writs Act* (AWA), uma lei curta e geral de 1789, que instituiu uma espécie de poder geral de cautela aos juízes: "a Suprema Corte e todas as cortes estabelecidas por um ato do Congresso podem emitir ordens [*writs*] em auxílio a suas respectivas jurisdições e em concordância com os usos e princípios do direito".[60] Segundo, o precedente da Suprema Corte *United States vs. New York Telephone Co*,[61] que, aplicando o AWA, gerou a regra de que terceiros podem ser obrigados a auxiliar em investigações criminais se três requisitos forem atendidos: (i) não estejam muito afastados da matéria em questão; (ii) seu auxílio é absolutamente necessário; (iii) a assistência técnica requisitada não é excessivamente onerosa. O FBI defendia que o precedente lhes dava autoridade para fazer o pedido à Apple; a empresa, e diversos outros grupos defensores de liberdades civis e empresas de tecnologia, negava. Apesar da atenção global que o caso ganhou, ele nunca foi decidido, como antecipado na introdução — o FBI abriu mão do pedido quando conseguiu uma "solução" para o desbloqueio do celular junto a um terceiro. Se o direito americano permite que um juiz obrigue uma empresa a escrever software que facilite o acesso a informações no âmbito de investigações é a questão que ficou sem resposta dos tribunais.

ante o avanço da tecnologia. In: LIMA, José Corrêa de; CASARA, R. R. Rubens. (Coord.). *Temas para uma perspectiva crítica do direito:* homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010. p. 483-499.

59 PFEFFERKORN, Riana. *Apple vs. FBI*: Where did it come from? What Is It? Where Is It Going? Palestra realizada na Universidade da Califórnia, Berkeley, 7 mar. 2016. p. 7-8. Disponível em: <https://cyberlaw.stanford.edu/files/blogs/Riana%20BIPLA%20talk%203-7-16.pdf>. Acesso em: 23 out. 2017.

60 ESTADOS UNIDOS DA AMÉRICA. *28 U.S.C. § 1651(a)*. Disponível em: <https://www.law.cornell.edu/uscode/text/28/1651>. Acesso em: 27 set. 2017.

61 ESTADOS UNIDOS DA AMÉRICA. Supreme Court of The United States. *United States vs. New York Telephone Co*, 7 dez. 1977, 434 U.S. 159.

3.3. Escopo da Resposta

Os argumentos vistos até aqui no Brasil e nos Estados Unidos sugerem que empresas de tecnologia e de internet não estão praticando nada que seja explicitamente proibido pelo direito desses países ao implementarem criptografia forte. Se isso mudar, é em razão de nova decisão judicial ou legislação. A pergunta que segue então é: deveria mudar? A maior parte dessa discussão envolve análise de custos, riscos e benefícios de uma política regulatória da criptografia forte, os quais serão analisados na seção seguinte (parte 4). Há, entretanto, uma questão fundamental de direito constitucional que resta apontar aqui: é admissível a criação de espaços que sejam 'inalcançáveis' pelo Estado — como um iPhone bloqueado da Apple e mensagens em fluxo do WhatsApp — ou há algo nas nossas concepções de Estado de Direito e legitimidade política que requeira essa possibilidade? Apesar de crucial ao debate, responder essa pergunta extrapola o escopo desse trabalho — o qual pretendeu, apenas, até aqui, descontruir a visão que assume ser evidente o dever de ser capaz de quebrar sigilo.

Cabe, entretanto, um comentário. Essa pergunta esconde o fato de que esses espaços não são em *todas* as circunstâncias 'inalcançáveis' — é possível que a autoridades consigam obter dados armazenados em backup (iCloud, no caso do iPhone) ou acesso físico ao celular (e exigir judicialmente a divulgação da senha por parte do investigado). Além disso, não é como se nunca antes existiram outros ambientes, conversas ou dados 'inalcançáveis' por agentes de segurança — conversas face a face ou documentos queimados, por exemplo. Por outro, não é por que essa *habilidade* de tornar comunicações e dados inacessíveis ao Estado exista naturalmente no mundo analógico que ela deva, necessariamente, ser reproduzida no ambiente virtual. Se deve ser, esse é um argumento sobre direito à privacidade frente ao interesse público em segurança pública que precisaria ser construído[62] — algo que ficará para outros trabalhos.

