Carlos **Liguori**

Direito e Criptografia

Direitos Fundamentais, Segurança da Informação e os limites da regulação jurídica na tecnologia

2022

saraiva jur

saraiva EDUCAÇÃO | saraiva jur

Av. Paulista, 901, 3º andar
Bela Vista – São Paulo – SP – CEP: 01311-100

SAC | sac.sets@saraivaeducacao.com.br

Diretoria executiva Flávia Alves Bravin
Diretoria editorial Ana Paula Santos Matos
Gerência editorial e de projetos Fernando Penteado

Novos projetos Aline Darcy Flôr de Souza
Dalila Costa de Oliveira

Gerência editorial Isabella Sánchez de Souza
Edição Daniel Pavani Naveira
Samantha Rangel Gonçalves
Stephanie Cristina Pereira
Tobias Viana Paiva

Produção editorial Daniele Debora de Souza (coord.)
Cintia Aparecida dos Santos
Daniela Nogueira Secondo

Arte e digital Mônica Landi (coord.)
Camilla Felix Cianelli Chaves
Claudirene de Moura Santos Silva
Deborah Mattos
Guilherme H. M. Salvador
Tiago Dela Rosa

Projetos e serviços editoriais Daniela Maria Chaves Carvalho
Emily Larissa Ferreira da Silva
Kelli Priscila Pinto
Klariene Andrielly Giraldi

Projeto gráfico Mônica Landi
Diagramação LGB Publicações
Revisão Amélia Ward
Capa Tiago Dela Rosa
Produção gráfica Marli Rampim
Sergio Luiz Pereira Lopes

Impressão e acabamento

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
VAGNER RODOLFO DA SILVA – CRB-8/9410

L727d Liguori, Carlos

Direito e Criptografia: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia / Carlos Liguori. – São Paulo : SaraivaJur, 2022.

328 p.

ISBN 978-65-536-2346-0 (impresso)

1. Direito. 2. Criptografia. 3. Direito Digital. 4. Criptografia. 5. LGPD. 6. Novas tecnologias. 7. Marco civil da internet. I. Título.

CDD 340.0285
2021-3897 CDU 34:004

Índices para catálogo sistemático:

1. Direito Digital 340.0285
2. Direito Digital 34:004

Data de fechamento da edição: 12-11-2021

Dúvidas? Acesse www.editorasaraiva.com.br/direito

CL 607201 CAE 785410

Para Zoraide Gonçalves de Andrade,

que agora nada ao lado de seu outro cisne.

CAPÍTULO 5

SOLUÇÕES JURÍDICAS PARA O PROBLEMA E OS PROBLEMAS JURÍDICOS DAS SOLUÇÕES

A partir da segunda metade da década de 2010, uma grande quantidade de países começou a debater projetos de lei e implementar legislações para responder as questões levantadas no debate "going dark". As soluções propostas variam desde normas que afetam diretamente o desenvolvimento, a implementação e a utilização de sistemas criptográficos, até a busca por mecanismos alternativos de investigação, de forma a viabilizar as atividades de investigação sem impor alterações nos sistemas. O objetivo deste capítulo é apresentar e analisar essas soluções. Para isso, ele será dividido em três partes:

Na primeira parte, apresentarei modelos regulatórios da criptografia adotados ao redor do mundo, fruto do mapeamento de legislações e políticas públicas produzido para uma pesquisa que coordenei no Centro de Ensino e Pesquisa em Inovação (CEPI, 2019). Apontarei suas características principais, apresentarei países que adotaram cada um deles e descreverei seus possíveis problemas.

Na segunda parte, apresentarei formas de investigação que são apresentadas como alternativas à restrição de sistemas criptográficos. São elas: análise de metadados; dados armazenados em nuvem e dados obtidos a partir de dispositivos da Internet das Coisas (IoT). Muitas vezes essas

soluções são apresentadas de forma circunstancial, sem o devido aprofundamento das complexas questões relativas a direitos fundamentais que elas ensejam. Este item busca suprir essa lacuna na literatura, tomando como referência as dificuldades que seriam enfrentadas no cenário brasileiro.

Por fim, tratarei em detalhes de um mecanismo alternativo de investigação que, em minha opinião, orientará todo o futuro do debate "going dark": o "hacking governamental" (*government/lawful hacking*) (BELLOVIN et al., 2014; MAYER, 2018; GUTHEIL et al., 2017). Trata-se da "manipulação de software, dados, sistema computacional, rede ou outro dispositivo eletrônico sem a permissão ou conhecimento da pessoa ou organização responsável por ele ou por demais dispositivos afetados por esta manipulação". Nesse sentido, ele pode consistir: (i) na exploração de vulnerabilidades de software ou hardware para acessar dados de comunicação ou armazenados pelo governo; ou também (ii) no desenvolvimento, pelo governo, de software malicioso nos dispositivos investigados para fins de monitoramento (STEPANOVICH, 2018). Argumento que esse mecanismo deve ser a principal solução a ser perseguida para adequar as autoridades de investigação à realidade do século XXI. No entanto, apontarei os diversos pontos complexos que devem ser levados em consideração no estabelecimento de um *framework* jurídico para *government hacking*, quais sejam: (i) definição e escopo de aplicação; (ii) operacionalização da atividade; (iii) desenvolvimento e aquisição de tecnologia; e (iv) *accountability* e transparência de vulnerabilidades e atores afetados.

5.1. Modelos de regulação jurídica da criptografia

Entre os anos 2017 e 2019, coordenei no Centro de Ensino e Pesquisa em Inovação da Fundação Getulio Vargas (CEPI) uma pesquisa de direito comparado com a finalidade de estabelecer um panorama global da regulação da criptografia (CEPI, 2019). Nosso objetivo foi, a partir de uma amostra de 40 países, identificar tendências e modelos de regulação da criptografia ao redor do mundo. Na conclusão da pesquisa, identificamos que 31 países já possuíam algum tipo de legislação consolidada sobre o tema, enquanto 18 países estavam debatendo projetos de lei (propondo legislação nova ou reformas à legislação preexistente).

A partir desse conjunto de dados, identificamos categorias em comum nas distintas legislações e, com isso, desenvolvemos alguns modelos de regulação da criptografia. Além disso, tive também a oportunidade de explorar cada um deles em trabalho posterior (LIGUORI FILHO, 2018). Importante notar que países podem adotar – e, em muitos casos, de fato adotam – mais de um modelo regulatório em seus ordenamentos jurídicos.

Pelo fato da exploração de soluções normativas ao debate "going dark" ser algo indispensável para esta obra, reproduzi-los-ei aqui de forma um pouco mais aprofundada, e ainda acrescentarei na análise meu posicionamento em relação às vantagens e desvantagens de cada um deles para as questões trabalhadas até agora.

Vale acrescentar que, ainda que a pesquisa do CEPI seja minha fonte principal, utilizarei subsidiariamente duas outras pesquisas: a primeira é uma consulta pública coordenada por David Kaye (2018), relator especial para a promoção e proteção do direito à liberdade de opinião e expressão[1]; e a segunda é um mapeamento realizado pelo professor da Universidade de Tilburg, Bert Jaap Koops (2013), em seu website *Crypto Law Survey*[2]. Koops vinha realizando uma ampla pesquisa sobre regulação jurídica da criptografia a partir de 1999, com o final das primeiras *Crypto Wars*. No entanto, a última atualização do mapeamento foi realizada justamente em fevereiro de 2013, apenas quatro meses antes das revelações de Snowden que, como visto, desencadearam o debate contemporâneo.

---

1 A pesquisa consistiu no envio, a representante dos países, das seguintes questões: "First, do the rights to privacy and freedom of opinion and expression protect secure online communication, specifically by encryption or anonymity? And second, assuming an affirmative answer, to what extent may governments, consistent with human rights law, impose restrictionson encryption and anonymity?". No final, 17 países contribuíram para a consulta. Disponível em: <https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx>. Acesso em: 31 de março de 2021.

2 KOOPS, Bert-Jaap. *Crypto Law Survey*, 2013. Disponível em: <http://www.cryptolaw.org/>. Acesso em: 31 de março de 2021.

5.1.1. Proibição de criptografia forte

Uma primeira abordagem normativa para lidar com a questão é simplesmente proibir a criptografia forte em território nacional, criminalizando seu desenvolvimento, sua implementação, sua disponibilização e/ou seu uso. Esse modelo costuma ser adotado por países autoritários, tendo em vista que a criptografia é uma forma de evitar o controle estatal sobre as atividades de seus cidadãos online.

Exemplo disso é o **Irã**, país historicamente conhecido pela censura à Internet. Durante os protestos ocorridos no país entre 2017 e 2018, o governo bloqueou massivamente o acesso a redes sociais, como Instagram, Facebook e YouTube e aplicativos de comunicação, como Telegram e Signal[3]. No final de 2019, o acesso à Internet de forma geral foi suspenso em resposta a manifestações populares em Tehran[4]. Ainda que grande parte da justificativa para o bloqueio dos serviços esteja atrelada ao conteúdo compartilhado por eles[5], o Irã conta com normas específicas relacionadas a proibição do uso de criptografia no país.

A principal delas está contida na Lei de Crimes Computacionais de 2009 que, em seu art. 10, estabelece:

> Art. 10. Toda pessoa que, sem poder para tal, impedir o acesso de pessoas autorizadas aos dados, ou sistema de computador ou de telecomunicações, escondendo dados, trocando senhas e criptografando dados, será punida com uma pena de 91 dias a 1 ano de prisão, ou com uma multa de 5.000.000 a 20.000.000 Rials, ou com a pena de prisão e multa[6].

Esse dispositivo pode ser interpretado tanto para proibir o uso de criptografia por usuários finais, quanto para proibir a disponibilização de aplicações que contem com sistemas de criptografia ponta a ponta, tendo em vista ser tecnicamente impossível para o provedor do serviço o fornecimento da chave às autoridades.

Outro país que se encaixa nesta categoria é o **Paquistão**. Assim como o Irã, o país é notório pelos esforços em censurar atividades online, com um longo histórico de censura e bloqueio a conteúdos na Internet[7]. A Lei de Prevenção de Crimes Eletrônicos de 2016[8] estabelece dispositivos bastante amplos que podem ser utilizados para justificar a proibição de criptografia no país. O mais relevante é o crime disposto na seção 15 da lei:

> Seção 15. Elaborar, obter ou fornecer dispositivo utilizado para comissão de crime. Produzir, desenvolver, adaptar, fornecer etc., determinado dispositivo ou sistema para ser utilizado (ou que pode ser primariamente utilizado) na comissão ou no auxílio para comissão dos demais crimes elencados na lei[9].

---

3 BRANDOM, Russell. Iran blocks encrypted messaging apps amidst nationwide protests. *The Verge* (2-1-2018). Disponível em: <https://www.theverge.com/2018/1/2/16841292/iran-telegram-block-encryption-protest-google-signal>; e DEAHL, Dani. Iran has banned Telegram after claiming the app encourages protests. *The Verge* (1º-5-2018). Disponível em: <https://www.theverge.com/2018/5/1/17306792/telegram-banned-iran-encrypted-messaging-app-russia>. Acesso em: 31 de março de 2021

4 FASSIHI, Farnaz. Iran Blocks Nearly All Internet Access. *The New York Times* (17-11-2019). Disponível em: <https://www.nytimes.com/2019/11/17/world/middleeast/iran-protest-rouhani.html>. Acesso em: 31 de março de 2021.

5 Para uma análise aprofundada das normas relacionadas à censura da Internet no Irã, cf. ZARWAN, Elijah. False Freedom: Online Censorship in the Middle East and North Africa. Relatório de Pesquisa – Human Rights Watch, 2005.

6 Tradução própria. Em inglês: "Art 10. Every person who, without authority, prevents authorized persons from access to data, or computer or telecommunication system by hiding data, changing passwords, and encrypting data shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine". Versão em inglês disponibilizada pelo Escritório das Nações Unidas sobre drogas e crime (UNODC). Disponível em: <https://www.unodc.org/res/cld/document/computer-crimes-act_html/Computer_Crimes_Act.pdf>. Acesso em: 31 de março de 2021.

7 Cf. BALOCH, Haroon; XYNOU, Maria; FILASTÒ, Arturo. Internet Censorship in Pakistan: Findings from 2014-2017. *Open Observatiori of Network Interference*, 2017. Disponível em: <https://ooni.org/post/pakistan-internet-censorship/>. Acesso em: 31 de março de 2021.

8 Versão oficial em inglês disponível em: <http://www.na.gov.pk/uploads/documents/1472635250_246.pdf>. Acesso em: 31 de março de 2021.

9 Tradução nossa (CEPI, 2019). No original, em inglês: "Sec. 15. Making, obtaining, or supplying device for use in offence. Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data

Essa norma é abrangente o suficiente para incluir qualquer tipo de sistema criptográfico: a criptografia ponta a ponta pode ser utilizada para a comunicação entre criminosos e a criptografia de disco rígido pode ser utilizada para armazenamento de material ilícito, por exemplo (CEPI, 2019).

A proibição da criptografia é uma saída autoritária, prejudicial aos direitos fundamentais e absolutamente ineficaz. Trata-se de uma forma de normatização da censura estatal, que afronta de forma direta a privacidade, a liberdade de expressão e os demais direitos viabilizados pela criptografia, como visto no Capítulo 2. Consubstanciado na necessidade de controle de comportamentos criminosos, a medida é ainda por cima ineficaz, uma vez que criminosos com conhecimento técnico simplesmente utilizarão serviços dotados de criptografia forte hospedados em outros países, em que a proibição é inexistente. A maioria dos prejudicados, no final das contas, serão os cidadãos comuns.

5.1.2. Licença ou Autorização Governamental para oferecimento e utilização de mecanismos criptográficos

Alguns países requerem a obtenção prévia de licença governamental para autorização de desenvolvimento, implementação e comercialização de sistemas criptográficos em seu território. Na maior parte das vezes, autorizações são concedidas mediante o cumprimento do requisitante com as requisições estabelecidas pelas autoridades. Por mais que consistam em formas de controle, modelos de licenciamento não necessariamente implicam imposições de restrições à criptografia, podendo consistir em limitações de importação ou apenas imposições burocráticas (LIGUORI FILHO, 2018, p. 68).

Israel adota esse modelo, diferenciando a utilização de criptografia para finalidades civis ou militares, com esta última sofrendo mais restrições do que a primeira[10]. A obtenção da licença envolve o cumprimento de alguns requisitos, como:

- Auditoria do lugar de produção do item, assim como o processo, produto criptográfico, registros relacionados à criptografia e as circunstâncias nas quais a produção e armazenamento de sistemas criptográficos estão sendo ou serão conduzidas;
- Demandas discricionárias de outros detalhes necessários;
- Cláusula de confidencialidade sobre o desenvolvimento de tecnologias criptográficas durante o processo de licenciamento;
- Proibição da exportação do produto para: Irã, Síria, Coréia do Norte, Líbano, Sudão e Cuba[11].

O Ministério da Defesa é o órgão responsável pelo licenciamento, pelo controle e pela categorização desses produtos[12]. O Ministério pode, ainda, de forma discricionária, isentar determinados produtos criptográficos dessa regulação[13]. A isenção costuma ser concedida a produtos criptográficos de código aberto e para uso particular[14].

---

or device, primarily with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to 6 months or with fine up to fifty thousand rupees or with both".

10 Cf Encryption Controls in Israel. *Ministry of Defense*. Disponível em: <https://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx>. Acesso em: 31 de março de 2021.

11 Cf. Announcements – Encryption Controls. *Ministry of Defense*. Disponível em: <https://www.mod.gov.il/English/Encryption_Controls/Pages/FAQ-Encryption-Controls-.aspx>. Acesso em: 31 de março de 2021.

12 Law Governing the Control of Commodities and Services, 1957 (5717): "(a) No one shall engage in encryption items unless he/she has been licensed to do so by the Director and according to the terms of license". Disponível em: <http://www.mod.gov.il/English/Encryption_Controls/Pages/order.aspx>. Acesso em: 31 de março de 2021.

13 A "Free Means" is a means of encryption for which a general license has been granted or which the Director-General has declared to be decontrolled. Once an encryption item is defined as a free means, it is free of the licensing restrictions. A periodically revised list of encryption items which have been declared "decontrolled" is published in the Official Gazette of the Government of Israel. Cf. <https://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx>. Acesso em: 31 de março de 2021.

14 Disponível em: <https://www.lexology.com/library/detail.aspx?g=b31fe40f-9564-44cf-b241-bcda18c0fc61>. Acesso em: 31 de março de 2021.

De forma mais restritiva, a Índia estabelece que provedores de telecomunicações e provedores de serviços de Internet devem utilizar sistemas criptográficos com chaves de, no máximo, 40 bits. No caso de sistemas mais robustos, deve-se obter uma licença excepcional do Departamento de Telecomunicações para oferecer seus serviços no país, e o requisito para tal inclui o fornecimento das chaves criptográficas ao Departamento (SWIRE, AHMAD, 2012, p. 418; BUDISH et al., 2018, p. 11):

> Cláusula 1.10.1 – Criptografia. Indivíduos/Grupos/Organizações têm permissão para usar criptografia com chaves até o tamanho 40 bits com algoritmos RSA ou seu equivalente em outros algoritmos sem a necessidade de obter permissão. Entretanto, se equipamentos de criptografia superiores a este limite forem implantados, indivíduos/grupos/organizações deverão fazê-lo com a permissão da Autoridade de Telecomunicações e depositar a chave criptográfica, dividida em duas partes, junto à Autoridade de Telecomunicações.

Essa restrição, colocada em prática em 1999, impõe fragilizações ao sistema em todos os cenários: aqueles que não desejam obter a licença governamental, devem adequar seus sistemas a um padrão de segurança exponencialmente mais fraco do que se costuma adotar ao redor do mundo[15]. Os que querem oferecer algo mais robusto, devem entregar as chaves à autoridade reguladora.

