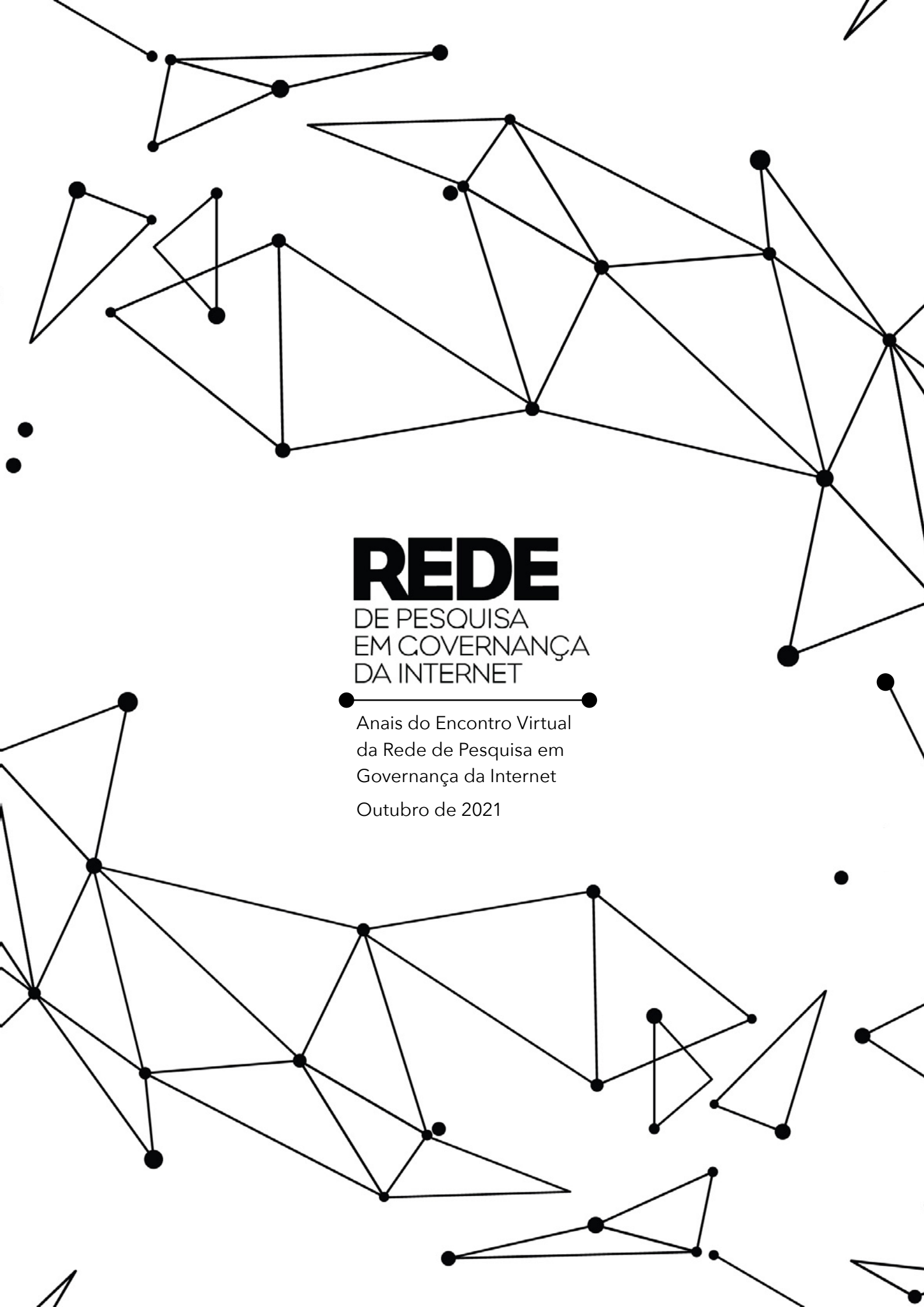

REDE
DE PESQUISA EM GOVERNANÇA DA INTERNET

Anais do Encontro Virtual da Rede de Pesquisa em Governança da Internet

Outubro de 2021

IV ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - REDE 2021

FICHA TÉCNICA

ANAIS DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET-VOL. 4, ISSN 2675-1690

Editores
Gustavo Ramos Rodrigues
Hemanuel Jhosé Veras Alves Veras
Kimberly de Aguiar Anastácio
Nathan Paschoalini Ribeiro Batista

Autores
Alexandre Arns Gonzales
André Ramiro
Carolina Fiorini Ramos Giovanini
Hemanuel Jhosé Alves Veras
João Paulo Aguiar
Luis Gustavo de Souza Azevedo
Marcos César M. Pereira
Maria Vitoria Pereira de Jesus
Mark William Datysgeld
Nathalia Sautchuk Patrício
Nathan Paschoalini Ribeiro Batista
Pedro Amaral
Sergio Marcos Carvalho de Ávila Negri

Revisores
Alexandre Arns Gonzales
Carolina Israel
Hemanuel Jhosé Alves Veras
Luis Gustavo de Souza Azevedo
Maria Vitoria Pereira de Jesus
Nathan Paschoalini Ribeiro Batista