4. Futuro: a criptografia forte deveria ser regulada?

As guerras de criptografia nunca se dão nos termos estritamente jurídicos vistos na seção anterior. Na verdade, o contexto em que se coloca a discussão sobre faculdades e deveres de empresas de tecnologia e de internet está rodeado de análises das consequências que um modelo regulatório da criptografia forte pode acarretar, isto é, sobre o impacto social de uma ação estatal — de qualquer um dos três Poderes — nessa área.[63] Quais os benefícios e custos envolvidos em permitir que empresas de tecnologia e internet desenhem aparelhos de armazenamento de dados e sistemas de comunicação de tal maneira que nem elas sejam capazes de decifrar dados e mensagens? Quais os benefícios e malefícios de proibir que elas tenham essa liberdade? Há alguma saída 'intermediária'? É para essa dimensão fundamental do debate que essa seção olha.[64]

4.1. 'Going Dark' e a necessidade de um acesso excepcional

A crítica mais emblemática às implementações de criptografia tais como do WhatsApp e da Apple é a de que autoridades de segurança pública estariam *going dark*[65], isto é, ficando no escuro, já que, cada vez menos,

62 Nesse sentido LESSIG, Lawrence. Reading the Constitution. *Cyberspace, Emory Law Journal*, v. 45, p. 881-882, 1996 ("There might have been *ability* to keep stuff hidden, since the technology to find it, and identify it, might have been limited. But *friction* doesn't convert to a right. An *argument* for this conversion is required – some reason why it makes sense"). Grifos no original.

63 A abordagem que olha para o impacto social é identificada por Sandra Braman como alternativa para avaliação de políticas de informação. Ver BRAMAN, Sandra. *Change of State:* Information, Policy, and Power. Cambridge: The MIT Press, 2007. p. 69.

64 Não há nenhuma pretensão de esgotar os argumentos do debate neste artigo; identificam-se e discutem-se os argumentos centrais ao redor de onde orbitam todos os demais.

65 COMEY, James. *Going Dark*: Are Technology, Privacy, and Public Safety in a Collision Course? Discurso proferido no Brookings Institute, 14 out. 2016. Disponível em: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-

conseguiriam coletar informações relevantes para investigações, mesmo quando observaram todo o devido processo legal (obtiveram ordem judicial baseada em suspeita razoável de prática de crime, por exemplo). Esse argumento recorre às consequências que a queda de efetividade de autoridades de investigação teria para a segurança pública: as técnicas de criptografia forte — isto é, insuperável até pelas empresas criadoras do software de criptografia — neutralizam um instrumento importante na prevenção e repressão de crimes e ataques terroristas, qual seja a "quebra de sigilo", seja de dados armazenados ou de comunicações em andamento. Como resultado, servem de escudo para terroristas, pedófilos, corruptos, traficantes e criminosos em geral.

Daí afirma-se que essa tendência precisaria ser contida. Como? Nos países estudados, é difícil encontrar quem defenda a *proibição* desse tipo de criptografia forte. Autoridades estatais reconhecem em seus discursos[66] que a criptografia é uma técnica imprescindível para um mundo cada vez mais digitalizado e crucial para a garantia de segurança contra crimes cibernéticos. Alguns admitem, inclusive, que qualquer esforço para proibir essa tecnologia seria completamente ineficaz, já que a generatividade[67] e a arquitetura global da internet permitem que aplicações de criptografia forte sejam criadas a qualquer momento, baixadas de qualquer lugar do mundo e utilizadas por qualquer agente interessado o suficiente para buscá-las; o conhecimento de técnicas de criptografia forte já não é algo que se consiga apagar da memória da humanidade e tirar das mãos de criminosos sofisticados.