Questiono, entretanto, a eficácia dessa imposição: na teoria, ela inviabiliza o oferecimento de sistemas de criptografia ponta a ponta no país, uma vez que não só os serviços mais populares (como WhatsApp e Signal) utilizam chaves de 256 bits, como também é tecnicamente impossível a essas empresas o fornecimento das chaves criptográficas, devido à própria estrutura desse tipo de criptografia[16]. Na prática, no

15 Sistemas criptográficos modernos utilizam chaves de, no mínimo, 128 bits (KERR, SCHNEIER, 2018, p. 994).

16 GRIFFIN, Andrew. WhatsApp end-to-end encryption update might have made chat app illegal in India. *Independent* (8-4-2016). Disponível em: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-end-to-end-encryption-update-might-have-made-chat-app-illegal-in-india-a6974921.html>. Acesso em: 31 de março de 2021.

entanto, a Índia é o país com o maior número de usuários de WhatsApp do mundo, cerca de 400 milhões[17].

Além disso, a medida é inconsistente com diversas regulações setoriais dentro da própria Índia. O Banco Central do país, por exemplo, recomenda a utilização de chaves de, no mínimo, 128 bits para serviços de *internet banking*[18].

Esse modelo regulatório não tem muito o que oferecer em relação às questões levantadas pelo debate "going dark". A modalidade adotada por Israel pouco responde aos anseios das autoridades de investigação, enquanto a da Índia incorre nas mesmas questões levantadas pela proibição da criptografia forte.

5.1.3. Obrigação de assistência

Alguns aprendizados das *Crypto Wars* 1.0 foram incorporados por governos em legislações recentes sobre acesso a dados criptografados e investigações criminais. Ao invés de propor *explicitamente* a implementação obrigatória de *backdoors* ou mecanismos de acesso excepcional em sistemas criptográficos – como na malfadada iniciativa do *Clipper Chip* nos anos 1990 –, países vêm propondo legislação que obriga pessoas físicas ou jurídicas a "prestar assistência" a autoridades de investigação em relação ao fornecimento de conteúdos criptografados. Essas normas não indicam de forma particular os meios para o cumprimento da obrigação, apenas estabelecem sua existência de forma geral.

Na pesquisa que conduzi na FGV (CEPI, 2019; LIGUORI FILHO, 2018), identificamos que essa obrigação de assistência pode estar descrita de forma *genérica* – simplesmente requerendo o "fornecimento de informações às autoridades"; ou *específica* – na forma de uma obrigação explícita de entrega das chaves criptográficas ou do fornecimento do conteúdo na forma legível.

17 SINGH, Manish. WhatsApp reaches 400 million users in India, its biggest Market. *Techcrunch* (26-7-2019). Disponível em: <https://techcrunch.com/2019/07/26/whatsapp-india-users-400-million/>. Acesso em: 31 de março de 2021.

18 Disponível em: <https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=243>. Acesso em: 31 de março de 2021.

Explorarei a seguir esses dois modelos na prática. Acrescentarei ainda uma abordagem particular de obrigação de assistência específica que merece destaque: a solução norueguesa de limitar o direito à não autoincriminação para fornecimento de dados biométricos para desbloqueio de sistemas.

5.1.3.1. Obrigação genérica de assistência

Na categorização de modelos regulatórios desenvolvidas por nós no CEPI (2019), definimos as obrigações genéricas de assistência como:

> Trata-se de uma obrigação, presente no ordenamento jurídico de determinado país, que pode ser invocada para solicitar que determinada pessoa (física ou jurídica) forneça informações criptografadas na forma legível ou auxilie neste processo de decriptação no contexto de investigações criminais. Encaixam-se na vertente genérica desse tipo de obrigação aqueles países que possuem mecanismos jurídicos que, por sua abrangência ao estabelecer obrigações de auxílio às autoridades de investigação, são entendidos como suficientes para impelir o solicitado a providenciar essa assistência. Não há menção explícita a criptografia ou a seus elementos neste modelo regulatório.

Como a própria nomenclatura já estabelece, trata-se simplesmente de uma obrigação geral de auxiliar as autoridades que é imposta a determinado sujeito. Essas obrigações não existem nos ordenamentos jurídicos para lidar especificamente com questões de acesso a dados criptografados por autoridades, mas o texto da norma é amplo o suficiente para ser utilizado com esta finalidade.

O **México**, por exemplo, dispõe que provedores de sistemas de comunicação privadas podem ser obrigados a prestar assistência a autoridades de investigação na condução de interceptações, sob pena de sanção. A obrigação se aplica a qualquer pessoa física ou jurídica, investigada ou não:

> **Artigo 301. Colaboração com a autoridade:** Os concessionários, titulares de autorização e outros proprietários dos meios ou sistemas suscetíveis à interceptação, devem colaborar eficientemente com a autoridade competente para o desenvolvimento de tais mecanismos de investigação, de acordo com as disposições aplicáveis. Da mesma forma, eles devem ter a capacidade técnica necessária para atender aos requisitos exigidos pela autoridade judicial para executar um mandado de interceptação de comunicações privadas. O não cumprimento desse mandato será punido de acordo com as disposições penais aplicáveis[19].

Outro país com normas na mesma linha é o **Canadá** que, em seu Código Criminal, estabelece uma obrigação genérica de assistência para o cumprimento de mandados judiciais que autorizem interceptações e/ou acesso a dados. Aqui, também, não é necessário que o sujeito obrigado a prestar assistência seja um dos investigados (GILL et al., 2018, p. 63):

> **Ordem de assistência – 487.02** Se uma autorização for dada sob as seções 184.2, 184.3, 186 ou 188 ou se um mandado for emitido com base nesta Lei, o juiz ou tribunal que der a autorização ou emitir o mandado pode ordenar que uma pessoa preste assistência, se a assistência da pessoa puder ser razoavelmente considerada necessária para dar efeito à autorização ou mandado. A ordem tem efeito em todo o Canadá[20].

Esse modelo é problemático porque o texto aberto das normas concede poderes de forma desproporcionada às autoridades de investigação,

19 Tradução própria. No original, em espanhol: "Artículo 301. Colaboración con la autoridad: Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con las disposiciones aplicables. Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas. El incumplimiento a este mandato será sancionado conforme a las disposiciones penales aplicables". Codigo Nacional de Procedimientos Penales. Disponível em: <http://dof.gob.mx/nota_detalle.php?codigo=5334903&fecha=05/03/2014>. Acesso em: 31 de março de 2021.

20 Tradução própria. No original, em inglês: "Assistance order – 487.02 If an authorization is given under section 184.2, 184.3, 186 or 188 or a warrant is issued under this Act, the judge or justice who gives the authorization or issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the authorization or warrant. The order has effect throughout Canada". Criminal Code. Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/C-46/page-111.html#docCont>. Acesso em: 31 de março de 2021.

principalmente em relação a terceiros não envolvidos no processo. Por se tratar de obrigações genéricas, não há como estabelecer de antemão o que pode e o que não pode ser solicitado pelas autoridades, sendo necessária a contestação da obrigação posteriormente.

Além disso, gera ainda insegurança jurídica a todas as partes envolvidas – à autoridade de investigação, que necessita ter certeza sobre a extensão da assistência que lhe é permitido solicitar, sob pena de ver anulada parte da instrução probatória e prejuízos à atividade investigativa; ao sujeito da obrigação, que deve judicializar ordens que julga abusivas ou desproporcionais; e ao investigado, que pode ter seus direitos violados a depender do grau de invasividade da ordem.

5.1.3.2. Obrigação específica de assistência

Definimos, no contexto da pesquisa do CEPI (2019), as obrigações específicas de assistência como:

> (...) uma obrigação, presente no ordenamento jurídico de determinado país, que pode ser invocada para solicitar que determinada pessoa (física ou jurídica) forneça informações criptografadas na forma legível ou auxilie nesse processo de decriptação no contexto de investigações criminais. Encaixam-se na vertente específica países que tratam explicitamente de criptografia e de seus elementos nas normas que tratam desse tipo de obrigação. Ordenamentos que possuam normas que obriguem a entrega de chaves criptográficas ou que explicitamente solicitem o fornecimento de informações em linguagem legível encaixam-se nesse modelo regulatório.

Exemplo deste modelo pode ser encontrado na **França**. O Código Penal Francês (*Code pénal*), em seu Artigo 434-15-2, criminaliza a recusa da entrega de chaves criptográficas que viabilizem o acesso a informação relacionada à preparação, à facilitação ou à comissão de crimes, estabelecendo como sanção multa e até mesmo prisão:

> Art. 434-15-2: É punido com três anos de prisão e uma multa de 270.000 euros para qualquer pessoa que, tendo conhecimento da informação necessária para decifrar um meio de criptografia que possa ter sido utilizado para preparar, facilitar ou cometer um crime ou delito, se recuse a entregar a referida informação às autoridades judiciais ou a implementá-la, a pedido dessas autoridades, emitido de acordo com os Títulos II e III do Livro I do Código de Processo Penal.
>
> Se a recusa for feita quando a entrega ou implementação da Convenção teria impedido a prática de um crime ou ofensa ou teria limitado seus efeitos, a pena é aumentada para cinco anos de prisão e uma multa de 450.000 euros[21].

Em 2016, o dispositivo foi alterado de forma a enrijecer as sanções relacionadas a esse crime. A razão desta alteração foi a promulgação da Loi 2016-731, voltada ao combate ao terrorismo e crime organizado (*Loi 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*)[22]. Essa lei surgiu em resposta aos atentados terroristas ocorridos em Paris em 2015 e 2016 e ampliou os poderes de vigilância do Estado francês em relação à interceptação de comunicações e acesso a dados (SEVERSON, 2016, p. 2-3).

A questão da possibilidade técnica de fornecimento de dados na forma legível e a subsequente necessidade de que aplicações alterem seus sistemas para viabilizar esse acesso é algo que vinha sendo debatido pelo governo francês na segunda parte da década de 2010 (ACHARYA

---

21 Tradução própria. No original, em francês: "Art. 434-15-2: Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.
Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende". Código Penal Francês. Disponível em: <https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418646&cidTexte=LEGITEXT000006070719>. Acesso em: 31 de março de 2021.

22 Loi 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. Disponível em: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id>. Acesso em: 31 de março de 2021.

et al., 2017a). Nas eleições de 2017, a preocupação com o uso de aplicativos de comunicação criptografados por terroristas foi uma das bandeiras levantadas pelo então candidato Emmanuel Macron[23]. Desde sua eleição, no entanto, não houve qualquer movimentação legislativa mais incisiva diante da questão no país.

Outro país que se encaixa nesta vertente é a **Austrália**. No final de 2018, o país promulgou o *Telecommunications and Other Legislation Amendment (Assistance and Access* – AA Act), que estabeleceu obrigações específicas a provedores de comunicação em relação ao fornecimento de dados e informações a autoridades de investigação e agências de inteligência.

Três instrumentos são dignos de nota em relação à criptografia: *technical assistance requests*, *technical assistance notices* e *technical capability notices*. Os três instrumentos consistem em notificações oficiais direcionadas a provedores de aplicações para que eles prestem assistência técnica às autoridades, fornecendo informações técnicas, viabilizando o acesso aos dispositivos e aos dados neles armazenados, dentre outras coisas (SHEARING, 2019).

Technical assistance requests são solicitações de assistência voluntária: não há nenhum tipo de sanção caso o provedor de comunicação se recuse a cumpri-las[24]. O cumprimento das *Technical assistance notices*, por sua vez, é obrigatório[25]. Estas consistem em notificações que exigem que os provedores assistam às autoridades na medida em que suas capacidades técnicas permitam. Por exemplo: se um provedor de serviços de armazenamento em nuvem armazena os arquivos de seus usuários na forma legível, ele pode ser obrigado a fornecer esses arquivos às autoridades. Caso a nuvem seja cifrada, a notificação não se aplicaria (Idem).

23 SEIBT, Sébastian. French candidate Macron targets encryption in fight against terrorism. *France 24* (12-4-2017). Disponível em: <https://www.france24.com/en/20170412-candidate-macron-encryption-fight-terror-whatsapp-telegram>. Acesso em: 31 de março de 2021.

24 Telecommunications and Other Legislation Amendment (Assistance and Access). Division 2 – Voluntary Technical Assistance. Arts. 317G-317K.

25 Telecommunications and Other Legislation Amendment (Assistance and Access). Division 3 – Technical Assistance Notices. Arts. 317L-317RA.

Por fim, as *technical capability notices*, diretamente baseadas no instrumento homônimo presente no ordenamento jurídico inglês, consistem em notificações oficiais que podem ser utilizadas para solicitar que empresas que utilizam sistemas criptográficos em seus serviços de comunicação alterem-nos de forma a viabilizar o acesso ao seu conteúdo na forma legível por autoridades de investigação[26].

O AA Act, quando ainda era debatido como projeto de lei, foi alvo de inúmeras críticas em relação a essa última forma de notificação: entendia-se, naquele momento, que o texto da lei era amplo o suficiente para ser interpretado no sentido de impor mecanismos de acesso excepcional em sistemas criptográficos[27]. O texto aprovado da lei, no entanto, incluiu um artigo que estabelece explicitamente que as *technical capabilities notices* não podem ser utilizadas para obrigar um provedor de aplicação a enfraquecer ou implementar quaisquer vulnerabilidades em seus sistemas[28]. No entanto, a lei é bastante recente e a real

26 Telecommunications and Other Legislation Amendment (Assistance and Access). Division 4 – Technical Capabilities Notices. Arts. 317S-317ZAA.

27 Cf. O'BRIEN, Danny. In the New Fight for Online Privacy and Security, Australia Falls: What Happens Next? *Electronic Frontier Foundation* (6-12-2018). Disponível em: <https://www.eff.org/pt-br/deeplinks/2018/12/new-fight-online-privacy-and-security-australia-falls-what-happens-next>; KARP, Paul. Australia's war on encryption: the sweeping new powers rushed into law. *The Guardian* (7-12-2018). Disponível em: <https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law>; WHITE, Nathan. What (we think) you should know about Australia's new encryption bill. *Access Now* (16-8-2018). Disponível em: <https://www.accessnow.org/what-we-think-you-should-know-about-australias-new-encryption-bill/>. Acesso em: 31 de março de 2021.

28 Art. 317ZG. Designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc. (1) A technical assistance request, technical assistance notice or technical capability notice must not have the effect of: (a) requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection; or (b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.
Interessante apontar que o Department of Home Affairs do Governo Australiano criou uma espécie de "FAQ" sobre o AA Act para sanar dúvidas acerca das *technical capabilities notices e backdoors*. Cf. Assistance and Access: Common Myths and Misconceptions. Disponível em: <https://www.homeaffairs.gov.au/about-us/our-

extensão do alcance desta modalidade de notificação ainda está para ser visto na prática.

5.1.3.3. Fornecimento de dados biométricos para acesso a sistema computacional

Após se deparar com diversos casos envolvendo apreensão de celulares bloqueados por biometria, o que suscitou diversas incertezas jurídicas acerca de como proceder no acesso ao seu conteúdo, a **Noruega** alterou o seu Código de Processo Penal em 2017 de forma bastante direcionada. A Seção 199-A do Código passou a dispor o seguinte:

> Sec. 199-A. Ao realizar uma busca em um sistema de processamento de dados, a polícia pode ordenar que todos que estejam lidando com o referido sistema forneçam as informações necessárias para obter acesso ao sistema ou para abri-lo por meio do uso de autenticação biométrica.
>
> Caso alguém se recuse a cumprir uma ordem de autenticação biométrica como mencionado no primeiro parágrafo, a polícia pode realizar a autenticação pela força.
>
> A permissão para usar a força de acordo com o segundo parágrafo é dada pela autoridade de acusação. Se o atraso implicar um risco de que a investigação seja prejudicada, a permissão poderá ser dada pela polícia no local. A decisão da polícia deve ser submetida à procuradoria[29].

Trata-se de uma forma de obrigação específica de assistência que busca responder aos questionamentos colocados no item 4.1.3.3 *supra*,

---

portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act>. Acesso em: 31 de março de 2021.

29 Tradução própria da versão em inglês produzida por Ingvild Bruce (2017, p. 28): "Sec. 199-A. When conducting a search of a data-processing system the police may order everyone who is dealing with the said system to provide the information necessary for gaining access to the system or to open it by use of biometric authentication. Should anyone refuse to comply with an order of biometric authentication as mentioned in the first paragraph, the police may perform the authentication by force. Permission to use force according to the second paragraph is given by the prosecuting authority. If delay entails a risk that the investigation will be impaired, permission may be given by the police on the spot. The decision by the police shall be submitted to the prosecuting authority".

acerca do fornecimento dos meios para decriptação e sua compatibilização com o direito a não autoincriminação. Aqui, o legislador optou por incluir explicitamente no texto a obrigação do fornecimento de autenticação biométrica para acesso ao conteúdo bloqueado, acrescendo isso às "informações necessárias para acesso ao sistema". Em uma primeira leitura, essa inclusão pode parecer redundante, mas é algo necessário na medida em que a autenticação biométrica envolve a realização de um ato físico do indivíduo com acesso ao sistema (*e.g.*, inserção da digital, escaneamento da íris etc.), e não apenas o fornecimento de uma informação que pode ser inserida por terceiros (*e.g.*, senha, PIN).

Houve discussões acerca da compatibilidade do dispositivo com o direito à não autoincriminação, que também está presente no ordenamento norueguês. No entanto, a avaliação da compatibilidade se baseou no que se estabeleceu no já mencionado caso Saunders *vs.* The United Kingdom, da Corte Europeia de Direitos Humanos[30]. O parlamento da Noruega entendeu que a autenticação biométrica forçada não entraria em conflito com a não autoincriminação, porque envolve o fornecimento de uma característica física do indivíduo que existe independentemente da sua vontade, e por isso não forçaria o suspeito a escolher entre mentir ou incriminar-se a si mesmo (BRUCE, 2017, p. 29).

Ao utilizar a expressão "sistema de processamento de dados" para referir-se ao que se pretende acessar, a norma é suficientemente ampla para abarcar dados contidos em dispositivos eletrônicos (hardware) e em aplicações (software) (Idem, p. 28). Nesse sentido, a autenticação pode ser solicitada tanto para desbloqueio de *smartphones* e computadores quanto para acesso a contas de e-mail ou de serviços de armazenamento em nuvem, por exemplo. Além disso, a expressão "autenticação biométrica" é um termo amplo o suficiente para abarcar quaisquer formas de fornecimento de dados biométricos que sejam necessários para o acesso ao sistema existente ou que possam surgir.