COMITÊ ORGANIZADOR

Núcleo de Coordenação da Rede de Pesquisa em Governança da Internet
Carolina Batista Israel
Diego Jair Vicentin
Fernanda R. Rosa
Gustavo Ramos Rodrigues
Hemanuel Jhosé Alves Veras
Kimberly de Aguiar Anastácio
Maria Vitoria Pereira de Jesus
Nathan Paschoalini Ribeiro Batista

Comitê Científico
Ana Paula Camelo
Daniela Araújo
Diego Jair Vicentin
Edison Spina
Fernanda Rosa
Flávio Rech Wagner
Gills Vilar-Lopes
Jean Santos
Leonardo Ribeiro da Cruz
Lisandro Granville
Maria Mónica Arroyo
Marta Mourão Kanashiro
Olga Cavalli
Raquel Gatto
Rodolfo Avelino
Rosemary Segurado

Moderadores
Ana Paula Camelo
Ana Claudia Farranha
Flávio Rech Wagner
Leonardo Ribeiro da Cruz
Marisa von Bulow
Maria Alexandra Viegas Cortez da Cunha
Rodolfo Avelino
Rodolfo Avelino
Rosemary Segurado

Debatedores
Hemanuel Jhosé Alves Veras
Luis Gustavo de Souza Azevedo
André Ramiro
Nathalia Sautchuk Patrício
Alexandre Arns Gonzales
Carolina Giovanini
Nathan Paschoalini Ribeiro Batista
Mark William Datysgeld
João Paulo Aguiar
Maria Vitoria Pereira de Jesus

INSEGURANÇA DISTRIBUÍDA: ECONOMIA E REGULAÇÃO DO HACKING GOVERNAMENTAL

André Ramiro, Pedro Amaral e Marcos Cesar M. Pereira

SUMÁRIO

INSEGURANÇA DISTRIBUÍDA: ECONOMIA E REGULAÇÃO DO HACKING GOVERNAMENTAL

André Ramiro,[1] Pedro Amaral[2] e Marcos Cesar M. Pereira[3]

RESUMO

O *hacking* governamental assenta-se na dinâmica técnico-procedimental das agências de investigação como "estado da arte" tecnológica na produção de provas digitais e encontra terreno fértil na digitalização das dinâmicas sociais e políticas dos indivíduos. Soluções de extração de dados e ferramentas forenses para aparelhos móveis são impulsionadas como alternativas diante de uma suposta "crise" face a um *obscurecimento* das capacidades investigativas causado pelo amplo uso de criptografia forte nas comunicações. Consequentemente, ferramentas de *hacking* ganham capilaridade nas forças policiais, que alimentam o capital de um "mercado de exploração de vulnerabilidades" internacional - este com insuficientes delineamentos regulatórios no circuito comercial-investigativo-judicial brasileiro. Questões seguem descobertas, como o direito de defesa dos acusados com base nessas ferramentas; transparência e auditoria de seus códigos; as bases legais para seu uso; a arriscada manutenção de vulnerabilidades em sistemas tecnológicos; além da ética relativa aos direitos humanos, uma vez que algumas dessas soluções são comercializadas com regimes autoritários para perseguição de dissidentes e jornalistas. O cenário alimenta uma insegurança distribuída e multifacetada tendo em vista a economia alimentada por essas ferramentas, a segurança da informação do ecossistema tecnológico e os direitos fundamentais daqueles cujos dados são explorados. Busca-se, portanto, uma revisão de literatura baseada em documentos administrativos e veículos de mídia brasileiros para dimensionar o nível de implementação dessas ferramentas no Brasil; em estudos centrados em cibersegurança e direitos humanos voltados para o *hacking* governamental, a fim de apontar seus riscos ao ecossistema

[1] Diretor do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Mestre em Ciências da Computação e bacharel em Direito, ambos pela Universidade Federal de Pernambuco. Foi Google Policy Fellow na ONG Derechos Digitales (Chile, 2019).

[2] Pesquisador do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Doutorando e Mestre em Sociologia pela Universidade Federal de Pernambuco. Bacharel em Ciências Sociais pela Universidade Federal de Pernambuco e pela Universität Hamburg.

[3] Estagiário do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Graduando em Ciências Sociais - Bacharelado pela Universidade Federal de Pernambuco.

de segurança e exercício de direitos; e na legislação nacional para avaliar sua legalidade, proporcionalidade e eficácia.

PALAVRAS-CHAVE
Hacking governamental; Segurança; Exploração de vulnerabilidades; Regulação; Direitos Humanos

ABSTRACT
Government hacking is based on the technical-procedure dynamic of law enforcement agencies in the technological “state of the art” of the production of digital evidence that found fertile ground in the digitalization of social and political dynamics of individuals. Data extraction solutions and forensic devices for mobile phones are driven as alternatives because of the widespread use of strong encryption in communications. Therefore, tools of hacking gain capillarity in the law enforcement agencies, that feed the capital of an international “market of exploiting vulnerabilities” with insufficient regulatory delineations in the Brazilian commercial-investigative-judicial circuit. Issues are still uncovered, such as the right of defense of the accused with basis on these tools; maintenance of vulnerability in technological systems; besides the ethical issues in relation to human rights, once some of these solutions are commercialized with authoritarian regimes for the persecution of dissidents and journalists. The paper aims a bibliographic revision based on administrative documents and Brazilian media vehicles to scale the level of implementation of these tools in Brazil; based in studies focused on cybersecurity and human rights, oriented to governmental hacking, intending to point its risks to the ecosystem of security and the exercise of rights in the technological environment; and based on national legal grounds to assess their legality, proportionality, and effectiveness.