Apesar disso, autoridades argumentam que é necessário devolver a capacidade de quebrar sigilo de comunicações, mesmo que, na prática, a regulação somente afete as maiores empresas do mercado (alvos mais fáceis de uma regulação efetiva) e detenha apenas criminosos comuns pouco sofisticados.[68] Esse já seria um ganho digno de se perseguir. A melhor maneira de alcança-lo seria, por meio de decisões judiciais, leis, ou negociações fechadas com empresas, pela construção e implementação de modelos de criptografia que não fossem fortes a ponto de estarem inacessíveis aos agentes de segurança, mesmo quando portando ordens judiciais; defendem sistemas de criptografia com algum tipo de "acesso excepcional", contornáveis por quem detenha alguma "chave de ouro".[69]

4.2. 'Going Bright' e os problemas de um acesso excepcional

Opositores contestam tanto a insinuação de que se está *going dark* quanto à proposta de um "acesso excepcional". Primeiramente, apesar de criptografia forte poder ser um obstáculo para alguns tipos de quebras de sigilo com os quais antes de contava, as pessoas agora guardam arquivos em servidores na nuvem, deixam inúmeros rastros por onde passam, sobre o que fizeram (online e offline) e quais seus contatos, o que faz com que muitos argumentem que, na verdade, ingressamos na "idade de ouro da vigilância" — estamos *going bright*.[70] Hoje o Estado é capaz de obter dados que simplesmente não estavam à disposição anos atrás e, com

safety-on-a-collision-course>. Acesso em: 23 out. 2017.

66 Ver, por exemplo, falas de membros do Ministério Público Federal e da Polícia Federal na Audiência Pública do Supremo Tribunal Federal YOUTUBE. *Bloqueio judicial do WhatsApp e o Marco Civil da Internet*. Disponível em: <https://youtu.be/3TNsQCNIOO>; e KAHN, Matthew. Deputy Attorney General Rod Rosenstein Remarks on Encryption. *Lawfare*, 10 out. 2017. Disponível em: https://www.lawfareblog.com/deputy-attorney-general-rod-rosenstein-remarks-encryption. Acesso em: 22 out. 2017.

67 Termo referente ao fato de que aplicações e sites podem ser criados e instantaneamente disponibilizados publicamente na internet para download e visualização em todo o mundo. Ver ZITTRAIN, Jonathan. *The Future of the Internet And How to Stop It*. New Haven: Yale University Press, 2008. p. 70.

68 Ver, por exemplo, KAHN, Matthew. Deputy Attorney General Rod Rosenstein Remarks on Encryption. *Lawfare*, 10 out. 2017. Disponível em: <https://www.lawfareblog.com/deputy-attorney-general-rod-rosenstein-remarks-encryption>. Acesso em: 23 out. 2017.

69 Ver, por exemplo, falas de membros do Ministério Público Federal e da Polícia Federal na Audiência Pública do Supremo Tribunal Federal YOUTUBE. *Bloqueio judicial do WhatsApp e o Marco Civil da Internet*. Disponível em: <https://youtu.be/3TNsQCNIOO>; e KAHN, Matthew. Deputy Attorney General Rod Rosenstein Remarks on Encryption. *Lawfare*, 10 out. 2017. Disponível em: <https://www.lawfareblog.com/deputy-attorney-general-rod-rosenstein-remarks-encryption>. Acesso em: 23 out. 2017.

70 SWIRE, Peter; AHMAD, Kenesa. Encryption and Globalization. *The Columbia Science & Technology Law Review*, v. 23, p. 466-470, 2012.

a Internet das Coisas[71], muitos outros metadados vão passar a ser gerados, e talvez esses registros já serão o suficiente para muitas investigações, de tal forma que criptografia não será um grande problema assim para o sucesso de investigações.[72]