Dois outros pontos também são dignos de nota: o primeiro é que a obrigação pode se estender a qualquer pessoa que tenha acesso ao siste-

---

30 Cf. 4.1.3.3 *supra*.

ma, não apenas o investigado; e o segundo é que, em harmonia com os demais dispositivos do Código de Processo Penal Norueguês (especificamente Seções 197 e 198), a obrigação do fornecimento dos meios de acesso ao sistema depende de ordem judicial anterior que a autorize[31].

Talvez o aspecto mais controverso da norma trata da possibilidade do uso de força para obtenção da informação ou autenticação biométrica. O CPP Norueguês estabelece que qualquer medida coercitiva só deve ser utilizada como *ultima ratio*, quando estritamente necessário e proporcional, e avaliando cada caso concretamente[32]. A ideia de necessidade e proporcionalidade, no entanto, é tratada de forma vaga demais pelo código, o que pode abrir espaço para abusos[33].

De forma geral, o modelo norueguês apresenta alguns elementos interessantes para uma saída interessante à questão do acesso a dados armazenados criptografados: não impõe nenhum tipo de fragilização geral no sistema; estabelece de forma específica o que deve ser fornecido (autenticação biométrica/informações para acesso ao sistema); exclui explicitamente do escopo de aplicação aqueles que não possuem acesso

31 Com duas exceções: a explícita autorização por escrito da parte investigada e, caso a demora da obtenção da ordem judicial apresente algum risco à investigação. "Section 197. Without the written consent of the person concerned, a search pursuant to sections 192, 194 and 195 may only be made pursuant to a court decision. If delay entails any risk, the decision may be made by the prosecuting authority. In the event of a search of editorial offices or the like, the decision shall be made by the public prosecutor, and only if it is probable that the investigation will be substantially impaired by waiting for a court decision. Any decision pursuant to the first or second paragraph shall as far as possible be in writing and specify the nature of the case, the purpose of the search, and what it shall include. An oral decision shall be reduced to writing as soon as possible." Código de Processo Penal Norueguês, atualizado até 21 de junho de 2013. Versão de Ronald Walford e Einar Høgetveit, disponibilizada pelo Escritório das Nações Unidas sobre Drogas e Crime (UNODC). Disponível em: <https://www.unodc.org/res/cld/document/nor/2006/the_criminal_procedure_act_html/The_Criminal_Procedure_Act.pdf>. Acesso em: 31 de março de 2021.

32 "Section 170 a. A coercive measure may be used only when there is sufficient reason to do so. The coercive measure may not be used when it would be a disproportionate intervention in view of the nature of the case and other circumstances." Ibidem.

33 ELECTRONIC FRONTIER NORWAY. Norway introduces forced biometric authentication. *EDRI* (26-7-2017). Disponível em: <https://edri.org/norway-introduces-forced-biometric-authentication/>. Acesso em: 31 de março de 2021.

ao sistema investigado (*e.g.*, exclui provedores de serviços de comunicação com criptografia ponta a ponta).

No entanto, sua viabilização em consonância com direitos fundamentais e o devido processo legal depende necessariamente do estabelecimento de requisitos restritivos para concessão da ordem judicial que autorize o ato, como a limitação dos tipos de crime que podem ensejar a obrigação de assistência; e a indicação, da forma mais detalhada possível, dos conteúdos que serão acessados dentro do sistema – evitando a devassa geral dos dados do investigado.

5.1.4. Estímulo à criptografia

Alguns países optaram por uma abordagem distinta dos modelos regulatórios discutidos até agora: ao invés de impor restrições ao desenvolvimento, oferecimento e uso de mecanismos criptográficos, esses países reforçaram sua importância para o exercício de direitos fundamentais, estimulando a sua adoção. Esse estímulo geralmente não se traduz na forma de norma jurídica, mas sim de políticas públicas. Dois países, com abordagens distintas, destacam-se na adoção deste modelo.

O primeiro é a **Holanda**, país que se manifestou de forma incisiva contra qualquer tipo de imposição de vulnerabilidades/mecanismos de acesso excepcional em sistemas de segurança[34]. Em 2016, o Ministério de Justiça e Segurança, ao lado do Gabinete Holandês (braço principal do Poder Executivo da Holanda), publicou uma nota oficial posicionando-se contra a restrição de mecanismos criptográficos e declarando que não tomaria nenhuma medida restritiva à implementação ou desenvolvimento destes mecanismos[35]. O Ministério citou a essencialidade da criptografia para a segurança e a privacidade dos usuários e para o

34 Dutch government says no to "encryption backdoors". *BBC* (7-1-2016). Disponível em: <https://www.bbc.com/news/technology-35251429>. Acesso em: 31 de março de 2021.

35 Nota do Ministério da Justiça e Segurança/Gabinete Holandês traduzida para o inglês disponível em: <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption>. Acesso em: 31 de março de 2021.

funcionamento pleno da Internet, e afirmou que o governo holandês estava procurando soluções alternativas para as necessidades das autoridades de investigação.

Além disso, ainda em 2016, o parlamento holandês colocou em prática o posicionamento do país em relação à criptografia ao doar 500.000 euros para o OpenSSL Software Project, um projeto que desenvolve mecanismos de criptografia de forma aberta e gratuita[36].

O segundo país é a **Alemanha**, que vem mantendo o mesmo posicionamento em relação à criptografia desde a década de 1990, com o final das primeiras *Crypto Wars*. Em 1999, o governo alemão divulgou os "5 pontos da política alemã de criptografia" (*Eckpunkte der deutschen Kryptopolitik*), um conjunto de objetivos que visavam orientar o desenvolvimento de políticas públicas envolvendo criptografia no país (HERPIG, HEUMANN, 2019):

1. Não haverá nenhum tipo de proibição ou limitação de produtos de criptografia;
2. Os produtos de criptografia deverão ser testados quanto à sua segurança, a fim de aumentar a confiança dos usuários em relação a eles;
3. O desenvolvimento de produtos de criptografia por fabricantes alemães é essencial para a segurança do país e para garantir às empresas alemãs a capacidade de competir internacionalmente. Por isso seu desenvolvimento deve ser estimulado;
4. As autoridades de investigação criminal e de segurança pública não devem ser enfraquecidas pelo uso generalizado da criptografia. Para isso, o desenvolvimento de competências técnicas adicionais para essas autoridades deve ser estimulado;
5. A cooperação internacional em questões de criptografia, tais como padrões abertos e interoperabilidade, é essencial e deve ser fomentada multilateralmente.

36 MCCARTHY, Kieren. Dutch govt says no to backdoors, slides $540k into OpenSSL without breaking eye contact. *The Register* (4-1-2016). Disponível em: <https://www.theregister.com/2016/01/04/dutch_government_says_no_to_backdoors/>. Acesso em: 31 de março de 2021.

A retomada do debate sobre regulação da criptografia nos anos 2010 não abalou o posicionamento do país, com o Ministério do Interior manifestando-se abertamente em favor da criptografia forte e reforçando, em 2015, a existência e validade das orientações adotadas pelo país 16 anos antes[37]. Esse posicionamento foi formalizado com a publicação da Estratégia de Cibersegurança para a Alemanha, em 2016[38].

É importante notar que a opção pelo estímulo à criptografia não significa que esses países simplesmente fecharam os olhos para o debate "going dark". Ao contrário: a Alemanha, por exemplo, fez valer o ponto 4 de sua política de criptografia: para atender os anseios das autoridades de investigação, capacitou suas agências e reformou parte de seu sistema processual penal, de forma a regulamentar outros mecanismos de investigação no ambiente digital que não implicam a restrição da criptografia, como o "hacking governamental"[39].

O restante deste capítulo será inteiramente dedicado à análise desses mecanismos alternativos.

37 MONROY, Matthias. Bundesinnenministerium: "Eckpunkte der deutschen Kryptopolitik" von 1999 haben immer noch Bestand. *Netzpolitik* (17-6-2015). Disponível em: <https://netzpolitik.org/2015/bundesinnenministerium-eckpunkte-der-deutschen-kryptopolitik-von-1999-haben-immer-noch-bestand/>. Acesso em: 31 de março de 2021.

38 Cf. BUNDESMINISTERIUM DES INNERN. Cyber-Sicherheitsstrategie für Deutschland 2016. Disponível em: <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile&v=3>. Acesso em: 31 de março de 2021.

39 Essa abordagem foi inicialmente estabelecida na Estratégia de Cibersegurança para a Alemanha em 2016, e foi posteriormente incorporada no ordenamento jurídico alemão por meio de uma reforma no Código de Processo Penal em agosto de 2017. Na Estratégia, estabelece-se explicitamente que: "(...) die deutschen Strafverfolgungs- und Sicherheitsbehör sind den unter strengen gesetzlichen Voraussetzungen befugt, ver schlüsselte Kommunikation zu entschlüsseln oder zu um gehen, wenn dies im Einzelfall zur Erfüllung ihres gesetz lichen Auftrages notwendig ist. (...) die technischen Fähigkeiten der Strafverfolgungs- und Sicherheitsbehörden zur Entschlüsselung parallel zu den technischen Entwicklungen in Sachen Verschlüsselungen stetig fortentwickelt werden. Sicherheitsbehörden zur Entschlüsselung parallel zu den technischen Entwicklungen in Sachen Verschlüsselungen stetig fortentwickelt werden".

5.2. A "era do ouro da vigilância": formas alternativas de investigação

Em oposição à restrição jurídica da criptografia, estudiosos e especialistas apontam que o desenvolvimento tecnológico e o uso generalizado de mecanismos de geração e coleta de dados apresentam diversas alternativas às autoridades, sem a necessidade de comprometimento dos sistemas criptográficos.

Criticando o uso da expressão "going dark" pra descrever as dificuldades da investigação no século XXI, Swire e Ahmed (2012, p. 463) vão além e sugerem que a existência dessas fontes alternativas de informação teriam o potencial tão grande de aprimoramento das atividades de investigação que poderíamos estar vivendo em uma "era de ouro de vigilância", mesmo no contexto da disseminação da criptografia forte por padrão.

Neste item, analisarei as alternativas sugeridas com mais frequência no debate, que são: (i) o acesso a dados armazenados em serviços em nuvem; (ii) a análise dos metadados de comunicações; e (iii) a análise de dados e metadados gerados no contexto da Internet das coisas (IoT). Como veremos a seguir, cada uma delas apresenta vantagens e problemas para as autoridades. Diversas questões devem ser enfrentadas com cautela para que essas alternativas de fato representem opções eficientes e menos danosas à restrição da criptografia.

Para definir as três categorias analisadas, utilizei como fonte principal 12 relatórios de pesquisa e *policy papers* cujo tópico principal é o debate contemporâneo sobre regulação da criptografia (ABELSON et al., 2015; BERKMAN KLEIN CENTER, 2016; NASEM, 2018; GILL et al., 2018; SCHULZ, Van HOBOKEN, 2016; KUEHN, MCCONNELL, 2018; LEWIS et al., 2017; CASTRO, MCQUINN, 2016; DUAN et al., 2018; CARNEGIE, 2019; PFEFFERKORN, 2017; SOESANTO, 2018), além das falas apresentadas na audiência pública sobre bloqueios de aplicativos no STF.

Por fim, vale fazer uma ressalva em relação a uma quarta alternativa sugerida em grande parte destes trabalhos: o chamado "hacking governamental". Trata-se do mecanismo alternativo de investigação que julgo mais complexo e relevante para este debate, por isso ele será analisado individualmente em outro item (5.3).

5.2.1. *Backup* de dados e armazenamento em nuvem: outras fontes, mesmo conteúdo

Como já mencionei, o debate contemporâneo sobre regulação da criptografia se debruça em duas preocupações: a impossibilidade de interceptação de dados em trânsito, por causa de mecanismos de criptografia ponta a ponta; e a impossibilidade de acesso a dados armazenados em dispositivos, por causa da criptografia forte implementada por padrão em sistemas operacionais. Em grande parte dos casos, no entanto, pode haver uma terceira via para acessar esses mesmos conteúdos: o *backup* de dados em serviços de armazenamento em nuvem (*cloud storage*).

Atualmente, serviços de armazenamento em nuvem são populares tanto entre usuários particulares quanto entre empresas. Dentre os maiores provedores temos o Google Drive, com mais de 800 milhões de usuários ativos[40], o iCloud, da Apple, com mais de 780 milhões de usuários[41] e o Dropbox, com 600 milhões[42].

De forma simplificada, esses serviços permitem que usuários transfiram arquivos de seus computadores pessoais para servidores externos, gerenciados e operacionalizados por provedores como Amazon ou Google. O enorme conjunto de servidores administrados por essas empresas é genericamente chamado de "nuvem". Esse serviço fornece três diferenciais ao usuário: (i) o primeiro é a possibilidade de armazenamento de arquivos sem que eles ocupem espaço no

40 Dados de 2017, cf. LARDINOIS, Frederic. Google updates Drive with a focus on its business users. *TechCrunch* (9-3-2017). Disponível em: <https://techcrunch.com/2017/03/09/google-drive-now-has-800m-users-and-gets-a-big-update-for-the-enterprise/>. Acesso em: 31 de março de 2021.

41 Dados de 2016, cf. Apple Music passes 11M subscribers as iCloud hits 782M users. *Apple Insider* (12-2-2016). Disponível em: <https://appleinsider.com/articles/16/02/12/apple-music-passes-11m-subscribers-as-icloud-hits-782m-users>. Acesso em: 31 de março de 2021.

42 Dados de 2019, cf. KOVAR, Joseph. Dropbox: New Products, Integration Will Help Drive Higher Productivity, Free Cash Flow In 2020. *CRN* (21-2-2020). Disponível em: <https://www.crn.com/news/storage/dropbox-new-products-integration-will-help-drive-higher-productivity-free-cash-flow-in-2020>. Acesso em: 31 de março de 2021.

disco rígido do computador, o que viabiliza a gestão de grandes quantidades de dados[43]; (ii) o segundo é a acessibilidade aos dados; bastam as credenciais (login e senha) e acesso à internet para que os arquivos armazenados na nuvem sejam acessíveis em qualquer dispositivo. Além disso, muitos desses serviços permitem que usuários compartilhem arquivos entre si; (iii) por fim, o terceiro e talvez mais importante diferencial desses serviços é sua função de *backup* de dados.

A realização periódica de *backups* (criação de cópias digitais da totalidade do conteúdo de determinado disco) é essencial para garantir a recuperação de dados comprometidos devido a falhas no disco rígido, infeção por *malware* ou perda do dispositivo. No passado, a cópia dos dados era gravada em disquetes ou CDs. Hoje em dia, costuma-se fazê-las em HDs externos e, principalmente, na nuvem. A vantagem desta última é a maior segurança em relação a disponibilidade dos dados: HDs externos podem ser destruídos, roubados ou perdidos; na nuvem, os dados estarão sempre disponíveis[44].

Outra funcionalidade de destaque oferecida por esses serviços é o *backup* em tempo real: no instante em que um arquivo é criado no dispositivo, realiza-se o *upload* de uma cópia para a pasta na nuvem. Não é necessário, portanto, fazer *backups* periódicos. É muito comum que provedores de sistemas operacionais ofereceram a modalidade gratuita da nuvem logo na configuração inicial de um novo dispositivo – o iCloud em aparelhos da Apple, Google Drive em *smartphones* com Android e em Chromebooks e OneDrive no Windows[45].

43 Serviços como o Google Drive oferecem armazenamento de 15GB na modalidade gratuita e chegam a 10 TB na mais cara modalidade *premium* – espaço muito superior ao disco rígido da vasta maioria dos notebooks à venda. Cf. <https://onedrive.live.com/about/pt-BR/plans/>. Acesso em: 31 de março de 2021.

44 A não ser, claro, que haja algum tipo de destruição ou apagamento de dados em massa nos *data centers* dos provedores do serviço, algo bastante improvável.

45 Seria incorreto afirmar que esses serviços oferecem a nuvem "por padrão", uma vez que há a necessidade de cadastro e ativação dela pelo usuário. No entanto, faz parte do modelo de negócio desses serviços estimular sua adoção em massa, seja por meio do uso dos dados dos usuários ou convencendo-os a assinar pacotes *premium*. Cf. <https://www.computerworld.com/article/2882210/warning-apple-wants-to-get-you-hooked-on-icloud.html>. Acesso em: 31 de março de 2021.

No debate sobre regulação da criptografia, alguns trabalhos sugerem que esse sistema poderia oferecer às autoridades um jeito de acessar, na forma legível, dados que estão criptografados nos aparelhos dos investigados, solicitando-os, na forma da lei, diretamente aos provedores do serviço em nuvem. Centrando esforços nessa hipótese, não haveria a necessidade de nenhum tipo de enfraquecimento do sistema criptográfico (DUAN et al., 2018, p. 7; NASEM, 2018, p. 71; KUEHN, MCCONNEL, 2018, p. 32; GILL et al., 2018, p. 14 e 100; CARNEGIE, 2019, p. 18; BERKMAN KLEIN CENTER, 2016, p. 12-14; SWIRE, 2012). Não houve, no entanto, menção ao mecanismo na audiência pública sobre bloqueio de aplicativos no Brasil – por mais que o *backup* de dados de *smartphones* inclua, naturalmente, cópia das conversas realizadas via WhatsApp.

A seguir, explorarei as vantagens e os problemas do acesso aos dados armazenados na nuvem como fonte alternativa de dados para investigações criminais.

5.2.1.1. Vantagens: dados na forma legível

A grande vantagem da nuvem é que, na vasta maioria dos casos, os provedores do serviço são capazes de acessar os conteúdos armazenados na forma legível. Isso não quer dizer que os dados são imprudentemente armazenados na forma legível ou que o seu sistema de segurança é frágil[46]. Além da necessidade de fornecimento de credenciais como login e senha, via de regra, os provedores desses serviços implementam mecanismos de criptografia forte tanto na transmissão dos dados (do dispositivo pessoal aos servidores externos e vice-versa, geralmente via SSL), quanto no armazenamento dos dados nos servidores (AES 128-bit no iCloud e Google Drive e AES 256-bit no Dropbox)[47]. No entanto, a

46 Obviamente, esses sistemas são sim mais frágeis do que aqueles em que não há guarda da cópia das chaves pelos provedores.