KEY WORDS
Government hacking; Security; Exploitation of vulnerabilities; Regulation; Human Rights

INTRODUÇÃO: PRIVACIDADE, CRIPTOGRAFIA E DESAFIOS INVESTIGATIVOS

A privacidade vem se consolidando como um padrão de mercado. A criptografia desempenha um papel central na proteção de milhões de pessoas, ainda que na maioria das vezes de forma desconhecida do grande público. Jonathan Mayer (2018) observa o curso trilhado por empresas como Apple, que adota criptografia para o armazenamento de dados em seus sistemas operacionais, uma ação que seria consequentemente acompanhada, por exemplo, na troca de mensagens do WhatsApp.

O uso da criptografia, cada vez mais comum às soluções tecnológicas, levanta duas questões aparentemente indissociáveis. Por um lado, assegura ao usuário que o conteúdo no seu aparelho ou aplicação não será acessado por terceiros em situações de normalidade. Por outro, cria-se um novo desafio para forças de segurança acessa-

rem os conteúdos trocados por possíveis “criminosos” nesses meios. A narrativa de um suposto *obscurecimento* das capacidades investigativas *(“going dark”)* passa a ser elaborada pela antiga conselheira-geral do *Federal Bureau of Investigation* (FBI) Valerie Caproni e popularizada pelo ex-diretor do FBI James Comey (2014):

> Aqueles encarregados de proteger nosso povo nem sempre são capazes de acessar a evidência necessária para investigar crimes e prevenir terrorismo mesmo com autoridade legal. Nós temos a autoridade legal de interceptar e acessar comunicações e informações de acordo com a ordem judicial, mas comumente não possuímos a habilidade técnica para fazê-la. (COMEY, 2014. Tradução nossa)

O centro dessa incapacidade técnica reside na encriptação dos dados em “movimento” e em “repouso”. Comey acredita que a disponibilidade de metadados para investigação criminal não é suficiente, pois seriam “informações incompletas” (COMEY, 2014). A narrativa será amplamente explorada e desenvolvida por outras lideranças notórias da investigação criminal nos Estados Unidos, como o Procurador-Geral, William Barr, e pelo então Vice-Procurador Geral, Rod Rosenstein, para estabelecer um imaginário de insegurança a partir de elaborações originadas na criptografia (RAMIRO, 2020).

A fim de circunscrever a criptografia, diferentes estratégias são traçadas por forças de investigação. Uma delas é um “acesso excepcional” a partir de um *backdoor*, forma de acessar o conteúdo decriptado quando assim fosse necessário, com auxílio do provedor ou intermediário, vulnerabilidade inserida propositalmente que permitiria acesso ao conteúdo. A solução é amplamente criticada pela comunidade tecnológica, considerada um regresso do desenvolvimento histórico das técnicas de segurança. Objeções e argumentos levantadas pelo artigo *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communication* (ABELSON et al., 2015) sintetizam os contrapontos e promovem um momento-chave no rechaçamento às políticas de acesso excepcional.[4]

O que se convencionou chamar de *hacking governamental* se insere como alternativa, como válvula de escape, a interferências à criptografia via obrigações aos intermediários que tornaram seus serviços mais inseguros. Através de meios tecnológicos próprios ou contratados, agências de investigação conseguiriam superar a proteção a

[4] É ampla a literatura que avalia negativamente os impactos eventualmente trazidos por políticas de acesso excepcional . Ver, por exemplo, LOUIS; ZHENG; CARTER, 2017; KHEL; WILDON; BANKSTON, 2015; ZITTRAIN et al, 2016; e RAMIRO; CANTO, 2020.

uma eventual prova encriptada sem necessidade de recorrer ao provedor (como a Apple ou o WhatsApp), habilitando novas técnicas forenses de produção de provas e vigilância. No entanto, a exploração de vulnerabilidades e os dados extraídos por tais expedientes colocam novos desafios de segurança, ao processo penal e aos direitos dos usuários.

Este trabalho, portanto, busca avaliar a inserção de ferramentas de hacking governamental no ecossistema de investigações criminais, os riscos envolvidos, as relações econômicas subjacentes e a (in)suficiência sobre as bases legais brasileiras para o uso de tais ferramentas. Será realizada, inicialmente, uma conceitualização da problemática, sua incidência no exterior e em território nacional. Buscará fornecer um perfil político-econômico de alguns dos principais atores no cenário mundial e como eles se articulam entre discursos solucionistas associados à geração inseguranças tecnológicas e legais. Para tal, foi realizada uma revisão de literatura, com base em estudos acadêmicos e de centros de pesquisa independentes, para contextualizar o fenômeno; foi feita a análise de documentos privados institucionais de empresas fornecedoras das tecnologias em questão, bem como de documentos administrativos governamentais, ambos acessíveis publicamente; e, por fim, a análise de fatos políticos, publicados em veículos de mídia, relacionando as relações entre tecnologias forenses de alto risco aos direitos com contextos políticos nacionais e internacionais.

HACKING GOVERNAMENTAL COMO SOLUÇÃO?