A sugestão de que criptografia forte comprometeria a segurança pública é, também, contestada pelo fato de que o uso dessa técnica *previne* diversos crimes, ou seja, promove a segurança[73]: hackers e bisbilhoteiros em geral não conseguem interceptar — um crime em si — conversas de WhatsApp; ladrões não conseguem invadir um iPhone — também outro crime em si. Além disso, criptografia não somente impede a realização desses crimes como coíbe outros relacionados, como fraudes, furtos de identidade, e extorsões, por exemplo, crimes comumente associados à obtenção ilícita de informações pessoais. Essa dimensão preventiva é ainda mais relevante e importante quando temos em mente potenciais vítimas como ativistas, jornalistas, pessoas em situação de vulnerabilidade e até mesmo agentes de segurança. Assim, por mais que a criptografia forte possa 'proteger criminosos', ela seria fundamental para proteger *todos*.

Acerca da proposta de 'acesso excepcional', afirma-se que não é possível desenvolver uma porta de acesso que se garanta que só vai ser explorada para fins legítimos — por agentes de segurança numa investigação legítima.[74] A ideia seria a seguinte: criptografia é matemática e, como tal, suas leis e códigos aplicam-se e podem ser operados por todos. Nesse sentido, modelos de criptografia em que o desenvolvedor não só opera troca de chaves, mas também retém essas chaves – um acesso privilegiado, tecnicamente equivalente a um *backdoor* — seriam inerentemente menos seguros e mais vulneráveis, pois estariam abertos a que essas chaves sejam descobertas por terceiros mal-intencionados: se a Apple e o WhatsApp são capazes de quebrar sigilo, agentes maliciosos podem encontrar um jeito de fazer o mesmo. Diante disso, argumenta-se que esse seria um risco enorme que se deve evitar o máximo possível.[75] Sem contar que, depois das revelações de Edward Snowden sobre espionagem da NSA com ajuda de grandes empresas americanas, ficaria mais difícil acreditar que esse "acesso excepcional" não será abusado.[76]

Também se aponta que a imposição de modelos de "acesso excepcional" acarretaria outros tipos de dano. Empresas seriam obrigadas a 'adaptar' seus produtos às jurisdições em que atuam, elevando custos para atuação em mercados globais e até o desincentivo de atuar onde há regulações hostis à criptografia forte.[77] Além disso, essa opção regulatória em países democráticos como Estados Unidos e Brasil poderia gerar um perigoso precedente a ser copiado por países com menores níveis de proteção de direitos e de observância do devido processo legal — outros países vão querer o tratamento "privilegiado". Assim, agravar-se-iam os riscos de abuso.

71 Termo utilizado para se referir ao fenômeno em que objetos cotidianos – como geladeiras, TVs, postes de luz, carros e lixeiras, por exemplo – passam a estar também conectados à Internet. Faz parte desse fenômeno o universo de dados gerados por "medidores inteligentes" de energia, por exemplo, discutidos neste volume. Ver GUIMARÃES, Lucas Noura. The dichotomy between smart metering and the protection of consumer's personal data in Brazilian law. *Revista Brasileira de Políticas Públicas,* v. 7, n. 3, 2017.

72 GASSER, Urs et al. Don't Panic. *Making Progress in the 'Going Dark' Debate*: Berkman Klein Center For Internet & Society. 1 fev. 2016. Disponível em: <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>. Acesso em: 23 out. 2017.

73 Ver PFEFFERKORN, Riana. A Response to "Responsible Encryption". *Center for Internet & Society at Stanford Law School Blog*, 11 out. 2017. Disponível em: <http://cyberlaw.stanford.edu/blog/2017/10/response-"responsible-encryption">; CERDEIRA, Pablo; FERREIRA, Helena. Permitir grampo no WhatsApp coloca a sociedade em risco. *Jota*, 2 jun. 2017. Disponível em: <https://jota.info/artigos/permitir-grampo-no-whatsapp-colocar-a-sociedade-em-risco-02062017>. Acesso em: 23 out. 2017.