47 WINDER, David. Cloud storage: How secure are Dropbox, OneDrive, Google Drive and iCloud? *ITPro* (14-2-2020). Disponível em: <https://www.itpro.co.uk/cloud-security/34663/cloud-storage-how-secure-are-dropbox-onedrive-google-drive-and-icloud>. Acesso em: 31 de março de 2021.

maior parte desses provedores guarda para si uma cópia da chave criptográfica, viabilizando que seus sistemas acessem e processem os arquivos dos usuários na forma legível (ZHANG, 2018).

Isso ocorre por três motivos principais. Em primeiro lugar, garante-se alguns benefícios aos usuários, como a possibilidade de recuperação das chaves, caso eles esqueçam seu login e senha ou tenham suas contas invadidas por terceiros. Não havendo a guarda da cópia das chaves, o conteúdo se perderia para sempre (VANDENBERG, 2017, p. 546). Além disso, o acesso e processamento dos dados pelo sistema são necessários para oferecer ao usuário mecanismos de indexação e busca de dados em suas plataformas, tanto na busca de arquivos quanto de conteúdos de arquivos (ZHANG, 2018; BERKMAN KLEIN CENTER, 2016, p. 11).

Em segundo lugar, o acesso aos dados na forma legível é necessário para garantir a segurança e a estabilidade dos servidores da nuvem, além de certificar que os materiais lá armazenados são lícitos. Nesse sentido, são realizados escaneamentos para identificação de malware, pornografia infantil, material que viole direitos autorais, dentre outros (JOHNSON, 2017, p. 874).

Por fim, em terceiro lugar, o próprio modelo de negócio das plataformas de serviços em nuvem gera desincentivos à implementação de mecanismos que as impeçam de acessar os conteúdos nelas armazenados. Principalmente no caso de plataformas que o fornecem de forma gratuita, o acesso aos dados é essencial para monetização do serviço: o tratamento dos dados dos usuários é realizado para o direcionamento de propagandas (BERKMAN KLEIN CENTER, 2016, p. 10; VANDENBERG, 2017, p. 546).

Nesse cenário, a nuvem pode oferecer às autoridades exatamente o mesmo conteúdo que está inacessível em sistemas criptográficos sem que haja restrição da criptografia.

5.2.1.2. Problemas: o futuro da nuvem e questões de jurisdição

Por causa do potencial invasivo do acesso aos dados na nuvem, são necessários robustos mecanismos jurídicos que viabilizem sua obtenção

de forma equilibrada com a proteção à privacidade e o devido processo legal[48].

Além disso, é possível que, futuramente, os provedores alterem seus sistemas de segurança de forma que eles não possuam mais acesso aos dados dos usuários na forma legível. O cenário pode mudar devido a incentivos regulatórios advindos de recentes legislações de proteção de dados, como a GDPR na União Europeia e a LGPD no Brasil, que impõem pesadas sanções às empresas no caso de vazamento de dados (VANDENBERG, 2017, p. 547).

Vazamentos de dados e outros problemas de segurança de serviços de armazenamento em nuvem estão frequentemente sob os holofotes. Fotos íntimas de celebridades foram vazadas do iCloud e compartilhadas na internet em 2014[49]; login e senha de 68 milhões de usuários do Dropbox vazaram em 2012[50]; credenciais de 5 milhões de usuários do Gmail – email vinculado ao Google Drive – vazaram em fóruns de discussão russos em 2014[51]. As recentes regulações, ao lado do crescente número de usuários e empresas que dependem desses serviços, podem estimular mudanças em suas políticas de segurança no futuro. Alguns provedores menos populares, como o Mega e o SpiderOak, oferecem o serviço de nuvem criptografada sem a guarda da cópia das chaves (ZHANG, 2018).

---

48 Esse genérico parágrafo inicial será repetido incessantemente na análise de todos os mecanismos alternativos de investigação deste capítulo. Todas essas medidas são incrivelmente invasivas e precisam observar os direitos fundamentais e o devido processo legal. A diferença delas e da restrição da criptografia é que nesta última há uma imposição legal de enfraquecimento dos sistemas, enquanto aquela busca viabilizar a exploração de informações já disponíveis no ecossistema digital, sem qualquer tipo de restrição jurídica.

49 ARTHUR, Charles. Naked celebrity hack: security experts focus on iCloud backup theory. *The Guardian* (1º-9-2014). Disponível em: <https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence>. Acesso em: 31 de março de 2021.

50 GIBBS, Samuel. Dropbox hack leads to leaking of 68m user passwords on the internet. *The Guardian* (31-8-2016). Disponível em: <https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach>. Acesso em: 31 de março de 2021.

51 RHODAN, Maya. Nearly 5 Million Google Passwords Leaked on Russian Site. *Time Magazine* (10-9-2014). Disponível em: <https://time.com/3318853/google-user-logins-bitcoin/>. Acesso em: 31 de março de 2021.

Além disso, há a questão da requisição de dados a provedores localizados fora do país onde ocorre a investigação. Isso é algo recorrente, uma vez que grandes provedores de serviços em nuvem possuem *data centers* distribuídos ao redor do mundo. A criação de efetivos vínculos de colaboração entre autoridades de investigação e essas empresas, além do aprimoramento de mecanismos de cooperação internacional em matérias criminais, como os MLATs, é essencial para garantir a eficácia da investigação na nuvem[52].

5.2.2. Metadados: Mesmas fontes, outro conteúdo

Por mais que sistemas de criptografia forte impossibilitem o acesso ao conteúdo do que está sendo comunicado ou armazenado, isso não implica a inacessibilidade de todo e qualquer tipo de informação referente aos dados cifrados. Nessa categoria, encontram-se os chamados metadados.

Metadados são geralmente definidos como "dados sobre dados", informações descritivas sobre arquivos digitais ou ações realizadas no ambiente virtual. Tratam-se de todas as informações sobre determinado(s) dado(s) que não sejam o seu conteúdo em si (SINGER, FRIEDMAN, 2014, p. 297). Tomemos como exemplo uma ligação telefônica: o seu conteúdo é a própria conversa – o diálogo travado entre as pontas da comunicação; os metadados, por sua vez, são informações como o número do telefone do emissor, o número do telefone do receptor, a operadora utilizada, a duração da ligação, entre outros[53].

52 O tema é muito extenso e complexo, e uma abordagem detalhada dele neste livro seria tematicamente incoerente e temporalmente inviável. Ficam aqui, no entanto, algumas recomendações de leitura para aqueles que quiserem se aprofundar no tema: WALDEN, Ian. Accessing data in the Cloud: The long arm of the Law Enforcement Agent. *Privacy and Security for Cloud Computing*. London: Springer, 2013, p. 45-71; SVANTESSON, Dan Jerker B.; VAN ZWIETEN, Lodewijk. Law enforcement access to evidence via direct contact with cloud providers: identifying the contours of a solution. *Computer Law & Security Review*, v. 32, n. 5, p. 671-682, 2016; e SVANTESSON, Dan; GERRY, Felicity. Access to extraterritorial evidence: The Microsoft cloud case and beyond. *Computer Law & Security Review*, v. 31, n. 4, p. 478-489, 2015.

53 Cf. What Are Call Detail Records (CDRs)? Onsip. Disponível em: <https://www.onsip.com/voip-resources/voip-fundamentals/what-are-call-detail-records-cdrs>. Acesso em: 31 de março de 2021.

Esses "rastros" deixados pela comunicação telefônica têm o potencial de serem particularmente relevantes para autoridades de investigação. Ainda que não apresentem especificamente o *que* foi comunicado, os metadados podem auxiliar nas respostas a diversos questionamentos sobre a conversa, como: (i) *quem* são as pontas da comunicação, ao indicar as linhas telefônicas utilizadas e, subsequentemente, seus titulares; (ii) *quando* a ligação foi realizada, por meio de data e hora; e (iii) *onde* a ligação foi realizada, pela localização da linha física, ou pela localização das antenas de telefonia no caso da comunicação via telefone celular (NASEM, 2018, p. 45). Por mais que esses dados por si só não resolvam com 100% de precisão cada um dos questionamentos, eles não deixam de ser informações relevantes para a investigação criminal.

Outra vantagem é que, ao contrário do conteúdo da conversa telefônica em si, que é instantânea e passageira, os metadados são facilmente registráveis e armazenáveis, além de gerenciados por um pequeno número de atores, os provedores de telefonia. Em muitas jurisdições, inclusive no Brasil, há diversas obrigações legais de guarda de determinados tipos de metadados por esses provedores, o que contribui também para sua disponibilidade às autoridades de investigação[54].

Na esfera digital, a quantidade de metadados gerada é mais vasta do que na comunicação telefônica. Eles não se restringem aos dados sobre comunicações entre usuários via Internet, incluindo também informações sobre arquivos armazenados e compartilhados[55], identifica-

54 Ver ABREU, ANTONIALLI (2017 p. 10) e item 4.1.3 *supra*.

55 Informações como: tipo de arquivo (foto, vídeo, texto), extensão (.jpg, .png, .mp4, .mkv), data de criação, tamanho (em bytes), privilégios de administrador, entre outros. Vale a pena mencionar um padrão de formato de arquivos (geralmente de foto e vídeo) frequentemente adotado em smartphones e câmeras fotográficas, o *Exif*. Esse padrão permite que diversos metadados sobre as imagens sejam incluídos no arquivo, como marca e modelo da câmera, velocidade do obturador, tipo de exposição, ISO, zoom, número de pixels, data e hora do registro e até mesmo dados de geolocalização. Essas informações são absolutamente relevantes para o fotógrafo profissional, e acabam sendo muito úteis também nas investigações criminais. Cf. COSSETTI, Melissa. O que são dados EXIF de fotos e como encontrá-los ou escondê-los. *Tecnoblog*. Disponível em: <https://tecnoblog.net/259798/o-que-sao-dados-exif-de-fotos-e-como-encontra-los-ou-esconde-los/>;

dores de conexões e dispositivos[56], registro de atividades em aplicações[57], entre outros.

Ao contrário da comunicação telefônica, em que os registros concentram-se basicamente nos provedores de telefonia, na comunicação via Internet metadados podem ser encontrados em diversas fontes, desde no nível da conexão à Internet, como endereços IP, *mac address* e informações sobre transferência de dados via TCP; até no nível das aplicações, como logs de conexão e dados cadastrais de usuários, além de informações sobre comunicações realizadas por meio dessas aplicações, como emissor, destinatário e assunto em mensagens de e-mail. Todas essas informações dispersas, quando tomadas em conjunto, viabilizam uma análise precisa sobre o comportamento e as atividades de usuários para as autoridades de investigação.

No debate sobre regulação da criptografia, a exploração dos metadados das comunicações criptografadas como meio de investigação criminal é sugerida com frequência como uma possível alternativa à restrição do uso de mecanismos criptográficos, ainda que seja pouco explorada. Argumenta-se que a coleta e análise dessas informações seria uma opção eficaz e preferível ao enfraquecimento proposital de sistemas de segurança (ABELSON et al., 105, p. 3; CARNEGIE, 2019, p. 5; GILL et al., 2018, p. 22; LEWIS et al., 2017, p. 35; KUEHN, MCCONNELL, 2018, p. 24; CASTRO, MCQUINN, 2016, p. 25; NASEM, 2018, p. 45, 71; SWIRE, AHMAD, 2012, p. 467).

---

e BARRETO, Alessandro; CASELLI, Guilherme. Exif Metadata – A investigação policial subsidiada por sua extração e análise. *Delegados – Portal Nacional* (26-6-2016). Disponível em: <https://delegados.com.br/noticia/exif-metadata-a-investigacao-policial-subsidiada-por-sua-extracao-e-analise>. Acesso em: 31 de março de 2021.

56 Endereço IP (que identifica a conexão de um dispositivo à Internet), número de porta do TCP (que identifica endereço MAC), entre outros.

57 Aqui entram os já bem conhecidos no direito brasileiro "logs de conexão", "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dado", de acordo com o MCI. A depender do nível de precisão que adotarmos para a definição de metadados, aqui podem entrar também todo e qualquer tipo de informação cadastral do usuário na aplicação, que variam desde nome de usuário e login até data de nascimento e outros dados pessoais.

Além disso, os metadados também foram mencionados com frequência na Audiência Pública do STF sobre bloqueio de aplicativos em 2017, em que autoridades da Polícia Federal e do Ministério Público ressaltaram a sua importância na investigação criminal contemporânea[58] e especialistas contrários à imposição de mecanismos de acesso excepcional apontaram-na como a melhor solução a ser buscada de forma a evitar o comprometimento da segurança dos sistemas[59].

---

58 Mais especificamente Ivo Peixinho, perito da PF: "Propõe-se que a empresa **forneça metadados**, que acreditamos que ela disponha, mediante ordem judicial referente a um caso em investigação (...), com a possibilidade talvez de notificar conteúdo relacionado a pornografia infantil, quando forem compartilhados elementos de mídia, como imagens e vídeos" (p. 21-22); e Fernanda Domingos, procuradora da República: "(...) embora o objeto das ações não discuta diretamente criptografia **e fornecimento de conteúdo de metadados**, são questões subjacentes ao descumprimento das ordens judiciais que ensejaram os bloqueios do aplicativo WhatsApp, pois **são relevantes para as investigações de crimes seríssimos**, é preciso lembrar, como tráfico de drogas, de armas e de pessoas, troca de pornografia infantil, preparação de sequestro, de homicídios e de atentados terroristas, dentre outros" (p. 48, grifos meus).

59 Uma grande quantidade de especialistas tocou nesse ponto em específico: Demi Getschko, do Comitê Gestor da Internet no Brasil: "só para avisar que não tem nenhum motivo de pânico, a internet é uma rede de controle. A nossa preocupação é evitar que ela vire um monitoramento geral de todo mundo, o tempo todo. Se há uma barreira a colocar, não é a barreira de menos visibilidade e, sim, a barreira de mais. Quer dizer, impedir que estejamos invadindo adicionalmente a vida do indivíduo. **Os metadados resolvem a maioria dos casos**" (p. 81); Anderson Nascimento, Professor da American University: "eu gostaria de comentar que existe a possibilidade de **metadados**, como foi colocado; geolocalização, se você tem acesso à companhia de telefonia celular, você pode obter as informações de onde aquela pessoa estava, com quem ela estava falando, a lista de contatos, **você pode montar o verdadeiro dossiê digital**" (p. 93); Diego Aranha, professor do IC-UNICAMP: "(...) **modernizar o aparato investigativo para que ele tenha condições de usar técnicas de investigação que sejam menos intrusivas. Já foi citada várias vezes aqui a análise de metadados**, por exemplo, que são de coleta obrigatória, armazenamento obrigatório nos termos do Marco Civil, lembrando que metadados nada dizem sobre o conteúdo das mensagens fotos e vídeos trafegados por esses canais, esses sistemas de comunicação" (p. 140); Marco Antonio Simplício, professor da POLI-USP: "Assim, **as respostas que são muito mais promissoras vão no sentido de obter metadados** e obter dados, memória, que não dependam da criptografia do canal de comunicação" (p. 157); Fabio Maia, da Assespro: "Você é capaz de, através do exame dos metadados de comunicação, construir toda uma hierarquia de relacionamento de uma organização criminosa. (...) É inacreditável a quantidade

Apesar dessas vantagens, a coleta e a análise de metadados gerados pelas atividades online podem causar diversos problemas relacionados à privacidade dos usuários e suscitar questões acerca da capacidade de vigilância do Estado sobre seus cidadãos – algo que as revelações de Edward Snowden mostraram já serem realizadas na prática.

A seguir, explorarei especificamente as vantagens e as desvantagens que a análise de metadados apresenta diante dos questionamentos trazidos no debate sobre regulação da criptografia, com foco na análise dos metadados gerados em comunicações online, e apontarei algumas questões jurídicas que devem ser enfrentadas de forma a viabilizar esse tipo de investigação sem que ela possa gerar abusos.

5.2.2.1. Vantagens: disponibilidade, estruturação e guarda obrigatória (em alguns casos)

Ainda que em sistemas de comunicação criptografados o conteúdo seja inacessível a terceiros, os metadados estão presente na forma legível mesmo nos mais robustos sistemas de criptografia ponta a ponta: informações sobre emissor, destinatário, hora e data da comunicação e até mesmo a localização razoavelmente precisa dos usuários (a partir do endereço IP) não são cifradas na maior parte dos aplicativos populares, como o iMessage e o WhatsApp[60]. Isso é necessário para que o sistema funcione corretamente: o conteúdo da mensagem em si é cifrado no aparelho do emissor, encaminhado para os servidores da Apple ou do WhatsApp e redirecionado para o destinatário, que decifra o conteúdo em seu próprio aparelho. Do modo como eles funcionam, o encaminhamento da mensagem não seria possível caso os metadados sobre emissor e destinatário fossem cifrados[61]. Uma vez que os provedores têm acesso a esse conteúdo na forma legível, não haveria a questão da impossibilidade técnica de fornecê-lo às autoridades[62].

Em alguns sentidos, esses metadados podem ser mais elucidativos para as autoridades de investigação do que o próprio conteúdo[63]. Do ponto de vista organizacional e analítico, David Hayes (2017, p. 198-199) indica algumas vantagens específicas, das quais destaco duas:

A primeira, é que metadados são estruturados: referem-se a informações específicas, sem deixar muita margem para interpretação. Os dados podem indicar hora e data de envio de mensagens, localização física razoavelmente precisa de onde as mensagens foram enviadas (endereço IP do receptor e emissor) etc. Nem sempre esse tipo de informação-chave é facilmente abstraída do conteúdo em si. Além disso, a estruturação permite melhor controle e análise dos dados.

A segunda, em relação ao tamanho dos arquivos, é que metadados são mais leves do que o conteúdo, requerendo menor poder computacional para seu processamento. Isso é extremamente vantajoso na análi-

---

de informação que você é capaz de coletar de um indivíduo, só observando metadados dele" (p. 184); Ronaldo Lemos, advogado e diretor do ITS-Rio: "Apesar de não ter o conteúdo, **esses metadados são poderosíssimos**. Tanto são poderosos que, depois do caso Snowden, nos Estados Unidos, a própria NSI resolveu diminuir a quantidade de metadados que eles guardavam, porque achavam que estavam exacerbados os limites constitucionais" (p. 244); Marcelo Amarante, pesquisador da UnB: "**A captura de metadados sempre é recomendada** e pode ser estudada caso a caso se seria útil utilizá-la, se seria útil, para a investigação" (p. 275); e Nelson Lago, do IME-USP: "**O poder dos metadados é enorme**. Você consegue obter muita coisa a partir dos metadados. Você sabe quais pessoas se comunicam regularmente, se aquelas pessoas se comunicaram, (...) Você tem um universo de informações que não teria em outras formas de comunicação" (p. 389, grifos meus).