Com a rota do *backdoor* cada vez mais impossibilitada devido às críticas de acadêmicos, especialistas em segurança da informação e pela histórica articulação da sociedade civil contra a medida, técnicas alternativas foram se sedimentando na cultura investigativa como forma de superar a encriptação. Uma das formas disponíveis no cenário é a do hacking governamental[5], que pode ser definido como

[5] Utilizamos a categoria "hacking governamental" a fim equacionar o trabalho com o debate internacional (Stapanovich et. al, 2016; Pfefferkorn, 2018; Mayer, 2018; Internet Society, 2020; Electronic Frontier Foundation, 2021; Privacy International, 2021). A discussão ainda pode ser encontrada a partir de terminologias como *lawful hacking* ("hacking legal" ou "hacking legítimo", em tradução literal), como os trabalhos de Bellovin et al. (2014) e Liguori (2020). A título de comentário, no entanto, observa-se que o "hacking estatal" seria preferível em detrimento dos dois últimos. O Estado moderno, pode ser concebido enquanto uma instituição que possui papel de coordenar atividades sociais, além de ter aparelhos de poder públicos exclusivos, incluindo políticos, militares e polícias (Bresser-Pereira, 2017). Em versão moderna, separa-se o Estado do governante que ocupa a cadeira deliberativa, mantendo o monopólio do uso legítimo da força no território que administra (WEBER, 1982). O Governo, por sua vez, conceitualiza Rocha (2008), é, sobretudo, o grupo político que está comandando um Estado. As forças de segurança, portanto, relacionam-se mais fortemente com o conceito de Estado que de governo, ainda que, por vezes, tais aparelhos estatais sejam instrumentalizados por governos especí-

> (...) entidades governamentais (por exemplo, agências de investigação ou segurança nacional, ou mesmo atores privados em nome do Estado) explorando vulnerabilidades em sistemas, softwares, ou hardwares para ganhar acesso à informação que esteja de outra forma encriptada ou inacessível. (INTERNET SOCIETY, 2020. Tradução nossa)

Apesar da relação com o debate sobre acesso excepcional a conteúdos encriptados, o hacking governamental não surge como consequência contemporânea direta. Olhando para os Estados Unidos, Kim Zetter (2016) buscou realizar um resgate sobre operações de hacking do FBI, destacando que, em 1998, já havia registro da primeira ferramenta de hacking em uso pelo FBI, a *Carnivore*. Utilizada ao menos 25 vezes com aval dos provedores de Internet, tinha a capacidade de filtrar e copiar metadados do alvo da vigilância. A descoberta se deu em 2000, quando a empresa *Earthlink* se recusou a instalar a ferramenta na sua rede, iniciando uma batalha judicial.

O caso *Heartbleed* também ilustra a exploração de vulnerabilidades por agências do Estado: Herpig e Schwartz (2019) documentam que o *bug* permitia que o atacante do sistema tivesse acessos a informações sensíveis dos usuários, tais como senhas. Ainda que o problema tenha sido descoberto por pesquisadores e anunciado publicamente pelo Google, rumores surgiram afirmando que a *National Security Agency* (NSA) já possuía conhecimento da situação antes mesmo do anúncio. O ex-coordenador de Cibersegurança da Casa Branca, Michael Daniel, afirmou não poder ter divulgado devido ao *Vulnerabilities Equities Process (*VEP), diretriz da NSA que busca delimitar, diante de uma vulnerabilidade descoberta, se será reportada ao provedor ou mantida em sigilo para utilização pela agência para fins de inteligência. Outros países possuem ou estão em processo de construção de instrumentos semelhantes à VEP estadunidense, como Reino Unido e Alemanha (HERPIG; SCHUETZE, 2018).

Partindo da definição acima, operações de hacking podem ser efetuadas tanto remotamente, como com aparelho em mãos. Para tal caso, a cultura investigativa aponta, em larga escala, para a contratação rotineira de empresas que fabricam e/ou fornecem serviços de extração de dados do aparelho desejado - em sua grande maioria *smartphones.* Buscando avaliar a incidência de tais ferramen-

ficos a fim de seguirem suas diretrizes e interesses políticos. Dessa forma, considera-se que o uso de ferramentas hacking por partes de forças de segurança, pela qual o Estado tem como desempenha sua força, seja melhor caracterizado por “estatal” do que “governamental”.

tas nos Estados Unidos, o relatório *Mass Extraction*, da UpTurn, utiliza o termo *mobile device forensic tools* (MDFT) para caracterizá-los, sendo elas capazes de extrair e copiar dados ao se conectarem com um aparelho celular, incluindo seu desbloqueio, além de analisar, com sofisticação, potencialmente tudo que há em um *smartphone* (KOEPKE et. al, 2020). O MDFT é caracterizado como:

> MDFTs são feitos para copiar todos dados comumente encontrados em um celular. [...] inclusive dados “deletados”.
> MDFTs facilitam para o *law enforcement* analisar e procurar os dados copiados dos celulares. [...]
> Enquanto recursos de segurança como criptografia do aparelho receberam atenção pública significativa, MDFTs podem circunscrever a maioria dos recursos de segurança a fim de copiar os dados. [...] (KOEPKE et al, 2020, p.10. Tradução nossa)

Empresas conhecidas por fornecerem serviços similares são, por exemplo, a Cellebrite, MSAB, Magnet Forensics e Grayshift . Alguns desses aparelhos receberam maior destaque na mídia por suas capacidades de invasão de smartphones, como o Grayshift (BREWSTER, 2020) e Cellebrite (MARLINSPIKE, 2021).