74 ABELSON, Hal et al. Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, v. 1, n. 1, p. 75-76, 2015.

75 Ver, além da nota acima, por exemplo, SANCHEZ, Julian. Old Technopanic in New iBottles. *Cato at Liberty,* 23 set. 2014. Disponível em: <https://www.cato.org/blog/old-technopanic-new-ibottles>. Acesso em: 22 out. 2017.

76 Ver, por exemplo, MONCAU, Luiz Fernando Marrey. O problema por trás do bloqueio do WhatsApp. *Jota,* 21 jul. 2016. Disponível em: <https://jota.info/artigos/o-problema-por-tras-bloqueio-whatsapp-21072016>. Acesso em: 22 out. 2017.

77 SWIRE, Peter; AHMAD, Kenesa. Encryption and Globalization. *The Columbia Science & Technology Law Review*, v. 23, p. 457-458;473-480, 2012.

4.3. Balanço de consequências

A discussão sobre custos e benefícios de criptografia forte não para aqui. Agentes de segurança, normalmente, têm tréplicas para os argumentos daqueles que defendem a criptografia forte: dizem que registros e metadados não possuem o mesmo peso como evidência que o conteúdo de comunicações — apontam que um suspeito esteve perto do local do crime, mas não confirmam que era ele quem atraiu a vítima à emboscada, por exemplo; também veem com certo ceticismo que a criptografia precise ser "tão forte assim" como WhatsApp e Apple o querem — outras empresas não conseguem garantir segurança aos seus clientes e ao mesmo tempo atender as necessidades de autoridades? Essas respostas levam, novamente, a mais uma rodada de contra-argumentos dos que defendem a criptografia forte.

Diante disso, cabe lembrar que somente é possível um debate racional sobre essas questões de política regulatória se ele for informado — baseado em evidências concretas, não em casos anedóticos e retórica do medo. Para falar que criptografia está realmente comprometendo investigações e a segurança pública em geral de uma forma que legitime a regulamentação de alguma forma, seria necessário um levantamento de evidência empírica robusta sobre todas as vezes em que essa dificuldade foi crítica para a não resolução de um caso, conjuntamente com levantamento de dados sobre qual tipo de crime se tratava.[78] Semelhantemente, para julgar potenciais alternativas regulatórias, é imprescindível uma séria avaliação de riscos para a cibersegurança individual, coletiva e nacional e para direitos humanos, discussão sobre viabilidade e operacionalização do modelo a nível global, efetividade da medida e impacto no mercado. Será importante, também, levar em conta o efeito colateral da utilização (e permissão) da criptografia forte na investida em técnicas de investigação via *hacking estatal*, tema que, também, desperta questões peculiares de privacidade e segurança.[79] Tudo isso dentro de um contexto regulatório que pode se alterar profundamente com o desenvolvimento tecnológico, como por exemplo pela eventual descoberta e disseminação de formas inovadoras de criptoanálise a serem exploradas por autoridades de segurança.[80]

5. Considerações finais

Por um acaso histórico, as tensões inerentes à criptografia estão pré-anunciadas no cenário nacional brasileiro desde 1945, de quando data o primeiro registro histórico da palavra 'criptografia' em jornais brasileiros. A citação é encontrada no folhetim semanal "A Mulher do Realejo", de Xavier de Montepin", no jornal *O Estado de São Paulo*.[81] Pelo que se entende da leitura do capítulo daquele dia, um juiz de instrução "interceptou" cartas que serviriam como instrumento de prova num processo, mas algumas delas estavam em outra língua, e, outra, criptografada. Ele, então, pergunta para seu assistente se ele tem alguma familiaridade com criptografia, ao que o assistente responde que "muito pouco". Quis a história que nós começássemos assim a nossa história com a criptografia: com um juiz tendo dificuldades em um processo em razão da criptografia.

78 Não se contesta que a criminalidade é facilitada por determinadas tecnologias, mas recomenda-se que a dimensão dessa facilitação deva ser discutida a partir de evidências. Sobre a criminalidade 'em rede', ver LADEUR, Karl-Heinz. New institutions for the protection of privacy and personal dignity in internet communication – "information broker", "private cyber courts" and network of contracts. *Revista Brasileira de Políticas Públicas*, Brasília, v. 10, n.1, p. 281-296, 2013.