60 Cf. NEWMAN, Lily Hay. Encrypted Messaging Isn't Magic. *Wired* (14-6-2018). Disponível em: <https://www.wired.com/story/encrypted-messaging-isnt-magic/> Acesso em: 31 de março de 2021.

61 É importante dizer que existem alguns aplicativos que cifram determinados metadados. O Signal, por exemplo, cifra metadados sobre o emissor da mensagem. Cf. LEE, Micah. Battle of the Secure Messaging Apps: How Signal Beats WhatsApp. *The Intercept* (22-6-2016). Disponível em: <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>. Acesso em: 31 de março de 2021.

62 Como se verá adiante, ainda que seja tecnicamente possível que os provedores forneçam esses metadados, questões jurídicas surgem acerca da obrigação da guarda dessas informações.

63 Seu poder elucidativo, no entanto, não é ilimitado. Nas palavras de Rozenshtein (2019, p. 1201): "os metadados podem ser suficientes para colocar um suspeito na cena do crime, mas não basta estabelecer que a pessoa realmente puxou o gatilho".

se de grandes conjuntos de dados, possibilitando o mapeamento detalhado das atividades dos investigados[64].

Em relação a sua disponibilidade, uma outra vantagem para as autoridades é que diversos países incluem em seus ordenamentos jurídicos obrigações de guarda de determinados tipos de metadados por provedores de telefonia e de serviços de Internet (conexão e aplicação).

No Brasil, por exemplo, provedores de telefonia fixa e móvel têm a obrigação de reter e manter à disposição de delegados de polícia e do Ministério Público "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais" por cinco anos[65]. Provedores de conexão à Internet devem armazenar registros de conexão ("o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados", definido no art. 5º, VI, do MCI) por um ano[66]. Provedores de aplicações de Internet, por sua vez, devem manter registros de acesso à aplicação (endereço IP do usuário e data e hora de acesso à aplicação) por seis meses[67].

Por fim, o uso de metadados foi substancial para o sucesso de investigações de grande importância no Brasil e ao redor do mundo. Por aqui, destacam-se os casos do assassinato da juíza Patrícia Acioli, em 2011, em que os investigadores analisaram uma grande quantidade de metadados telefônicos para a identificação de seis Policiais Militares responsáveis

64 Como se verá adiante, esse ponto é uma faca de dois gumes, pois foi a facilidade na coleta e na análise de bancos de dados massivos de metadados que viabilizou também o desenvolvimento do arsenal e da vigilância da NSA, revelado por Snowden.

65 Lei n. 12.850/2013 (Lei de Organizações Criminosas), art. 17.

66 MCI, art. 13. Questiona-se, no momento, se haveria também uma obrigação de armazenamento das portas lógicas de acesso. Decisão recente do STJ aponta no sentido da existência dessa obrigação. Cf. Provedor deve fornecer porta lógica para identificar usuário acusado de atividade irregular na internet. *Portal do STJ* (3-12-2019). Disponível em: <http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Provedor-deve-fornecer-porta-logica-para-identificar-usuario-acusado-de-atividade-irregular-na-internet.aspx>. Acesso em: 31 de março de 2021.

67 MCI, art. 15.

pela comissão do crime[68]; e o assassinato da vereadora Marielle Franco e do motorista Anderson Gomes, em 2018, em que os dados de localização de telefones celulares e históricos de navegação, em conjunto com centenas de outros gigabytes de metadados, foram usados pelas autoridades para encontrar os responsáveis[69].

Metadados vêm se tornando cada vez mais essenciais para autoridades de investigação ao redor do mundo, especialmente com a popularização dos *smartphones* – o que intensificou o volume de solicitações a essas informações a grandes provedores de aplicação[70]. Na Austrália, por exemplo, o departamento do *Attorney General* apresenta relatórios anuais sobre interceptações e acesso a dados por autoridades de investigação. Entre 2016 e 2017, autoridades australianas foram autorizadas a acessar determinados metadados de comunicação 291.353 vezes[71].

5.2.2.2. Problemas: abrangência, vigilância em massa e privacidade

O poder elucidativo dos metadados é também seu maior problema: sua coleta e sua análise em massa suscitam diversas questões sobre pri-

68 Cf. Investigação de morte de juíza fecha o cerco sobre policiais acusados de crimes. *Veja* (24-8-2011). Disponível em: <https://veja.abril.com.br/brasil/investigacao-de-morte-de-juiza-fecha-o-cerco-sobre-policiais-acusados-de-crimes/>; e Justiça mantém penas de seis PMs envolvidos na morte de juíza no Rio. *Folha de S. Paulo* (5-10-2016). Disponível em: <https://www1.folha.uol.com.br/cotidiano/2016/10/1820061-justica-mantem-penas-de-seis-pms-envolvidos-na-morte-de-juiza-no-rio.shtml>. Acesso em: 31 de março de 2021.

69 PADRÃO, Marcio. Caso Marielle: como celulares levaram a acusados e por que isso é um avanço. *UOL-Tilt* (13-3-2019). Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/03/13/como-os-celulares-ajudaram-a-achar-o-assassino-de-marielle-franco.htm>. Acesso em: 31 de março de 2021.

70 <https://techcrunch.com/2018/03/18/report-police-are-increasingly-asking-google-for-area-based-user-data-to-solve-crimes/>.

71 A definição estabelecida pelo sistema australiano inclui aqui "subscriber data" e "traffic data": "'subscriber data' (...) includes information identifying the user of a telecommunications service. (...) 'traffic data' (...) include information such as the time, duration, and source of a communication". Cf. AUSTRALIAN GOVERNMENT. DEPARMENT OF HOME AFFAIRS. Telecommunications (Interception and Access) Act of 1979 Annual Report 2018-19, p. 71. Disponível em: <https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-18-19.pdf>. Acesso em: 31 de março de 2021.

vacidade e vigilância[72]. Todas as vantagens apresentadas (disponibilidade, estruturação e facilidade de processamento) viabilizam a elaboração de um mapeamento comportamental detalhado dos indivíduos, sem qualquer necessidade de acesso ao conteúdo de comunicações. O desenvolvimento das tecnologias de coleta e análise dessas informações permitem a formação de grandes bancos de dados e até mesmo o desenvolvimento de algoritmos preditivos de comportamentos – metadados são parte fundamental do fenômeno do *big data*[73] (BALKIN, 2018, p. 1156). Nesse cenário, alguns especialistas apontam que eles seriam mais intrusivos que o conteúdo em si, o que suscita a necessidade de mecanismos de proteção para evitar usos abusivos dessas informações (MAYER et al., 2016; GRAY, 2016; MAURUSHAT et al., 2015)[74].

Foi possível conferir na prática o potencial invasivo dos metadados: o programa PRISM da NSA, um dos alvos principais das revelações de Snowden, envolvia a coleta massiva de metadados de comunicações telefônicas e via Internet para realização de atividades de vigilância em

72 O tópico é incrivelmente complexo e possui lugar de destaque nos Estudos de Vigilância (*Surveillance Studies*), uma crescente área de pesquisa interdisciplinar que se dedica a "compreender as formas cada vez mais dinâmicas de coleta, armazenamento, transmissão, verificação e utilização de informações como meio de influenciar e gerir pessoas e populações" (LYON, 2002, p. 1). Está fora do escopo deste livro o desenvolvimento de um estudo aprofundado sobre essas questões específicas. Sobre Estudos de Vigilância de forma geral, cf. LYON, David. *Surveillance studies*: An overview. Polity, 2007; e MARX, Gary T. Surveillance studies. *International encyclopedia of the social & behavioral sciences*, v. 23, p. 733-741, 2015. Na América Latina, destaca-se a produção da LAVITS (Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade, em <http://lavits.org>). Sobre a importância dos metadados para vigilância e os problemas que surgem com isso, cf. LYON, David. *Surveillance after Snowden*. New Jersey: John Wiley & Sons, 2015; e SCHNEIDER, Bruce. Metadata= surveillance. *IEEE Security & Privacy*, v. 12, n. 2, 2014, p. 83-84.

73 Tratei sobre *big data* brevemente no item 3.2 *supra*.

74 Susan Landau em entrevista para a revista New Yorker. Cf. MAYER, Jane. What's the Matter with Metadata? *New Yorker* (6-6-2013). Disponível em: <https://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata>; e SCHNEIDER, Bruce. Metadata= surveillance. *IEEE Security & Privacy*, v. 12, n. 2, 2014. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6798571>. Acesso em: 31 de março de 2021.

massa[75]. Em 2004, a Agência possuía uma base de dados com mais de 85 bilhões de registros de metadados, com 125 milhões de novas informações sendo acrescentadas a cada dia[76]. Dando credibilidade a tudo isso, o ex-*General Counsel* da NSA e ex-*Assistant Secretary* do Departamento de Segurança Interna dos EUA (*Department of Homeland Security*) afirmou em 2013 que "Os metadados dizem absolutamente tudo sobre a vida das pessoas. Se você tem acesso a metadados suficientes, você realmente não precisa do conteúdo... [É] meio vergonhoso o quão previsíveis somos nós como seres humanos"[77].

O que se verifica ao redor do mundo é a ausência de regulações jurídicas específicas que tratem da coleta e uso de metadados por autoridades de investigação, ainda que, como já dito, alguns países estabeleçam a provedores a obrigação de guarda desses dados para esses fins. Alia-se a isso o fato de o termo "metadado" abranger basicamente todo e qualquer tipo de informação que não seja "conteúdo", o que torna essa situação ainda mais complicada[78].

Contextualmente, grande parte dos metadados utilizados em investigações criminais, por se referirem a indivíduos específicos, se enquadrariam na categoria de dados pessoais (*e.g.*, endereço IP e endereço MAC; emissor e destinatário de e-mails etc.). Isso evidencia a necessida-

75 Cf. ELECTRONIC FRONTIER FOUNDATION. NSA Timeline 1791–2015. Disponível em: <https://www.eff.org/nsa-spying/timeline>. Acesso em: 31 de março de 2021.

76 SZOIDRA, Paul. Leaked NSA document says metadata collection is one of agency's "most useful tools". *Business Insider* (7-12-2016). Disponível em: <https://www.businessinsider.com/nsa-document-metadata-2016-12>. Acesso em: 31 de março de 2021.

77 No original, em inglês: "Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content...[It's] sort of embarrassing how predictable we are as human beings". Cf. RUSBRIDGER, Alan. Life after Snowden: Journalists' new moral responsibility. *Columbia Journalism Review* (5-6-2015). Disponível em: <https://www.cjr.org/opinion/edward_snowden_impact.php>. Acesso em: 31 de março de 2021.

78 Nos EUA, por exemplo, a diferenciação entre "conteúdo" e "não conteúdo" dita o nível de proteção que determinada informação merece, com base no ECPA, lei de 1986. Bellovin et al. (2016) questiona até que ponto essa divisão faz sentido no contexto de comunicações online.

de de um diploma normativo que trata do uso desses dados para esses fins, nos moldes da Diretiva 2016/680 da União Europeia. Como visto no item 4.1.2.2, o Brasil não possui regulação nesse sentido, o que é um entrave para a efetivação da exploração dessas informações como solução menos problemática do que a restrição da criptografia.

Regulação nesse sentido não seria importante apenas para salvaguardar a privacidade e a proteção de dados de usuários investigados ou afetados pelas investigações, mas também para garantir eficácia e segurança jurídica às autoridades, deixando claro quais dados devem ser fornecidos pelos provedores e quais os procedimentos necessários para sua obtenção.

5.2.3. Um breve comentário sobre a "Internet das Coisas"

Além da onipresença dos *smartphones* e computadores pessoais, algo que sustentaria a existência dessa "era do ouro da vigilância" é a chamada "Internet das coisas" (majoritariamente conhecida por sua sigla em inglês, "IoT", de *Internet of things*). Trata-se de um termo genérico para se referir um ecossistema de dispositivos e sensores conectados à Internet (que não se restringem a computadores pessoais e *smartphones*) que interagem com usuários e comunicam-se entre si. Muitos desses dispositivos consistem em objetos do cotidiano (as "coisas" da expressão), como *smartTVs*, geladeiras inteligentes, assistentes virtuais, câmeras de segurança inteligentes, *smartwatches* etc. (XIA et al., 2012, p. 1101).

Essa conexão e integração permite que os dispositivos ofereçam diversos serviços feitos sob medida para seus usuários: *smartwatches* podem fornecer desde dados relativos à atividade física (distância percorrida, monitoramento cardíaco etc.), até conexão direta com *smartphones* (notificações sobre recebimento de e-mails e mensagens); câmeras de segurança permitem que usuários acessem suas imagens via *streaming* remotamente; assistentes virtuais (Amazon Alexa, Google Home) viabilizam um controle centralizado, por meio de comandos de voz, de funcionalidades do lar, como controle de aparelhos de som, da luz e termostatos. Esses objetos costumam ser chamados de "dispositivos inteligentes".

Por estarem em constante comunicação via Internet, gerando enormes quantidades de dados e metadados, esses dispositivos podem ser ricas fontes de informações para autoridades de investigação, permitindo traçar comportamentos e atividades de investigados de forma incrivelmente detalhada. Como boa parte desses serviços exige que os dados sejam comunicados aos provedores para seu funcionamento (*e.g.*, assistentes virtuais e câmeras de segurança inteligentes), a sua solicitação às empresas responsáveis é viável e seu fornecimento é possível tecnicamente. No debate sobre regulação da criptografia, a alternativa da Internet das coisas aparece diversas vezes (BERKMAN KLEIN CENTER, 2016, p. 15; KUEHN; MCCONNELL, 2018, p. 24 e 40; PFEFFERKORN, 2018, p. 13; PELL, 2016, p. 629).

Algo que se mostra com bastante frequência em relação a dispositivos da IoT são seus problemas de segurança. Nos últimos anos, vêm sendo reportadas invasões a assistentes virtuais[79], a câmeras de segurança inteligentes[80], a brinquedos inteligentes[81] e até mesmo o uso de dispositivos conectados para a realização de ataques DDoS[82]. Essas falhas podem ser explicadas por fatores como a ausência de padrões e diretrizes de segurança para o desenvolvimento dos dispositivos, dificuldades na atualização de software e firmware, entre outros[83].

---

79 Cf. GREENBERG, Andy. Hackers Found a (Not-So-Easy) Way to Make the Amazon Echo a Spy Bug. *Wired* (8-12-2018). Disponível em: <https://www.wired.com/story/hackers-turn-amazon-echo-into-spy-bug/>. Acesso em: 31 de março de 2021.

80 Cf. SACKS, Brianna. An 8-Year-Old Girl Had A Terrifying Exchange With A Stranger After He Hacked Her Family's Ring Camera. *BuzzFeed News* (13-12-2019). Disponível em: <https://www.buzzfeednews.com/article/briannasacks/ring-camera-hack-stranger-speaks-to-girl>. Acesso em: 31 de março de 2021.

81 Cf. FRENKEL, Sheera. A Cute toy just brought a hacker into your home. *The New York Times* (21-12-2017). Disponível em: <https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html>. Acesso em: 31 de março de 2021.

82 Cf. OLSHANKY, Steve; WILTON, Robin. Internet of Things Devices as a DDoS Vector. *Internet Society* (11-4-2019). Disponível em: <https://www.internetsociety.org/blog/2019/04/internet-of-things-devices-as-a-ddos-vector/>. Acesso em: 31 de março de 2021.

83 Cf. ILASCU, Ionut. You Ask We Answer 5. Why Is IoT Insecure? *BitDefender* (15-5-2019). Disponível em: <https://www.bitdefender.com/box/blog/iot-news/why-is-iot-insecure/>. Acesso em: 31 de março de 2021.

A insegurança desses sistemas tem o potencial de ser um prato cheio para as autoridades, que podem explorar suas vulnerabilidades para acesso aos dados, às custas da privacidade de usuários e da possibilidade da exploração dos mesmos mecanismos por criminosos[84]. Contudo, a tendência é que, conforme esses dispositivos sejam adotados em massa e se tornem cada vez mais essenciais – ao lado da constante exposição dos problemas de segurança na mídia –, as empresas concentrem seus esforços na segurança da informação.

Em relação à eficácia da IoT como fonte de dados para investigações no Brasil, é preciso considerar que a adoção desses dispositivos não é tão disseminada quanto nos EUA e na União Europeia – onde a maior parte dos relatórios e trabalhos acadêmicos sobre o debate da regulação da criptografia são desenvolvidos. Muitos desses aparelhos são caros ou indisponíveis por aqui, ainda que o mercado nacional esteja em constante crescimento[85]. Trata-se de uma solução que pode se tornar viável a longo prazo, dependendo totalmente da adoção dos dispositivos pelos consumidores brasileiros.

5.3. O inevitável futuro do debate: "Hacking Governamental"

Dentre todas as alternativas apresentadas por aqueles que defendem a não restrição de criptografia forte, destaca-se o chamado "hacking governamental"[86]: a exploração de vulnerabilidades preexistentes no sistema, além de outras ferramentas de *hacking*, pelas autoridades, para acessar determinadas informações contidas em dispositivos eletrônicos, no contexto de investigações criminais[87].

Defensores da modalidade sugerem-na especificamente como possível alternativa à imposição de mecanismos de acesso excepcional em sistemas criptográficos: em vez de forçar as empresas de tecnologia a inserirem vulnerabilidades em seus próprios sistemas de segurança, propõe-se focar na identificação e na exploração das falhas de segurança preexistentes (e não intencionais) nesses sistemas e, com isso, acessar os dados lá contidos (HENNESSEY, 2016; LANDAU, 2017, p. 138).

A ideia de "hacking governamental" como técnica de investigação não é nada revolucionária, sendo possível encontrar registros de sua utilização pelo governo dos EUA desde o final da década de 1990 (QUINLAN; WILSON, 2017). O seu uso pode ser identificado até mesmo nas *Crypto Wars* contemporâneas, uma vez que foi por meio de uma ferramenta de *hacking*, adquirida de terceiros, que o FBI conseguiu acessar o conteúdo do iPhone de San Bernardino e fez a agência desistir do caso Apple *vs.* FBI.