De forma semelhante, é possível identificar uma disseminação de aparelhos MDFTs em todas as cinco regiões do Brasil. A partir da coleta de dados em portais de notícias e portais da transparência governamentais, David Leal e Yuri Felix (2020) identificam a atuação da Cellebrite e da MSAB em solo brasileiro, atestando o uso ou posse dos equipamentos em São Paulo e Minas Gerais (Sudeste), Mato Grosso (Centro-Oeste); e Rio Grande do Sul (Sul). Por meio de consultas no Portal da Transparência e notícias por parte dos autores deste trabalho, identificou-se que, pelo menos na Região Norte, os estados do Acre[6], Rondônia[7] e Roraima[8], e, no Nordeste, os estados de Alagoas[9] e de Pernambuco possuem MDFTs.

Esses aparelhos ganharam destaque na mídia pela capacidade de solucionar crimes de grande comoção pública. Recentemente, o caso de assassinato do menino Henry Borel, de 4 anos, para além da repercussão devido o teor do crime, destacou-se na imprensa o uso de aparelhos da Cellebrite pelos investigadores da

[6] Secretaria de Estado de Justiça e Segurança Pública (SEJUSP). Licitação: 2020000037/Número do processo:0819.012803.00077/2020-60

[7] Polícia Técnico-Científica/POLITEC. Processo: 0022.227692/2018-11; Polícia Civil de Rondônia Processo: 0019.341840/2018-68; Fundo de Desenvolvimento Institucional do MP/RO Processo: 201600112000713 Evento: 400091 nº Doc.: 2016OB00325;

[8] Secretaria de Estado da Segurança Pública (SESP). Admin.: 07749/2015 Licit.: 042/2015

[9] Perícia Oficial do Estado de Alagoas. CONTRATO 025/2019 PROCESSO 21020.0000000252/2018

Polícia Civil. A ferramenta foi considerada central para recuperação de mensagens apagadas do aplicativo WhatsApp e prisão de seu padrasto, o vereador Dr. Jairinho, e de sua mãe, Monique Medeiros (GUIMARÃES et al, 2021). Em Pernambuco, a Polícia Científica afirma que o uso dos aparelhos da Cellebrite ajudaram a esclarecer mais de 80% dos casos que foram encaminhados para o setor (BUARQUE, 2018). A própria Cellebrite destacou a parceria que realizou com a Polícia Federal na Operação Enterprise (JAFFE, 2021).

Do ponto de vista político, veículos de mídia destacaram a negociação do Ministério da Justiça e Segurança Pública para aquisição do *malware* Pegasus, desenvolvido pela empresa israelense NSO Group. A licitação teve envolvimento direto do filho do Presidente da República Jair Bolsonaro, Carlos Bolsonaro, o que levou à desistência do NSO Group na negociação, conforme divulgado pela matéria do UOL (VALENÇA, 2021b). O Pegasus é conhecido por infectar aparelhos por meio de mensagens, ligações e outras formas de *malwares*, possibilitando ao invasor ter acesso a todo conteúdo no aparelho de forma remota, sem o conhecimento do alvo infectado.[10] O Pegasus ficou conhecido por ser utilizado por regimes autoritários para perseguição de jornalistas, ativistas e opositores, como vem denunciando levantamentos do Citizen Lab (MARCZAK et al, 2018) e da Anistia Internacional (CALLAMARD, 2021). A solução já era conhecida por agentes da Polícia Federal no Brasil, quando foi oferecida a possibilidade de aquisição por 2,7 milhões de dólares, conforme aponta matéria no jornal O Globo. (ABBUD, 2019).

Apesar das forças de investigação repetidamente demandarem por acesso a aparelhos e serviços encriptados para solucionar crimes hediondos como terrorismo e pedofilia, há ampla difusão de MDFTs nas agências de polícia dos Estados Unidos, inclusive para repressão de infrações de baixa periculosidade, como pixação, furtos, posse de maconha e prostituição (KOEPKE et al, 2020). Além da considerável capacidade em acessar dados encriptados, contradizendo a narrativa do *obscurecimento*, seria possível apontar riscos de seletividade socioeconômica e racista que podem

[10] Note-se que seria possível fazer uma diferenciação operacional entre ferramentas de hacking *preventivo* e *repressivo*. Por exemplo, enquanto os MDFTs, descritos acima, seriam instrumentalizados no curso de investigação criminal, para a coleta de provas com o aparelho do suspeito em mãos (modelo repressivo), o Pegasus se enquadraria, em grande parte das vezes, em uma operação de vigilância pretérita à instauração oficial de investigação, como forma de monitorar agentes suspeitos (modelo preventivo).

vulnerabilizar minorias diante do uso de ferramentas de extração e acesso forçado a dados pessoais pelas forças policiais, sobretudo considerando o histórico das abordagens policial no Brasil (SINHORETTO & MORAIS, 2017).

MERCADORES DA INSEGURANÇA

O cenário desregulado do mercado de vulnerabilidades envolve, muitas vezes, ex-agentes de forças policiais e de inteligência, assim como funcionários e fornecedores de outras soluções para essas mesmas agências (KHARROUB, 2021). Isso aponta que há relações obscuras entre fornecedores de soluções de hacking e as agências estatais que as adquirem. Como forma de amostragem do mercado, destacamos três fornecedores representativos do setor de provimento de soluções de hacking para Estado: a Grayshift, a NSO Group e a Cellebrite.