79 Ver KERR, Orin; SCHNEIER, Bruce. Encryption Workarounds. *Georgetown Law Journal,* 2018. Disponível em: <https://ssrn.com/abstract=2938033>. Acesso em: 20 out. 2017; BANKSTON, Kevin. Ending The Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors. *Lawfare*, 14 jun. 2017. Disponível em: <https://www.lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors>. Acesso em: 6 dez. 2017; ABREU, Jacqueline de Souza. From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp. *Columbia Journal of Transnational Law Online Edition*, 17 out. 2016. Disponível em: <http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/>. Acesso em: 28 set. 2017.

80 Sobre essa possibilidade, ver PFEFFERKORN, Riana. Everything Radiates: Does The Fourth Amendment Regulate Side-Channel Cryptanalysis? *Connecticut Law Review*, v. 49, n. 5, p. 1393-1452, 2017.

81 O ESTADO DE SÃO PAULO, p. 5, 9 maio 1945.

O cenário está fadado a continuar assim quando estamos lidando com criptografia forte. No direito brasileiro e estadunidense atuais, argumentei neste artigo que não há nada que proíba expressamente empresas de internet e de tecnologia de desenvolverem sistemas seguros de comunicação e armazenamento de dados. E mais: razões de política regulatória desencorajam qualquer alteração desse cenário; pelo menos no atual estado da técnica[82] e nas mais recentes avaliações de riscos. Com isso, por ora, é importante que agentes de segurança reconheçam esse novo tipo de obstáculo à obtenção de provas tal como outras dificuldades com as quais já frequentemente têm de lidar, como falecimento de vítimas, destruição de provas e encontros pessoais. Ainda assim, na medida em que o desenvolvimento tecnológico avança, é improvável que o embate entre autoridades de segurança pública e empresas pare por aqui. Haverá outras batalhas.[83]

Referências

ABELSON, Hal et al. The risks of key recovery, key escrow, and trusted third-party encryption. *Columbia University Academic Commons*, 1997. Disponível em: <http://academiccommons.columbia.edu/catalog/ac:127127>. Acesso em: 23 out. 2017.

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

ABREU, Jacqueline de Souza. From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp. *Columbia Journal of Transnational Law Online Edition*, 17 out. 2016. Disponível em: <http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/>. Acesso em: 28 set. 2017.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. E quando o policial vira hacker? *Blog InternetLab*, 17 jul. 2017. Disponível em: <http://www.internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/> Acesso em: 6 dez. 2017.

ANTONIALLI, Dennys et al. Especial: o que dizem especialistas em criptografia sobre bloqueio do WhatsApp. *Deu nos Autos*, 21 jul. 2016. Disponível em: <http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/>. Acesso em: 27 set. 2017.

BADARÓ, Gustavo Henrique Righi Ivahy. Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In: LIMA, José Corrêa de; CASARA, R. R. Rubens. (Coord.). *Temas para uma perspectiva crítica do direito:* homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010. p. 483-499.

BANKSTON, Kevin. Ending The Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors. *Lawfare*, 14 jun. 2017. Disponível em: <https://www.lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors>. Acesso em: 6 dez. 2017.

BARRETO, Alesandro Gonçalves; CASELLI, Guilherme. WhatsApp: é possível cumprir decisões judiciais? *Direito & TI,* 10 abr. 2016. Disponível em: <http://direitoeti.com.br/artigos/whatsapp-e-possivel-cumprir-decisoes-judiciais/>. Acesso em: 23 out. 2017.

82 Quem faz juízo de cautela semelhante é POWLES, Julia; CHAPARRO, Enrique. In the wake of Apple vs. FBI, we need to face some uncomfortable truths. *The Guardian*, 29 mar. 2016. Disponível em: <https://www.theguardian.com/technology/2016/mar/29/apple-fbi-encryption-san-bernardino-uncomfortable-truths>. Acesso em: 22 out. 2017.