No entanto, quando ela é explorada como possível alternativa no contexto do debate sobre regulação da criptografia, diversas questões se colocam, desde sua viabilidade técnica, custos associados a sua condução e a necessidade do estabelecimento de um arcabouço jurídico que estabeleça regras, contrapesos e garantias para a atividade – algo ainda incipiente na maior parte dos ordenamentos jurídicos ao redor do mundo.

Apesar de ser uma alternativa preferível à imposição de *backdoors*, o "hacking governamental" traz um complexo conjunto de problemas e desafios regulatórios, tendo em vista possíveis impactos que sua

84 Vide item 5.3 *infra*.

85 Para uma melhor análise do cenário da Internet das coisas no Brasil, cf. MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV, 2018; e BNDES; MCTIC. Internet das Coisas: um plano de ação para o Brasil – Relatório Final do Estudo, 2018. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/d22e7598-55f5-4ed5-b9e5-543d1e5c6dec/produto-9A-relatorio-final-estudo-de-iot.pdf?MOD=AJPERES&CVID=m5WVIld>. Acesso em: 31 de março de 2021.

86 Em inglês, essa modalidade de investigação é frequentemente referida como *lawful* ou *government hacking* (em alguns casos, *law enforcement hacking*). O primeiro desafio em trazer o tópico para o debate brasileiro é a própria tradução da expressão *lawful/government hacking*: para abarcar corretamente o conceito, teríamos algo como "*hacking* autorizado por lei e conduzido para fins de investigação criminal". Para fins de simplificação, optei por utilizar "hacking governamental", a fim de adequar ao debate internacional e simplificar a leitura. Reconheço, no entanto, a limitação da tradução, uma vez que governos autoritários, de forma ilegítima, podem se utilizar de ferramentas de *hacking* para cometer abusos e violações de direitos humanos, e essa atividade também poderia ser chamada de "hacking governamental".

87 Ou para fins de inteligência nacional. De forma a manter a coerência com o debate "going dark", vamos focar exclusivamente no "hacking governamental" para fins de investigação criminal.

Carlos **Liguori**

Direito e Criptografia

Direitos Fundamentais, Segurança da Informação e os limites da regulação jurídica na tecnologia

2022

saraiva jur

A insegurança desses sistemas tem o potencial de ser um prato cheio para as autoridades, que podem explorar suas vulnerabilidades para acesso aos dados, às custas da privacidade de usuários e da possibilidade da exploração dos mesmos mecanismos por criminosos[84]. Contudo, a tendência é que, conforme esses dispositivos sejam adotados em massa e se tornem cada vez mais essenciais – ao lado da constante exposição dos problemas de segurança na mídia –, as empresas concentrem seus esforços na segurança da informação.

Em relação à eficácia da IoT como fonte de dados para investigações no Brasil, é preciso considerar que a adoção desses dispositivos não é tão disseminada quanto nos EUA e na União Europeia – onde a maior parte dos relatórios e trabalhos acadêmicos sobre o debate da regulação da criptografia são desenvolvidos. Muitos desses aparelhos são caros ou indisponíveis por aqui, ainda que o mercado nacional esteja em constante crescimento[85]. Trata-se de uma solução que pode se tornar viável a longo prazo, dependendo totalmente da adoção dos dispositivos pelos consumidores brasileiros.

5.3. O inevitável futuro do debate: "Hacking Governamental"

Dentre todas as alternativas apresentadas por aqueles que defendem a não restrição de criptografia forte, destaca-se o chamado "hacking governamental"[86]: a exploração de vulnerabilidades preexistentes no sistema, além de outras ferramentas de *hacking*, pelas autoridades, para acessar determinadas informações contidas em dispositivos eletrônicos, no contexto de investigações criminais[87].

Defensores da modalidade sugerem-na especificamente como possível alternativa à imposição de mecanismos de acesso excepcional em sistemas criptográficos: em vez de forçar as empresas de tecnologia a inserirem vulnerabilidades em seus próprios sistemas de segurança, propõe-se focar na identificação e na exploração das falhas de segurança preexistentes (e não intencionais) nesses sistemas e, com isso, acessar os dados lá contidos (HENNESSEY, 2016; LANDAU, 2017, p. 138).

A ideia de "hacking governamental" como técnica de investigação não é nada revolucionária, sendo possível encontrar registros de sua utilização pelo governo dos EUA desde o final da década de 1990 (QUINLAN; WILSON, 2017). O seu uso pode ser identificado até mesmo nas *Crypto Wars* contemporâneas, uma vez que foi por meio de uma ferramenta de *hacking*, adquirida de terceiros, que o FBI conseguiu acessar o conteúdo do iPhone de San Bernardino e fez a agência desistir do caso Apple *vs.* FBI.

No entanto, quando ela é explorada como possível alternativa no contexto do debate sobre regulação da criptografia, diversas questões se colocam, desde sua viabilidade técnica, custos associados a sua condução e a necessidade do estabelecimento de um arcabouço jurídico que estabeleça regras, contrapesos e garantias para a atividade – algo ainda incipiente na maior parte dos ordenamentos jurídicos ao redor do mundo.

Apesar de ser uma alternativa preferível à imposição de *backdoors*, o "hacking governamental" traz um complexo conjunto de problemas e desafios regulatórios, tendo em vista possíveis impactos que sua

84 Vide item 5.3 *infra*.

85 Para uma melhor análise do cenário da Internet das coisas no Brasil, cf. MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV, 2018; e BNDES; MCTIC. Internet das Coisas: um plano de ação para o Brasil – Relatório Final do Estudo, 2018. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/d22e7598-55f5-4ed5-b9e5-543d1e5c6dec/produto-9A-relatorio-final-estudo-de-iot.pdf?MOD=AJPERES&CVID=m5WVIld>. Acesso em: 31 de março de 2021.

86 Em inglês, essa modalidade de investigação é frequentemente referida como *lawful* ou *government hacking* (em alguns casos, *law enforcement hacking*). O primeiro desafio em trazer o tópico para o debate brasileiro é a própria tradução da expressão *lawful/government hacking*: para abarcar corretamente o conceito, teríamos algo como "*hacking* autorizado por lei e conduzido para fins de investigação criminal". Para fins de simplificação, optei por utilizar "hacking governamental", a fim de adequar ao debate internacional e simplificar a leitura. Reconheço, no entanto, a limitação da tradução, uma vez que governos autoritários, de forma ilegítima, podem se utilizar de ferramentas de *hacking* para cometer abusos e violações de direitos humanos, e essa atividade também poderia ser chamada de "hacking governamental".

87 Ou para fins de inteligência nacional. De forma a manter a coerência com o debate "going dark", vamos focar exclusivamente no "hacking governamental" para fins de investigação criminal.

utilização pode gerar para privacidade de usuários, segurança de sistemas e até mesmo ao próprio devido processo legal. São esses desafios que, a meu ver, deveriam estar sob os holofotes do debate contemporâneo sobre acesso a dados criptografados, visando à regulação responsável dessa modalidade de investigação que é inevitável na sociedade conectada.

Neste item, elaborarei um panorama geral dos principais desafios regulatórios do "hacking governamental", indicando também suas vantagens diante das regulações restritivas à criptografia e analisando algumas recentes legislações voltadas ao tema.

5.3.1. Vantagens do "Hacking Governamental" como alternativa ao acesso excepcional

É sempre razoável supor que desenvolvedores de software se esforçam ao máximo para que seus produtos sejam os mais seguros possíveis e funcionem do jeito que é esperado que funcionem. No entanto, assim como todo e qualquer produto da atividade humana, o código é passível de falhas, erros, bugs etc. Mais ainda, quanto maior e mais complexo o código, mais passível de falhas não intencionais ele está sujeito, por mais que melhores práticas tenham sido empregadas em seu desenvolvimento. Essas falhas sempre existirão, não há código perfeito e por isso softwares são constantemente corrigidos por meio das (muitas vezes irritantes) atualizações.

A principal ideia do "hacking governamental" é explorar justamente isto: ao invés de obrigar desenvolvedores a inserir vulnerabilidades nos seus sistemas (mecanismos de acesso excepcional/*backdoors*), as autoridades de investigação utilizariam ferramentas para explorar as vulnerabilidades não intencionais já contidas neles e assim acessar as informações que buscam.

A grande vantagem dessa modalidade de investigação, em oposição à exigência de *backdoors*, é não gerar nenhum tipo de insegurança *adicional* aos usuários de determinado sistema além daquela a qual eles estão sujeitos de qualquer jeito (ROZENSHTEIN, 2019, p. 1198). Nesse sentido:

> (...) a escolha é entre formalizar (e, portanto, restringir) a capacidade das autoridades de investigação utilizarem as vulnerabilidades de segurança preexistentes – algo que o FBI e outras autoridades já fazem quando necessário, sem grande escrutínio público ou jurídico – ou viver com essas vulnerabilidades e impor intencional e sistematicamente um conjunto de novas vulnerabilidades que, independentemente dos melhores esforços, poderão ser exploráveis por todos[88] (BELLOVIN et al., 2014, p. 5).

O "hacking governamental" foi fundamental em investigações criminais recentes em que criminosos se utilizaram de sistemas criptográficos como medida antiforense. Além do caso do iPhone de San Bernardino, o uso da técnica foi essencial para a condução de diversas operações de grande complexidade na chamada *darkweb*[89]. Ela consiste na parte não indexada da web[90], que é acessível apenas pelo sistema Tor, um mecanismo que, por meio de conexões criptografadas, viabiliza a navegação anônima na Internet[91]. Por isso, as suas páginas não são facilmente aces-

88 Tradução própria. No original, em inglês: "(...) the choice is between formalizing (and thereby constraining) the ability of law enforcement to occasionally use existing security vulnerabilities – something the FBI and other law enforcement agencies already do when necessary without much public or legal scrutiny – or living with those vulnerabilities and intentionally and systematically creating a set of predictable new vulnerabilities that despite best efforts will be exploitable by everyone".

89 "The Dark Web is a collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address. (...) the Dark Web is a collection of websites that are publicly visible, yet hide the IP addresses of the servers that run them. That means anyone can visit a Dark Web site, but it can be very difficult to figure out where they're hosted – or by whom." Cf. GREENBERG, Andy. Hacker Lexicon: What is the Dark web? *Wired* (19-11-2014). Disponível em: <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>. Acesso em: 31 de março de 2021.

90 Isso quer dizer simplesmente que as páginas que compõem a *darknet* não podem ser compiladas por mecanismos de busca como o Google.

91 De forma simplificada, o sistema Tor (The Onion Router) consiste em um software (navegador) e uma rede aberta de servidores espalhados ao redor do mundo que permitem ao usuário navegar de forma quase totalmente anônima na Internet. Sua estrutura e seu funcionamento são bastante complexos, mas basicamente estabelece-se uma conexão dotada de diversas camadas de criptografia entre o dispositivo do usuário e um dos servidores Tor espalhados ao redor do mundo. Esses mais de 7 mil servidores são mantidos principalmente por universidades, centros de pesquisa e organizações do terceiro setor. Os dados transitam de forma

síveis e a identificação dos usuários da rede é incrivelmente complexa, para não dizer impraticável (ADAMS, 2017, p. 735).

Por causa dessas características, a *darkweb* e a rede Tor são utilizadas para o bem e para o mal: tanto por usuários comuns para escapar da vigilância governamental em países autoritários quanto por criminosos, que formam comunidades para comércio de armas, drogas e redes de pedofilia. Nesse contexto, o uso de técnicas de "hacking governamental" foi essencial para o desmantelamento de websites criminosos na *darkweb* e para a identificação de seus usuários.

Em relação ao tráfico de drogas e de outros materiais ilícitos, a Operação *Onymous*, conduzida em 2014, consistiu na cooperação entre o FBI e a Interpol para derrubar e apreender responsáveis por mercados ilícitos existentes na *darkweb*, como a *Silk Road* 2.0, o *Black Market* e a *Hydra* (QUINLAN, WILSON, 2017). Vulnerabilidades na rede Tor foram utilizadas ao longo da operação para identificar atores e sistemas utilizados por esses portais[92].

segura em alguns dos servidores até chegar ao destinatário final. A partir dessa estrutura e do sistema criptográfico no trânsito, é muito difícil rastrear o endereço de IP originário do emissor. Para mais informações, cf. QUINTIN, Cooper. 7 Things You Should Know About Tor. *EFF* (1º-7-2014). Disponível em: <https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor>; KUMAR, Mohit. Warning: Critical Tor Browser Vulnerability Leaks Users' Real IP Address – Update Now. *The Hacker News* (4-11-2017). Disponível em: <https://thehackernews.com/2017/11/tor-browser-real-ip.html>; e Tor Exit Nodes located and mapped. *Hacker Target*. Disponível em: <https://hackertarget.com/tor-exit-node-visualization/>. Acesso em: 31 de março de 2021.

A rede Tor não garante o anonimato de forma perfeita, uma vez que vulnerabilidades podem ser encontradas na implementação do sistema criptográfico no navegador Tor e uma vulnerabilidade de outros tipos de dados relacionados ao uso do sistema podem levar ao usuário inicial. De qualquer jeito, esse tipo de vigilância é bastante custosa e demorada, e a ferramenta continua sendo amplamente utilizada por dissidentes, ativistas de direitos humanos e usuários que prezam por sua privacidade em regimes autoritários. A robustez do sistema torna-o consideravelmente mais lento do que uma conexão padrão à Internet, limitando um pouco sua funcionalidade para algumas atividades online.

92 Cf. GREENBERG, Andy. Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains. *Wired* (7-11-2014). Disponível em: <https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/>. Acesso em: 31 de março de 2021.

Exploração de vulnerabilidades nos websites e na própria rede Tor também foram essenciais para o desmantelamento de redes de pedofilia na rede, como nas operações Torpedo, de 2011[93], e Pacifier, de 2015[94], ambas conduzidas com sucesso por meio da cooperação de autoridades de investigação de diversos países – esta última acarretou na identificação de 185 suspeitos ao redor do mundo (LANDAU, 2017, p. 139; FINKLEA, 2017, p. 3).

O "hacking governamental" já é uma realidade na investigação criminal do século XXI e seu protagonismo tende apenas a crescer, reflexo de uma sociedade cada vez mais dependente de ferramentas digitais e com criminosos tecnologicamente experientes. Ainda que os principais exemplos sejam casos de grande complexidade, parece ser natural que o uso da modalidade se expanda. Nesse sentido, é extremamente importante apontar também a miríade de problemas que ele pode acarretar.

5.3.2. Problemas do "Hacking Governamental"

O fato de o "hacking governamental" ser preferível à imposição de mecanismos de acesso excepcional e à restrição da criptografia não afasta os problemas de sua utilização. Trata-se de uma modalidade de investigação extremamente invasiva, tanto sob a perspectiva das informações potencialmente acessíveis, quanto da segurança dos dispositivos explorados. Além disso, é extremamente complexa no que tange ao desenvolvimento, à implementação e à manutenção das ferramentas desenvolvidas para tal.

Sobre o ponto da privacidade: assim como a imposição de mecanismos de acesso excepcional, o objetivo final do "hacking governamental" é

93 BISSON, David. FBI Used Metasploit Hacking Tool in "Operation Torpedo". *Tripwire* (16-12-2014). Disponível em: <https://www.tripwire.com/state-of-security/latest-security-news/fbi-used-metasploit-hacking-tool-in-operation-torpedo/>. Acesso em: 31 de março de 2021.

94 ALFIN, Dan. Playpen' creator sentenced to 30 Years. *FBI News* (5-5-2017). Disponível em: <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years>. Acesso em: 31 de março de 2021.

garantir o acesso a informações contidas em dispositivos eletrônicos, esteja esse dispositivo sob custódia da autoridade de investigação ou acessado remotamente. Retomam-se aqui as mesmas preocupações relacionadas à privacidade e à segurança dos usuários exploradas anteriormente: ao contrário de outras formas invasivas de investigação, como a interceptação telefônica (cujo acesso se dá apenas ao conteúdo de conversas pontuais, via de regra entre apenas duas pessoas), o acesso aos dados armazenados em dispositivos via *hacking* é substancialmente mais agressivo, uma vez que boa parte da vida pessoal e profissional de cidadãos está registrada nesses aparelhos e serviços. No que tange ao conteúdo de mensagens e e-mails, há ainda a questão do acesso a registros da vida pessoal de indivíduos que não fazem parte da investigação (STEPANOVICH, 2016, p. 13; PRIVACY INTERNATIONAL, 2018, p. 6-7).

Sobre o ponto da segurança dos sistemas e dispositivos[95]: a descoberta e a exploração de vulnerabilidades preexistentes pelas autoridades não impede que elas sejam encontradas por criminosos. A depender de sua gravidade e do número de sistemas e usuários possivelmente afetados, questiona-se se haveria a necessidade de as autoridades alertarem os desenvolvedores do software sobre a existência da vulnerabilidade para que ela possa ser corrigida (HERPIG, 2018, p. 15; PRIVACY INTERNATIONAL, 2018, p. 23). Em contraposição, encontrar tais vulnerabilidades costuma ser um processo bastante trabalhoso e custoso. Como veremos de forma mais profunda no item 5.3.3.4, esta é uma das questões mais complexas e controversas do "hacking governamental".

Por fim, há ainda uma questão específica do "hacking governamental" como meio de obtenção de prova: a ausência de um arcabouço jurídico que o operacionalize em conformidade aos direitos fundamentais e ao devido processo legal. Suas características bastante particulares e seu potencial invasivo requerem o desenvolvimento de regulação jurídica específica para sua utilização. A seguir, explorarei os principais desafios a serem enfrentados para sua implementação.

95 Outras questões técnicas sobre segurança no "hacking governamental" são exploradas com detalhes em PFEFFERKORN (2018).

5.3.3. Desafios regulatórios

Identifico cinco tópicos principais que devem ser abordados em uma possível regulação jurídica do "hacking governamental": (i) a sua definição jurídica e as suas modalidades; (ii) o estabelecimento de pré-requisitos para sua autorização; (iii) o desenvolvimento e compartilhamento das ferramentas de *hacking* entre autoridades de investigação; (iv) a transparência e a divulgação das vulnerabilidades; e (v) as questões jurisdicionais.