Grayshift

A Grayshift, através da solução GrayKey, ganhou fama após quebrar a segurança do iOS da Apple e, desde o começo de 2021, consegue, oficialmente, o mesmo resultado para o sistema operacional Android, da Google (BREWSTER, 2021). Cada licença anual custa 10.000 mil dólares e a ferramenta seria capaz de acessar e extrair as informações em menos de um dia. Em 2018 e 2019, a agência governamental estadunidense Immigration and Customs Enforcement (ICE), cuja missão é combater o “crime transfronteiriço e imigração ilegal” - e com alguns precedentes de violações aos direitos humanos - gastou cerca de 1.2 milhões de dólares com produtos da Grayshift (BREWSTER, 2019). Em 2019, a agência foi processada pela American Civil Liberties Union e pela Electronic Frontier Foundation por ações arbitrárias, sem justificativa e sem mandado judicial (HANDEYSIDE et al, 2019). Tendo levantado 47 milhões de dólares em rodadas de financiamento (BREWSTER, 2020), foi originalmente fundada por um ex-funcionário da Endgame, outra empresa fornecedora de ferramentas de hacking para militares estadunidenses e para a NSA (GREENBERG, 2014), durante a batalha judicial entre o FBI e a Apple sobre a requisição de desbloqueio do iPhone de um dos autores do ataque terrorista em San Bernardino (BREWSTER, 2018). Desde então, a solução da Grayshift tem sido adquirida por diversas agências policiais e de inteligência nos EUA (COX, 2018), atuando em cerca de 30 países, como Reino Unido (BURGESS, 2018), por

mais de mil agências. No relatório anual de crescimento de 2021, a Graysfhit aponta 90% de crescimento de receita ano após ano, triplicação da base de funcionários desde 2020, aumento de 48% na quantidade de licenças ativas, uma taxa de 98% de renovação, bem como 107% de crescimento anual em receitas internacionais (GRAYSHIFT, 2021).

NSO Group Technologies

Nos últimos anos, o spyware Pegasus, desenvolvido pela NSO Group, tem ganhado destaque devido a sua conexão com regimes autoritários e por ter sido central para a perseguição de dissidentes políticos, ativistas e jornalistas, inclusive relacionado a casos de homicídios. Segundo seu "Transparency and Responsibility Report" (NSO GROUP, 2021), publicado em junho, a empresa fornece a 60 clientes, em 40 países, sendo 38% agências de aplicação da lei, 11% militares e 51% agências de inteligência. A contratação do Pegasus para espionar dez iPhones custava 650 mil dólares mais uma taxa de instalação de meio milhão de dólares, segundo reportagem do New York Times (PERLROTH, 2016). O lucro da NSO Group, em 2018, foi de 125 milhões de dólares, cerca de 50% do total da receita da empresa (PETERSON & GAL, 2019). NSO Group não revela oficialmente informações sobre lucro, mas informações vazadas à Business Insider indicam que 40% dos clientes são do Oriente Médio, 30% da Europa, 21% da Ásia, 5% da África, 3% da América do Sul e Caribe e 1% da América do Norte. O valor da NSO Group foi calculado em 1 bilhão de dólares, quando adquirida recentemente por dois dos co-fundadores, cujo empréstimo para compra da empresa foi marcado por negação da oferta por vários investidores devido às preocupações éticas envolvidas (REUTERS STAFF, 2019), valores que estariam sendo investidos na chamada "NSO Mafia", um conjunto de startups e subsidiárias do NSO que desenvolvem outros produtos de vigilância (PETERSON, 2019). O Pegasus, seu principal produto, tem sua exportação controlada pelo Ministério de Defesa israelense por ser considerado uma arma. Na prática, contudo, vem sendo denunciado que a cúpula do Estado israelense vem fazendo o mesmo que faz com toda sua indústria bélica: usando a exportação de armas como cartão diplomático, atraindo governos para sua órbita a partir do "brinquedo que qualquer agente de inteligência quer" (NEAL, 2021). Vale mencionar que o CEO da NSO Group, Shalev Hulio, é reservista do exército israelense.

Cellebrite

Fundada em 1999 e sediada em Israel, emprega técnicas de coleta, análise e gestão de dados de dispositivos apreendidos. Em 2021, a empresa anunciou que vai se tornar pública por meio de uma fusão, com valor estimado em 2.4 bilhões de dólares. Em 2007, a Cellebrite criou uma unidade independente focada em soluções de extração de dados de dispositivos, as MDFTs, cuja marca central é o UFED, que abriga um conjunto de produtos específicos. Uma licença da ferramenta pode custar entre 6 mil e 15 mil dólares, a depender de especificações. Segundo relatório do segundo trimestre de 2021, a receita anual recorrente da Cellebrite, que se refere a receita advinda de assinaturas por período, foi de 142 milhões de dólares, com crescimento de 42% em relação ao ano anterior (CELLEBRITE, 2021). Entre 2017 e 2019, os contratos com a já citada Immigration and Customs Enforcement (ICE) giravam em torno de 2,2 a 35 milhões de dólares. Em 2017, um hacker teve acesso a cerca de 900 GB de dados confidenciais dos servidores externos da Cellebrite (COX, 2017), com evidências que indicavam contratos de fornecimento com a Turquia, Emirados Árabes e Rússia. Em 2021, após vazamento do uso de ferramentas da Cellebrite em investigação da vida privada da líder de oposição russa, Lyubov Sobol, um ativista israelense entrou com processo na Suprema Corte de Israel contra a empresa, resultando no término do contrato com os governos da Rússia e da Bielorússia (YARON & GOICHMAN, 2021). Segundo a própria Cellebrite, a empresa fornece para mais de 6.700 agências em mais de 140 países.