83 Agradeço a Caio Gentil Ribeiro, Daniel Murata e Guilherme Bandeira pelos comentários a uma versão preliminar deste artigo. Por conversas e oportunidades que me ajudaram a organizar e amadurecer as ideias apresentadas, também agradeço a Amy Zhang, Artur Pericles Lima Monteiro, Beatriz Kira, Bruno Bioni, Dennys Antonialli, Francisco Brito Cruz, Lisa Patel, Mariana Cunha e Melo, Mariana Valente, Riana Pfefferkorn, Ronaldo Macedo, Ryan Budish, Tobias Boelter e Urs Gasser.

BRAMAN, Sandra. *Change of State:* Information, Policy, and Power. Cambridge: The MIT Press, 2007.

COMEY, James. *Going Dark*: Are Technology, Privacy, and Public Safety in a Collision Course? Discurso proferido no Brookings Institute, 14 out. 2016. Disponível em: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>. Acesso em: 23 out. 2017.

CERDEIRA, Pablo; FERREIRA, Helena. Permitir grampo no WhatsApp coloca a sociedade em risco. *Jota*, 2 jun. 2017. Disponível em: <https://jota.info/artigos/permitir-grampo-no-whatsapp-colocar-a-sociedade-em-risco-02062017>. Acesso em: 23 out. 2017.

DIFFIE, Whitfield; HELLMAN, Martin. New directions in cryptography. *IEEE transactions on Information Theory*, v. 22, n. 6, p. 644-654, 1976. Disponível em: <https://www-ee.stanford.edu/~hellman/publications/24.pdf>. Acesso em: 26 out. 2017.

DIFFIE, Whitfield; LANDAU; Susan. *Privacy on the Line:* The Politics of Wiretapping and Encryption. Cambridge: The MIT Press, 2007.

DONEDA, Danilo. A regulação da criptografia e o bloqueio do WhatsApp. *Consultor Jurídico*, 30 maio 2017. Disponível em: <https://www.conjur.com.br/2017-mai-30/danilo-doneda-regulacao-criptografia-bloqueio-whatsapp>.

FERRAZ JUNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, p. 439-459, 1993.

FERRAZ JUNIOR, Tercio Sampaio; MARANHÃO, Juliano; FINGER, Marcelo. O desafio do WhatsApp ao Leviatã. *Folha de S. Paulo*, São Paulo, 16 ago. 2016. Opinião. Disponível em: <http://www1.folha.uol.com.br/opiniao/2016/08/1803323-o-desafio-do-whatsapp-ao-leviata.shtml>.

GASSER, Urs et al. Don't Panic. *Making Progress in the 'Going Dark' Debate*: Berkman Klein Center For Internet & Society. 1 fev. 2016. Disponível em: <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>. Acesso em: 23 out. 2017.

GUIMARÃES, Lucas Noura. The dichotomy between smart metering and the protection of consumer's personal data in Brazilian law. *Revista Brasileira de Políticas Públicas,* v. 7, n. 3, 2017.

MARCACINI, Augusto. *Direito e Informática:* uma abordagem jurídica sobre a criptografia. São Paulo: edição eletrônica, 2010. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DireitoECriptografia>. Acesso em: 23 out. 2017.

KERR, Orin; SCHNEIER, Bruce. Encryption Workarounds. *Georgetown Law Journal,* 2018. Disponível em: <https://ssrn.com/abstract=2938033>. Acesso em: 20 out. 2017.

KOOPS, Bert-Jaap. *The Crypto Controversy:* 0. The Haag: Kluwer Law International, 1999.

KAHN, Matthew. Deputy Attorney General Rod Rosenstein Remarks on Encryption. *Lawfare*, 10 out. 2017. Disponível em: <https://www.lawfareblog.com/deputy-attorney-general-rod-rosenstein-remarks-encryption>. Acesso em: 23 out. 2017.