Ao longo dos últimos anos, alguns países vêm implementando em seu ordenamento jurídico leis que tratam direta ou indiretamente de "hacking governamental". Algumas dessas leis sugerem respostas aos pontos aqui analisados. Oportunamente, farei referência a essas soluções ao longo do texto.

5.3.3.1. Definição de "Hacking Governamental" e suas modalidades

Um primeiro desafio que se coloca no debate sobre "hacking governamental" é a sua própria conceptualização. Na literatura, é possível encontrar inúmeros termos para se referir à prática: mais abrangentes, como "lawful hacking", "government hacking" e "law enforcement hacking", e mais específicos, como "network investigative techniques" (apenas para acesso a redes) e "uso de malware em investigação criminal" (restringindo a ferramenta de *hacking* ao *malware*). Optei, aqui, por utilizar o termo "hacking governamental", por ser mais popular e abrangente que os demais.

De forma ampla, *hacking* pode ser definido como "manipulação de software, dados, sistema computacional, rede ou outro dispositivo eletrônico sem a permissão ou conhecimento da pessoa ou organização responsável por ele ou por demais dispositivos afetados por essa manipulação"[96] (STEPANOVICH, 2016, p. 5). Nesse sentido, o "hacking go-

96 Tradução própria. No original, em inglês: "the manipulation of software, data, a computer system, network, or other electronic device without the permission of the person or organization responsible for that software application, data, computer system, network, or electronic device, and/or without the permission or knowledge of users of that or other software, data, computers, networks, or devices ultimately affected by the manipulation".

vernamental" consiste, no contexto de investigações criminais[97], na utilização dessas técnicas e suas respectivas ferramentas[98] para acessar dados em redes e dispositivos a partir da exploração de vulnerabilidades[99] existentes no sistema.

Regulações devem se estruturar a partir dessa definição mais abrangente, uma vez que esta não limita a atividade de *hacking* à exploração de vulnerabilidades de técnicas de software ou hardware, abrangendo também técnicas de engenharia social (*e.g.*, *phishing* ou *pretexting*), focando no acesso a dados, que é, no final das contas, seu objetivo principal.

Tomando o acesso a dados como referencial, o "hacking governamental" pode ser dividido em duas categorias principais: (i) utilização de ferramentas de *hacking* para acesso remoto a dispositivos e, consequentemente, aos dados neles armazenados (por exemplo, instalação remota de um *keylogger* para fins de monitoramento das atividades de determinado usuário); ou (ii) utilização de ferramentas de *hacking* no contexto da perícia de determinado dispositivo apreendido (por exemplo, acesso aos conteúdos de um *smartphone* criptografado, como no caso San Bernardino).

Ainda que ambas as modalidades apresentem ameaças à privacidade de usuários e segurança de redes e dispositivos, a intrusividade, o

97 E para fins de inteligência nacional. Como foge do escopo deste livro, não tratarei desse ponto em específico.

98 Utilizarei de forma genérica a expressão "**ferramenta de *hacking***" para me referir a qualquer tipo de ferramenta (software ou hardware) que viabilize: o acesso a redes e a dispositivos de terceiros sem autorização do administrador e/ou o controle das funções de administrador dessas redes e dispositivos. Busco incluir na expressão ameaças à segurança da informação, como *malware, spyware, trojans, keyloggers, rootkits, bootkits, logic bombs*, dentre outros. A diferenciação técnica dessas ameaças, ainda que relevantíssima na Ciência da Computação, foge do escopo deste livro.

99 Utilizarei, aqui, a definição de vulnerabilidade proposta por Bellovin et al. (2014, p. 22): "A vulnerability is a weakness in a system that can potentially be manipulated by an unauthorized entity to allow exposure of some aspect of the system. Vulnerabilities can be bugs (defects) in the code, such as a 'buffer overflow' or a 'use-after-free instance', or misconfigurations, such as not changing a default password or running open, unused services. Another common type of vulnerability results from not correctly limiting input text (this is also known as not sanitizing input), *e.g.*, 'SQL injection'. Alternatively, a vulnerability can be as simple as using a birth date of a loved one as a password. A vulnerability can be exploited by an attacker".

alcance e os riscos do *acesso remoto a dados* devem ser tratados com particular cautela. Essa divisão e a diferença de tratamento devem ser observadas na regulação do "hacking governamental".

5.3.3.2. Requisitos de admissibilidade

Assim como todo meio de obtenção de prova, o "hacking governamental", seja na modalidade de acesso aos dados em aparelhos apreendidos, seja no acesso a dados na forma remota, deve observar os direitos fundamentais e o devido processo legal. No contexto da sociedade da informação, intrinsicamente dependente de dispositivos digitais, faz sentido afirmar que o "hacking governamental" é uma medida muito mais invasiva que técnicas tradicionais de investigação, como a interceptação telefônica. O maior grau de invasividade gera, naturalmente, a necessidade de limitar seu escopo de aplicação e estabelecer condições para que ela só seja utilizada quando realmente necessário.

É essencial que, em futuras legislações sobre o tema, a medida seja utilizada apenas *ultima ratio*, após o esgotamento dos demais meios menos intrusivos de investigação (mesmo que eles também sejam bastante intrusivos, como a já mencionada interceptação telefônica), além, claro, de ponderações acerca da proporcionalidade do uso da medida, avaliada caso a caso.

Nesse sentido, o primeiro passo é estabelecer a necessidade de ordem judicial específica para o seu uso. Em relatório específico sobre emergentes regulações de "hacking governamental" na União Europeia, Gutheil et al. (2017, p. 47) indica a obrigatoriedade de ordem judicial na maior parte dos países analisados (França, Alemanha, Itália, Holanda e Polônia). Além disso, algumas legislações estabelecem outras medidas de contenção interessantes, como a limitação temporal do uso da medida quando na modalidade de acesso remoto a dados[100], e a necessidade de delimitar

100 A recente reforma do Código de Processo Penal alemão (*Strafprozessordnung* – StPO), de agosto de 2017, estabeleceu talvez a mais abrangente regulação jurídica do "hacking governamental". A limitação temporal encontra-se no § 100(a-g) da lei. Na França, a reforma do Código de Processo Penal (*Code de Procedure Pénal* – CPP-Fr), pela Loi n. 2016-731 de 2016, também incluiu determinados dispositivos sobre

ao máximo os alvos da investigação para concessão da ordem judicial, indicando indivíduos, dispositivos e tipos de informações/dados da forma mais precisa possível[101].

Ainda em relação às ordens judiciais, um desafio que transcende a mera regulação jurídica do tema é a qualificação de juízes e desembargadores sobre o funcionamento básico e o grau de instrusividade do "hacking governamental", de forma que estes possam decidir de forma qualificada.

Uma outra ferramenta de limitação, presente nas legislações alemãs[102] e francesas[103], por exemplo, é o estabelecimento de uma lista taxativa de tipos penais, baseados em sua gravidade, que autorizam o uso da técnica na investigação, de abuso de menores a terrorismo.

Esses tipos de restrições não apenas visam coibir abusos, mas também otimizar a alocação de recursos, algo que, como se verá a seguir, é um dos principais desafios da viabilização do "hacking governamental" como meio de investigação.

5.3.3.3. Desenvolvimento, aquisição e compartilhamento de ferramentas

Razoavelmente pouco analisado em estudos estadunidenses e europeus, os custos de desenvolvimento e a aquisição de ferramentas de "hacking governamental" consistem em um grande desafio para autoridades de investigação não tão bem financiadas. De um lado, as ferramentas podem ser bastante caras, como supostamente aconteceu no caso de San Bernardino, em que reportou-se que a solução custou certa de 1 milhão de dólares[104]. De outro lado, os custos desse tipo de atividade são

a medida, com a limitação estando presente nos artigos 706-102-1 e 706-102-2 (GUTHEIL et al., 2017, p. 72).

101 A necessidade de indicação específica dos alvos encontra-se no § 100(a-g) do StPO alemão, além de estar prevista também no ordenamento jurídico holandês, no recente Computer Crime III Act (*wet Computercriminaliteit III*) de 2019.

102 A lista de crimes pode ser encontrada no § 100ª (2) do StPO.

103 A lista pode ser encontrada nos artigos 706-73 e 706-73-1 do CPP-Fr.

104 Cf. YADRON, Danny. 'Worth it': FBI admits it paid $1.3m to hack into San Bernardino iPhone. *The Guardian* (21-4-2016). Disponível em: <https://www.

necessariamente recorrentes, uma vez que as vulnerabilidades exploradas são constantemente corrigidas em atualizações dos sistemas, tornando-as rapidamente inutilizáveis (NASEM, 2018, p. 73; HENNESSEY, 2016).

O preço e a facilidade de obtenção dessas ferramentas variam de acordo com o tipo e segurança do sistema que as autoridades policiais buscam acessar. Sistemas de segurança de código aberto[105] desenvolvidos com a segurança do usuário em mente, como é o caso do aplicativo Signal, costumam apresentar pouquíssimas vulnerabilidades. Isso ocorre porque o código aberto permite a realização de auditorias externas (geralmente realizadas pela comunidade do software livre e pela academia) para identificação e rápida correção de falhas de segurança.

Mesmo os sistemas de código fechado, como os aplicativos de mensagem iMessage e WhatsApp e os sistemas operacionais Windows e macOS, também passam por verificações de segurança rigorosas e constantes, uma vez que sua adoção por boa parte dos usuários torna-os frequente alvos de ataques de *hackers* maliciosos.

Exemplos dessas ferramentas mais complexas são as vulnerabilidades *zero-day*, vulnerabilidades não intencionais que são descobertas e exploradas antes do conhecimento do desenvolvedor[106]. Essas condições tornam-nas difíceis de serem encontradas, caras (caso adquiridas de terceiros) e, como mencionado anteriormente, utilizáveis temporariamente, até a devida atualização que as corrija[107].

Com isso em mente, duas questões principais podem ser colocadas: como essas ferramentas serão adquiridas e quem arcará com os custos de pesquisa e desenvolvimento delas?

theguardian.com/technology/2016/apr/21/fbi-apple-iphone-hack-san-bernardino-price-paid>. Acesso em: 31 de março de 2021.

105 Software de código aberto é aquele cujo código encontra-se publicamente disponível.

106 Cf. 1.2.3.3 *supra*.

107 Parte-se, aqui, do pressuposto que os usuários frequentemente atualizem os sistemas para correção das vulnerabilidades. Caso um investigado não o faça, por alguma razão, a vulnerabilidade ainda poderá será utilizada pela autoridade de investigação.

Sobre a aquisição de ferramentas, podemos elencar três possibilidades principais (FINKLEA, 2017, p. 9): (i) utilização de vulnerabilidades encontradas em bancos de dados públicos; (ii) desenvolvimento de ferramentas pelas próprias autoridades; e (iii) aquisição das ferramentas de terceiros.

(i) Utilização de vulnerabilidades encontradas em bancos de dados públicos, como a *National Vulnerabilities Database*[108] e o *Metasploit Project*[109]. É natural que a maior parte das vulnerabilidades disponíveis nesses bancos de dados já tenham sido corrigidas em atualizações do sistema, mas elas ainda são úteis caso o usuário investigado não tenha instalado a atualização – algo que costuma ser bastante recorrente.

(ii) Desenvolvimento das ferramentas internamente, realizado pelas próprias autoridades de investigação. Em teoria, trata-se do cenário ideal, uma vez que isso garante maior controle sobre seu funcionamento, sua disponibilidade e sua aplicação.

No entanto, ao contrário dos tradicionais grampos telefônicos, que envolvem um número limitado de tecnologias e agentes (uma vez que os grampos são realizados dentro da infraestrutura dos provedores de serviços de telefonia), o "hacking governamental" pode envolver uma multiplicidade de softwares, hardwares e sistemas de segurança. As soluções de "hacking governamental" tendem a ser feitas sob medida para seu alvo.

Além disso, o custo do desenvolvimento é contínuo, uma vez que as ferramentas de *hacking* podem se tornar inúteis após a vulnerabilidade explorada ser encontrada e corrigida pelo fornecedor. Essa necessidade de investimento recorrente pode ser uma barreira para países mais pobres.

(iii) Aquisição de ferramentas desenvolvidas por terceiros. Superam-se, nesse caso, os custos e o tempo para desenvolvimento e a falta de

108 Banco de vulnerabilidades públicas administrado pelo NIST: <https://nvd.nist.gov/vuln>. Acesso em: 31 de março de 2021.

109 Plataforma/banco de dados sobre vulnerabilidades de sistemas; fornece ferramentas geralmente utilizadas para testes de segurança: <https://www.metasploit.com/>. Acesso em: 31 de março de 2021.

capacidade técnica, adquirindo uma solução sob medida para o sistema-alvo da investigação. Desvantagens incluem, como tratado no item 5.3.2, o fortalecimento de um mercado dessas ferramentas (PFEFFERKORN, 2018, p. 5) e um desestímulo geral à divulgação de vulnerabilidades – para que divulgar ao administrador do sistema se ela pode ser vendida às autoridades? (BELLOVIN et al., 2014, p. 47).

Ademais, pode-se levantar também algumas questões éticas da aquisição dessas ferramentas com determinadas empresas: gigantes do ramo, como a italiana *Hacking Team* e a israelense *NSO Group*, têm histórico de negociação com governos autoritários, que se utilizam dessas ferramentas para cometer graves violações a direitos humanos[110].

Finalmente, outra questão relacionada ao desenvolvimento e à aquisição das ferramentas refere-se ao seu compartilhamento de forma segura entre autoridades de investigação nacionais e locais, além da devida capacitação técnica de agentes acerca de sua utilização. Tudo isso é necessário para garantir a eficácia da medida em todas as esferas das forças policiais (ROZENSHTEIN, 2019, p. 1201).

5.3.3.4. Transparência e Divulgação de vulnerabilidades

O ponto mais controverso na incipiente literatura sobre "hacking governamental" refere-se à necessidade ou não de divulgação das vulnerabilidades exploradas pelas autoridades aos fornecedores dos softwares ou hardwares afetados e como essa divulgação deve ser conduzida.

De um lado, a não divulgação da vulnerabilidade pode gerar consequências desastrosas para os usuários do sistema afetado, uma vez que a mera existência dessas vulnerabilidades possibilita que elas sejam

110 Sobre a utilização de *spyware* da NSO Group pelo governo da Arábia Saudita, ver: MARCZAK, Bill et al. The Kingdom Came to Canada How Saudi-Linked Digital Espionage Reached Canadian Soil. *The Citizenlab* (1º-10-2018). Disponível em: <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>; sobre negociações entre o *Hacking Team* e governos da Síria, Bahrein e Turquia, ver: CURRIER, Cora; BOIRE, Morgan. A Detailed Look at Hacking Team's Emails About Its Repressive Clients. *The Intercept* (7-7-2015). Disponível em: <https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/>. Acesso em: 31 de março de 2021.

encontradas e exploradas por criminosos. Além disso, há ainda o perigo de criminosos acessarem toda a base de dados de vulnerabilidades não divulgadas sob a guarda das autoridades de investigação. A depender do seu alcance (quais sistemas atinge) e severidade (que tipo de acesso/controle ela viabiliza), as consequências de um vazamento podem ser desastrosas (ROZENSHTEIN, 2019, p. 1208; NASEM, 2018, p. 72).

Um caso recente ilustra muito bem o nível que o problema pode chegar: no início de 2017, um grupo de cibercriminosos autointitulado "The Shadow Brokers" publicou na Internet uma série de arquivos secretos da NSA relacionados às suas atividades de vigilância cibernética. A publicação incluía diversas vulnerabilidades (incluindo *zero-days*) utilizadas pela Agência para tal. Uma delas, apelidada de "EternalBlue", era utilizada para invasão de diversos sistemas operacionais Windows (Vista, 7, 8 e 10). Ainda que tenha sido corrigida pela Microsoft em atualizações posteriores desses sistemas, a vulnerabilidade vazada foi utilizada para disseminar o *ransomware* Wannacry[111], que se proliferou em dezenas de países, afetando hospitais, empresas e até mesmo o Tribunal de Justiça de São Paulo ao longo de 2017[112]. Posteriormente, a mesma vulnerabilidade foi utilizada para o desenvolvimento e a disseminação de um *ransomware* ainda mais potente, o NotPetya, que afetou redes e plataformas públicas e privadas na Ucrânia, na França, na Alemanha, na Rússia, no Reino Unido, dentre outros países[113].

De outro lado, a divulgação de vulnerabilidades pode torná-las descartáveis para as autoridades de investigação, uma vez que é natural

111 Cf. BARRETT, Brian. The Encryption Debate Should End Right Now. *Wired* (jun./2017). Disponível em: <https://www.wired.com/story/encryption-backdoors-shadow-brokers-vault-7-wannacry/>. Acesso em: 31 de março de 2021.

112 Cf. Ciberataque faz sistema do Tribunal de Justiça de SP cair; sites do MP e do TRT também saem do ar. *G1* (mai./2017). Disponível em: <https://g1.globo.com/sao-paulo/noticia/sites-do-governo-de-sp-do-tj-e-do-mp-saem-do-ar-apos-ciberataques-em-larga-escala.ghtml>. Acesso em: 31 de março de 2021.

113 Cf. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired* (22-8-2018). Disponível em: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. Acesso em: 31 de março de 2021.

que os fornecedores a corrijam em atualizações subsequentes do sistema[114]. Nesse sentido, caso as autoridades precisem acessar o sistema novamente, elas precisariam encontrar e explorar uma nova vulnerabilidade. Naturalmente, reincidem-se aqui os custos de aquisição/desenvolvimento das ferramentas, algo explorado no item anterior (HENNESSEY, 2016; ROZENSHTEIN, 2019, p. 1209).