Essa breve exposição de atores do mercado de hacking para Estados busca contribuir com elementos de dimensionamento de um mercado bilionário. Há diversas outras empresas fornecedoras e, dependendo de onde são baseadas, podem ou não negociar com determinados Estados. Pressão legal pode ser uma ferramenta para evitar que ferramentas ofensivas sejam disponibilizadas para regimes autoritários. No entanto, como no caso da agência estadunidense ICE, violações de direitos humanos não são exclusividades dos regimes considerados autoritários.

O estabelecimento de regulações insuficientes para contratação de ferramentas de exploração de vulnerabilidades permite a formação de mercados cujo produto é produzir ou explorar inseguranças em sistemas cada vez mais importantes (PFEFFERKORN, 2018), fatores que desenham uma auto-regulação de operações de hacking governamental sob regras da iniciativa privada. O modelo, tendo por base a expansão

comercial e o lucro, faz com que empresas dificilmente supervisionem a integridade do uso que Estados fazem de seus produtos.

Pfefferkorn (2018) aponta que o hacking governamental cria desincentivos aos governos para que comuniquem vulnerabilidades encontradas às empresas expostas, ao mesmo tempo em que podem colocar uma perspectiva ofensiva acima das medidas defensivas, permitindo que agências policiais e de inteligência façam *lobby* junto às empresas por padrões mais fracos de segurança, como já aconteceu com o *National Institute for Standards and Technology* (NIST) e o protocolo criptográfico RSA (MENN, 2014).

Se os Estados garantem uma reserva de mercado de vulnerabilidades, é possível visualizar uma contínua consolidação e expansão da atividade de exploração de brechas de segurança sem busca por correção, ou seja, vulnerabilizando usuários e sistemas e reduzindo exponencialmente os níveis de cibersegurança para uma nação ou coletividade. Somado ao franco crescimento de fraudes e megavazamentos de dados (COUTINHO, 2021; AXUR, 2021), a manutenção de vulnerabilidades abre margem a sua exploração para finalidades colaterais, enquanto a exploração por agentes do Estado segue sem regulação.

FABRICANDO INSEGURANÇA E O TECNO-SOLUCIONISMO NA CULTURA DE CONTROLE

No cenário de segurança pública, o medo e a indignação moral em relação a determinados crimes e ao terrorismo é uma ferramenta tradicional empregada por agentes de aplicação da lei. O terrorismo, a exploração sexual infantil e o crime organizado são peças centrais para exploração das moralidades e dos afetos, seja em estratégias privadas, como os “enclaves fortificados” que restringem as possibilidades de interação urbana (CALDEIRA, 2011), seja nas políticas de “lei e ordem” nas últimas décadas. Não por acaso, o medo é usado também para venda, aos Estados, de tecnologias intrusivas (DOS REIS PERÓN & OLIVEIRA PAOLIELLO, 2021).

O “pânico moral” diz respeito à percepção de que há ameaças aos fundamentos morais da sociedade (FUREDI, 2018). A referência a esses medos não é acidental: o uso de “dispositivos morais” aponta para a dimensão capacitadora e criativa da moralidade (WERNECK, 2015), aqui, a construção de estratégias de segurança, baseadas na vigilância, no controle e punição (GARLAND, 2008). A “capacidade crítica” (BOL-

TANSKI & THEVENOT, 1999) é empregada por agentes da lei contra a “impunidade e o descontrole do crime” como forma de “justificação” de políticas de vigilância.

A narrativa do obscurecimento, acima mencionada, ignora ou subestima um conjunto de questões lógicas e práticas: ganhos em segurança da informação previnem crimes, aumentando os custos e reduzindo os ganhos. Por exemplo, a encriptação por padrão dos iPhones reduziu a recompensa por furtos desses dispositivos, resultando em queda dessa prática (ETHERINGTON, 2015). Por outro lado, grupos organizados criminais frequentemente possuem rotinas e estruturas de comunicação diferentes daquelas oferecidas no mercado legal, através de fabricação própria ou por aparelhos descartáveis (MOODY, 2016; LOUIS; ZHENG; CARTER, 2017).

Enquanto pedem o enfraquecimento sistêmico da segurança digital, as agências governamentais têm mantido esforços de vigilância massiva. Nesse sentido, é importante contrastar o “obscurecimento” com as crescentes capacidades que caracterizam a “era de ouro da vigilância” (SWIRE; AHMAD, 2011): a crescente migração das atividades cotidianas para o meio digital e maior uso de diversos dispositivos digitais resulta em maior quantidade de sensores e de dados sobre indivíduos (GASSER et al, 2016).

Essas capacidades envolvem não apenas a coleta e análise de grandes quantidades de dados disponíveis publicamente, (ou “*OSINT”, open source intelligence),* mas também de dados privados acessíveis via mandados judiciais endereçados a provedores. Nos casos de informações encriptadas ou inacessíveis, a exploração de vulnerabilidades em dispositivos e aplicações surge como alternativa - muitas vezes à revelia de bases legais e enquanto fenômeno gerador de inseguranças à cadeia de usuários.