LADEUR, Karl-Heinz. New institutions for the protection of privacy and personal dignity in internet communication: "information broker", "private cyber courts" and network of contracts. *Revista Brasileira de Políticas Públicas*, Brasília, v. 10, n.1, p. 281-296, 2013.

LESSIG, Lawrence. Reading the Constitution. *Cyberspace, Emory Law Journal*, v. 45, p. 869-910, 1996.

LEVY, Steven. *Crypto:* how the code rebels beat the government saving privacy in the digital age. New York: Penguin Books, 2001.

LIMA, Caio César Carvalho. Criptografia e (ou?) interceptação das comunicações. *Jota*, 31 maio 2017. Disponível em: <https://jota.info/colunas/direito-digital/criptografia-e-ou-interceptacao-das-comunicaco-

es-31052017>. Acesso em: 23 out. 2017.

MONCAU, Luiz Fernando Marrey. O problema por trás do bloqueio do WhatsApp. *Jota,* 21 jul. 2016. Disponível em: <https://jota.info/artigos/o-problema-por-tras-bloqueio-whatsapp-21072016>.

PFEFFERKORN, Riana. *Apple vs. FBI*: Where did it come from? What Is It? Where Is It Going? Palestra realizada na Universidade da Califórnia, Berkeley, 7 mar. 2016. Disponível em: <https://cyberlaw.stanford.edu/files/blogs/Riana%20BIPLA%20talk%203-7-16.pdf>. Acesso em: 23 out. 2017.

PFEFFERKORN, Riana. A Response to "Responsible Encryption". *Center for Internet & Society at Stanford Law School Blog*, 11 out. 2017. Disponível em: <http://cyberlaw.stanford.edu/blog/2017/10/response-"responsible-encryption">.

PFEFFERKORN, Riana. Everything Radiates: Does The Fourth Amendment Regulate Side-Channel Cryptanalysis? *Connecticut Law Review*, v. 49, n. 5, p. 1393-1452, 2017.

POWLES, Julia; CHAPARRO, Enrique. In the wake of Apple vs. FBI, we need to face some uncomfortable truths. *The Guardian*, 29 mar. 2016. Disponível em: <https://www.theguardian.com/technology/2016/mar/29/apple-fbi-encryption-san-bernardino-uncomfortable-truths>. Acesso em: 23 out. 2017.

RICE, Eric. The Second Amendment and the Struggle Over Cryptography. *Hastings Science and Technology Law Journal*, v. 9, p. 29-88, 2017.

ROSA, João Luiz Moraes. Sigilo e persecução penal. *Justiça do Direito*, v. 31, n. 1, p. 120-150, jan./abr. 2017.

ROZENSHTEIN, Alan Z. Surveillance Intermediaries. *Stanford Law Review*, v. 70, p. 29, 2018. Disponível em: <https://ssrn.com/abstract=2935321>. Acesso em: 10 out. 2017.

SANCHEZ, Julian. Old Technopanic in New iBottles. *Cato at Liberty,* 23 set. 2014. Disponível em: <https://www.cato.org/blog/old-technopanic-new-ibottles>. Acesso em: 23 out. 2017.

SILVA, Alexandre Assunção e. *Sigilo das Comunicações na Internet*. Curitiba: Juruá, 2017.

SINGH, Simon. *The Code Book:* The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 1999.

SWIRE, Peter; AHMAD, Kenesa. Encryption and Globalization. *The Columbia Science & Technology Law Review*, v. 23, p. 416-481, 2012.

SOBRAL, Carlos Eduardo. Por que a Justiça deve bloquear o WhatsApp. *Jota*, 4 jul. 2016. Disponível em: <https://jota.info/artigos/por-que-justica-deve-bloquear-o-whatsapp-quando-nao-ha-colaboracao-04072016>. Acesso em: 23 out. 2017.

SOLOVE, Daniel; SCHWARTZ, Paul. *Information Privacy Law*. 4. ed. New York: Wolters Kluver, 2015.

ZITTRAIN, Jonathan. *The Future of the Internet and How to Stop It*. New Haven: Yale University Press, 2008.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.