Devido aos diversos tipos de vulnerabilidades, seu alcance, seus efeitos e seus impactos, não acredito que uma única solução regulatória possa resolver a questão da divulgação. Conforme sugerido em trabalhos anteriores (LIGUORI, 2020 e LI et al., 2018), acrescentado soluções propostas por Pell e Finochiaro (2017, p. 1565-1568), sugiro que o procedimento deve se pautar com base em quatro considerações:

1. Impacto da vulnerabilidade

Para responder à primeira e principal questão, *se* a vulnerabilidade deve ser divulgada ou não, deve-se avaliar uma série de questões técnicas. Pell e Finochiaro (2017, p. 1565) sugerem avaliar o impacto da vulnerabilidade na segurança da informação a partir de quatro pontos: (i) a *prevalência* da vulnerabilidade, que consiste no número de sistemas afetados por ela; (ii) sua *densidade*, ou seja, a quantidade de informações que podem ser expostas por meio dessa vulnerabilidade; (iii) a *sensibilidade* dessas informações, avaliando seu conteúdo, usuários e setores afetados; e (iv) a *severidade* da vulnerabilidade, que leva em consideração questões técnicas de sua utilização, como facilidade de exploração, privilégios administrativos garantidos por ela, complexidade de ataques, entre outros.

Esse primeiro ponto é exclusivamente técnico, fugindo do escopo deste livro dissertar sobre a melhor forma de sua condução.

2. Momento da divulgação

Superada a primeira questão, é necessário definir em que momento a vulnerabilidade deve ser divulgada. Deve-se aguardar o fim do pro-

114 Vale ressaltar que a vulnerabilidade só será de fato inutilizável caso, além da correção realizada pelo fornecedor, o usuário investigado também atualize o sistema. Isso nem sempre é o caso, como os *ransomwares* WannaCry e NotPetya claramente demonstraram.

cesso como um todo, o fim da investigação criminal ou ela já deve ser divulgada logo após a obtenção dos meios de prova? Caso a vulnerabilidade esteja sendo usada para obtenção de meios de prova em investigações concomitantes, deve-se aguardar o fim de todas elas? Quais outros fatores devem ser levados em consideração?

3. Partes informadas

É importante que a divulgação seja feita ao fornecedor do software/hardware onde a vulnerabilidade foi encontrada, mas é necessário informar também outras partes afetadas, especialmente os usuários dos sistemas explorados. Não proponho, obviamente, divulgar aos usuários o funcionamento da vulnerabilidade, mas apenas informar sua existência e a necessidade de atualização do sistema.

A forma de divulgação aos usuários é importante porque, dependendo do que exatamente é revelado, criminosos podem ser capazes de identificar o funcionamento interno da vulnerabilidade e utilizá-la para invadir sistemas desatualizados. Esforços para conscientizar os usuários sobre a importância das atualizações de software por razões de segurança são obrigatórios; caso contrário, tanto o rigoroso processo de divulgação de vulnerabilidades pelas autoridades quanto as correções feitas pelo fornecedor podem se tornar inúteis na prática.

4. Forma de divulgação

Por fim, muito cuidado deve ser empreendido na forma da divulgação da vulnerabilidade ao fornecedor, de maneira que esta ocorra com segurança, sem que criminosos possam ter acesso a ela antes que o fornecedor tenha a oportunidade de corrigir o sistema em nova atualização.

Questões de transparência e divulgação de vulnerabilidades vêm sendo abordadas em emergentes regulações de "hacking governamental" ao redor do mundo. Na **Alemanha**, em relação à transparência às partes afetadas na investigação, a recente reforma no Código de Processo Penal alemão (StPO) incluiu dois mecanismos relevantes: o primeiro[115] refere-se à necessidade de informar as partes afetadas pela investigação (investigados e terceiros) no instante em que a divulgação não afete a sua condução (GUTHEIL et al., 2017, p. 80).

O segundo mecanismo consiste na obrigação das autoridades de investigação elaborarem relatórios de transparência sobre a utilização de técnicas de "hacking governamental" para o Departamento Federal de Justiça (*Bundesamt für Justiz*)[116]. O relatório deve conter, dentre outras coisas: (i) o número de investigações em que o "hacking governamental" foi usado para obtenção de informações; (iii) o número de ordens judiciais autorizando o procedimento; (iii) a descrição dos meios utilizados na investigação (leia-se: as ferramentas de *hacking*); (iv) a descrição dos sistemas/redes afetados e o que foi feito neles; (v) o tipo criminal que ensejou a autorização da medida; e (vi) as informações sobre os tipos de dados coletados na investigação (HERPIG, 2018, p. 12; GUTHEIL et al., 2017, p. 80; LIGUORI, 2020, p. 329). Não há na Alemanha, ainda, nenhum tipo de regulação específica para divulgação de vulnerabilidades aos fornecedores.

Ainda que não possua nenhuma lei que trate especificamente de "hacking governamental", os **Estados Unidos** possuem um mecanismo bastante interessante de avaliação de divulgação de vulnerabilidades, trata-se do *Vulnerabilities Equities Process* (VEP). Este é um processo de deliberação administrativo que busca determinar se vulnerabilidades utilizadas por autoridades de investigação e agências de inteligência devem ser divulgadas aos fornecedores e, caso positivo, estabelecer qual deve ser o procedimento para tal (PELL, FINOCHIARO, 2017, p. 1554). O órgão responsável por isso é a *Equities Review Board*, um fórum deliberativo composto por membros de diversas esferas do governo estadunidense[117].

115 Cf. StPO § 101 em geral.

116 Cf. StPO § 100b (6) e (7).

117 A *Equities Review Board* é composta por membros dos seguintes órgãos: Departamento de Justiça, Departamento do Tesouro, Departamento de Estado, Departamento de Segurança Nacional, CIA, Departamento de Defesa, Departamento de Energia, Departamento de Comércio e o Escritório do Diretor de Inteligência Nacional.

Por muitos anos, a própria existência do VEP existiu sob sigilo, com confirmações sobre seu funcionamento ocorrendo apenas em 2014, após a *Electronic Frontier Foundation* ajuizar uma ação FOIA[118] contra a NSA sobre o uso de vulnerabilidades pela agência[119]. No final de 2017, após o imbróglio gerado com a divulgação do *EternalBlue* e os *ransomwares* WannaCry e NotPetya, o governo estadunidense publicou oficialmente um documento detalhando a estrutura administrativa da *Equities Review Board* e o procedimento deliberativo do VEP[120]. De forma geral, levam-se em consideração quatro pontos principais para decidir se determinada vulnerabilidade deve ser divulgada ou não: (i) seu impacto no sistema afetado e em seus usuários; (ii) sua importância operacional para as atividades de investigação e inteligência; (iii) o impacto comercial da vulnerabilidade; e (iv) riscos que a divulgação pode acarretar para relações internacionais dos EUA[121].

A existência desse tipo de procedimento é essencial na regulação das atividades de "hacking governamental", mas o VEP em específico é problemático na medida em que as suas atividades ainda ocorrem em sigilo, sem um arcabouço jurídico que estabeleça mecanismos de transparência e *accountability*. A falta deste, além das limitadas informações públicas sobre o VEP, tornam difícil avaliar se o mecanismo é, de fato, eficaz diante do que se propõe a fazer.

118 *Freedom of Information Act*. *FOIA requests* e *FOIA lawsuits* são procedimentos estadunidenses para viabilizar acesso a informações não divulgadas do governo dos EUA.

119 Informações sobre o processo: EFF *vs.* NSA, ODNI – Vulnerabilities, FOIA. Disponível em: <https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia>. Acesso em: 31 de março de 2021. O documento que resultou do ajuizamento da FOIA lawsuit e confirmou a existência do VEP pode ser encontrado aqui: <https://www.eff.org/document/vulnerabilities-equities-process-january-2016>. Acesso em: 31 de março de 2021.

120 WHITE HOUSE. Vulnerabilities Equities Policy and Process for the United States Government, November 15, 2017. Disponível em: <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External - Unclassified VEP Charter FINAL.PDF>. Acesso em: 31 de março de 2021.

121 Uma lista razoavelmente detalhada dos critérios levados em consideração no VEP pode ser encontrada no Anexo B do documento mencionado na nota anterior.

5.3.3.5. Jurisdição e outras questões relevantes

A questão jurisdicional[122] está especificamente relacionada à modalidade de "hacking governamental" de acesso remoto a dados: e se uma rede ou dispositivo-alvo estiver localizado fora da jurisdição onde o *hacking* foi autorizado? A estrutura transnacional da Internet, juntamente com a popularidade dos serviços em nuvem (cujos servidores estão espalhados por todo o mundo), uso de VPNs e uso da rede Tor evidenciam o problema jurisdicional.

Todo esse ecossistema exige, na esfera nacional, o estreitamento das relações entre autoridades de investigação a nível estadual e federal, e, na esfera transnacional, um aprimoramento dos tratados internacionais sobre cooperação entre autoridades de investigação, para que os esforços locais de "hacking governamental" sejam eficazes.

Por fim, vale ainda mencionar uma questão exclusivamente técnica, mas que deve ser impreterivelmente enfrentada na condução do "hacking governamental": uma vez que determinadas ferramentas podem garantir ao invasor certos privilégios administrativos do sistema – como a possibilidade de alteração das informações lá contidas –, é preciso garantir que eventuais meios de prova colhidos não tenham sido alterados pelas autoridades. Vale apontar que cientistas da computação têm se debruçado sobre essa questão específica[123].

122 Questões jurisdicionais na Internet, não apenas em relação a investigações criminais, são incrivelmente complexas e merecem estudos de direito internacional dedicados exclusivamente a elas. Por essa razão, além de limitações temporais, este livro não tratará de forma aprofundada sobre esse ponto. Indicarei ao longo do texto, no entanto, que se trata de uma preocupação relevante. Para uma abordagem mais aprofundada da matéria em geral, ver: SVANTESSON, Dan Jerker B. *Solving the internet jurisdiction puzzle*. Oxford: Oxford University Press, 2017. Sobre jurisdição e "hacking governamental" em específico, ver GHAPPOUR, Ahmed. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. *Stanford Law Review*, v. 69, p. 1075, 2017; e KERR, Orin S.; MURPHY, Sean D. Government Hacking to Light the Dark Web: What Risks to International Relations and International Law. *Stanford Law Review Online*, v. 70, p. 58, 2017.

123 Ver, por exemplo, COSIC, Jasmin. BACA, Miroslav. Do We Have Full Control Over Integrity in Digital Evidence Life Cycle? *Proceedings of the ITI 2010 32nd Int. Conf. on Information Technology Interfaces*, 2010.

5.3.4. Emergência do tema e ausência do debate no Brasil

O "hacking governamental" é, de longe, a alternativa à imposição de mecanismos de acesso excepcional mais sugerida em trabalhos acadêmicos e *policy papers* sobre o tema[124]. No entanto, poucos deles lidam com a temática de maneira profunda, explorando suas vantagens, desvantagens e seus desafios e indicando em quais situações específicas sua utilização responderia satisfatoriamente aos anseios das autoridades de investigação no contexto do debate "going dark".

Enquanto parte dos acadêmicos e especialistas, no debate público, concentram seus esforços em denunciar os problemas da regulação restritiva de sistemas criptográficos, alguns países vêm propondo e implementando legislações sobre "hacking governamental", seja em oposição ou em adição à regulação da criptografia, sendo exemplos notáveis a França[125], a Austrália[126] e a Alemanha[127] (LIGUORI FILHO, 2020; LI et al., 2018).

---

124 Realizei, em trabalho anterior (LIGUORI FILHO, 2020), um breve levantamento de relatórios e artigos que exploram ou sugerem como solução ao debate "going dark" o "hacking governamental". São eles: HENNESSEY (2016); ROZENSHTEIN (2019); KUEHN; MCCONNELL (2018); LEWIS et al. (2017); NGUYEN (2017.); CASTRO; MCQUINN, 2016; KOOPS; KOSTA (2018); NASEM (2018). Além de ser o principal objeto de estudo em STEPANOVICH (2016), MAYER (2018), LI et al. (2018) e Herpig (2018).

125 Na França, optou-se por uma abordagem dupla, com normas tratando tanto da limitação ao uso da criptografia quanto sobre "hacking governamental". O principal diploma normativo responsável por essas alterações é a Lei 2016-731, que alterou tanto o Código Penal como o Código de Processo Penal francês. O Código Penal (artigo 434-15-2) foi alterado a fim de endurecer a norma relacionada à recusa da entrega de chaves criptográficos quando exigido por uma ordem judicial. O Código de Processo Penal foi alterado na secção 6 do Capítulo II do Título XXV do Livro IV, expandindo os poderes de investigação no que diz respeito ao acesso remoto aos dados informáticos. Ver, em geral, ACHARYA et al., 2017 e LIGUORI FILHO, 2020.

126 Na Austrália, o acesso do governo aos dados criptografados é regulamentado e o *hacking* do governo é regulado pela Lei de Telecomunicações (Interceptação e Acesso) de 1997, a Lei de Dispositivos de Vigilância de 2004 e a Lei de Crimes de 1914. Todas essas leis foram recentemente alteradas pela Telecommunications and Other Legislation Amendment (Assistência e Acesso) de 2018, que ampliou razoavelmente os poderes de investigação da lei. Cf, em geral, ACCESSNOW, 2018.

127 A Alemanha, por sua vez, optou por uma abordagem distinta em 2017: no lugar de legislar de forma restritiva ao desenvolvimento, à implementação e ao uso da criptografia, o país reformou seu ordenamento processual penal de forma a expandir

No Brasil, discussões sobre o tema são praticamente inexistentes. A medida não veio à tona no debate sobre os bloqueios do WhatsApp e a produção acadêmica sobre ela é quase nula[128]. Entretanto, recentes movimentações legislativas e judiciais têm o potencial de impactar abordagens do "hacking governamental" no país, por mais que não lidem diretamente com ele.

Na esfera judicial, uma recente decisão do STJ, o **RHC 99.735/SC**[129], de relatoria da Ministra Laurita Vaz, declarou nula uma prova obtida por meio do "espelhamento"[130] de uma conta de WhatsApp de um investigado no computador das autoridades de investigação. No acórdão, a Ministra indica que a obtenção de provas por meio do espelhamento seria um "tipo híbrido de obtenção de prova", uma vez que permite o acesso tanto às mensagens trocadas em tempo real quanto às mensagens armazenadas, afastando a possibilidade de simples analogia à interceptação telefônica ou telemática. Além disso, a Ministra aponta um outro problema do uso da técnica, a possibilidade de as autoridades interferirem no conteúdo das mensagens, seja apagando antigas ou enviando novas:

> (...) ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, no espelhamento via WhatsApp Web o investigador

---

e procedimentalizar as atividades de acesso remoto a dados (chamado no Código de Processo Penal de *online-durchsuchung*, "buscas online") e de interceptações telefônicas e telemáticas. Cf. HERPIG, 2018; LI et al., 2018.

128 Notáveis exceções são o CryptoMap (LIGUORI FILHO et al., 2018), que trabalha o "hacking governamental" como uma das alternativas à restrição da criptografia; e um artigo de opinião escrito pelos pesquisadores do InternetLab Dennys Antonialli e Jacqueline Abreu, "E Quando o Policial Vira Hacker?". Disponível em: <http://www.internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/>. Acesso em: 31 de março de 2021.

129 RECURSO EM HABEAS CORPUS 99.735. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2018/12/document.pdf>. Acesso em: 31 de março de 2021.

130 O WhatsApp fornece um serviço chamado "WhatsApp Web", no qual o usuário pode utilizar o aplicativo em um navegador web por meio de uma conexão entre seu celular e seu computador. Para conectar os dispositivos, basta escanear um "QRCode" na tela do computador. Uma vez ativa a conexão entre os dispositivos, é possível acessar, do computador, todas as mensagens de WhatsApp armazenadas no celular e até mesmo enviar e receber mensagens a contatos.

> de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma online, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura.

Ainda que não envolva o desenvolvimento ou aquisição de caras e complexas ferramentas de *hacking* com vulnerabilidades *zero-day*, a questão suscitada nesse caso é fundamentalmente uma questão de "hacking governamental" na modalidade de acesso remoto a dispositivos. O seu resultado final – acesso a conversas armazenadas e em tempo real – seria exatamente o mesmo se a conta de WhatsApp fosse acessada por meio da exploração de alguma vulnerabilidade do sistema. Nesse sentido, a decisão pode representar um marco importante para uma a ascensão do debate sobre isso no Brasil.

Na esfera legislativa, entretanto, a recente reforma no sistema processual penal brasileiro por meio do "Pacote Anticrime" (Lei n. 13.962/2019) concede ao juiz das garantias, de forma vaga, poderes para decidir sobre os requerimentos de "interceptação telefônica, do fluxo de comunicações em sistemas de informática e telemática ou de outras formas de comunicação"[131]. O texto, bastante genérico em sua última parte, pode ser interpretado de forma a viabilizar a autorização do uso de ferramentas de *hacking* nas investigações sem lidar com nenhum dos problemas levantados anteriormente.

O fato é que o "hacking governamental" já é uma realidade presente e sua importância tende apenas a crescer – lado a lado com seus problemas e desafios. De forma a evitar regulações incompletas e problemáticas, é extremamente importante que o tema tome protagonismo no debate público. O debate sobre acesso a dados criptografados em investigações só será superado quando ele puder ser desvinculado da pressão pela restrição da criptografia, e isso não será possível enquanto as soluções alternativas não estiverem sob os holofotes da discussão.

131 Art. 3º-B, XI, *a*, do Código de Processo Penal.

CAPÍTULO 6

LIÇÕES E RECOMENDAÇÕES: AVANÇANDO O DEBATE "GOING DARK"

Ao longo desta obra, teci considerações sobre abordagens regulatórias que buscaram resolver, de uma maneira ou de outra, o debate "going dark". No capítulo anterior, busquei analisar criticamente modelos regulatórios da criptografia presentes em diversos países, além de apontar para a existência de mecanismos alternativos de regulação e suas vantagens e desvantagens. O objetivo deste capítulo é, de forma compilada e sistematizada, apresentar as minhas contribuições prescritivas para o debate. Pretendo contribuir de duas formas.

A primeira contribuição, com viés mais objetivo, consiste em propor algumas orientações e sugestões, tiradas de tudo o que foi estudado aqui até agora, sobre o papel do direito na regulação da criptografia, indicando o que deve ser promovido e o que deve ser limitado. Além disso, proporei alternativas jurídicas para enfrentamento do problema a curto e longo prazos, com base no que foi estudado no Capítulo 5. A pretensão não é resolver, de maneira alguma, o debate de forma definitiva – isso exige o diálogo e participação constante dos setores público, privado, técnico, acadêmico e da sociedade civil –, mas sim de propor orientações mais concretas e objetivas com relação ao encaminhamento futuro do debate.