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.