O enfraquecimento da segurança em detrimento do hacking governamental implica na exploração de vulnerabilidades que geralmente afetam pessoas não relacionadas aos crimes investigados. No caso do Ethernal Blue, por exemplo, uma vulnerabilidade explorada pela NSA foi descoberta e replicada por agentes mal intencionados, gerando danos econômicos enormes para empresas e pessoas. É necessário analisar criticamente a dinâmica “tecno-solucionista” que aumenta as capacidades de vigilância do Estado ao tentar atender as demandas práticas morais por segurança, punição e controle em detrimento de outras esferas de segurança que passam sem proteção do Estado.

DIREITOS HUMANOS SOB AMEAÇA DO HACKING GOVERNAMENTAL

O debate necessário sobre regulação do hacking governamental deve partir da preliminar desmistificação - já largamente explorada por especialistas (BELLOVIN; LANDAU, 2018; SOLOVE, 2011) - de uma suposta dualidade contraditória entre segurança e privacidade: não deveria haver conflito entre o interesse público por segurança e o interesse individual por privacidade, mas sim duas perspectivas sociopolíticas e tecnológicas distintas da segurança. As duas acepções podem ser traduzidas, respectivamente, em agendas expansivas de repressão e investigação criminal baseadas no uso de novas técnicas e na interferência tecnológica em dados e comunicações pessoais, e, de outro, uma consideração holística da governança da segurança em um ambiente crescentemente conectado.

É da natureza da vigilância e da investigação a busca pela relativização do sigilo de dados e comunicações - seja invasão, infiltração, quebra da segurança de dispositivos ou demais expedientes que visem o desvio dos sistemas de segurança - e a suspensão de direitos fundamentais em detrimento da função institucional das representações investigativas. A linha tênue garantidora de que a suspensão de direitos atende ao interesse público dependerá da observação de parâmetros como legitimidade, legalidade e proporcionalidade das ações policiais (HERPIG, 2018).

O acesso malicioso a dados e comunicações pessoais interfere na proteção à vida privada - com amplo reflexo em dados e comunicações armazenadas e trafegadas através de dispositivos pessoais. A interferência sobre o sigilo das informações em um *smartphone,* por exemplo, abre um expansivo leque para a formação de múltiplos dossiês sobre o investigado, envolvendo aplicações de mensageria, redes sociais, histórico de deslocamento, ou aplicações de relacionamento. As operações de hacking sem previsão de delimitação expressa sobre a natureza dos dados objeto de busca irão tender à arbitrariedade e à desproporcionalidade.

Como consequência direta (NYST, 2013) do efeito inibitório (*chilling effect*) causado pela mera possibilidade de vigilância por autoridades, via suspensão do sigilo a partir de técnicas de hacking, o potencial de expressão do indivíduo é silenciado, afetando o desenvolvimento de sua personalidade, como, por exemplo, aponta Hill-Collins (2002) sobre o desenvolvimento de autonomia no movimento de mulheres negras nos Estados Unidos. A dimensão política desse impacto ganha relevo se levado em consideração não somente o aspecto inibidor, mas a interferência direta, via malware, sobre

a integridade do discurso e sobre seu alcance, reprimindo a expressão e o dissenso político, por exemplo, de ativistas, jornalistas ou opositores a governamentalidades abusivas. Consequentemente, direitos políticos conexos à liberdade de expressão têm seu alcance reduzido, como de associação e de reunião.

O potencial de erosão aos direitos humanos derivados de um cenário de frágil regulação de técnicas de hacking governamental alcança também direitos processuais de eventuais investigados. Como apontam Gomes et al (2021), restrições ao amplo direito de defesa é derivação direta de casos investigativos baseados em hacking que não possibilitem, por exemplo, a auditoria independente da ferramenta por parte do réu para averiguação da integridade das provas, das evidências e de seus métodos de produção. A falta de transparência sobre os métodos de extração de dados e comunicações igualmente interferem na presunção de inocência dada a hipossuficiência informativa e técnica da defesa em produzir sua própria perícia.

Tendo por parâmetro os direitos consolidados em diplomas internacionais como a Declaração Universal dos Direitos Humano e o Pacto Internacional sobre os Direitos Civis e Políticos, Stepanovich et al (2016), detalham diferentes dimensões dos direitos humanos impactados por ferramentas de hacking, que também se associam a danos colaterais relativos à propriedade diante do comprometimento do dispositivo, às finanças diante da exploração de ativos econômicos e perda de clientes, e à reputação diante de possível vazamento de dados.

Outros dois elementos se conectam na frequência da insegurança distribuída posta em cena com a institucionalização de ferramentas de hacking: sua politização (além da *policização*) e a desconfiança da sociedade, ao mesmo tempo alimentada por históricos de abusos e falta de transparência em sua operacionalização. Efetivamente, o imaginário sociotécnico (JASANOFF, 2015) resultante de sucessivos fatos políticos que denunciam programas sigilosos de vigilância, vazamento de dados e cibercrimes (inclusive tendo Estados como agentes primários), contribuem à desconfiança distribuída da coletividade. Ilustram esses elementos, por exemplo, levantamentos realizados por entidades internacionais da sociedade civil que vêm evidenciam o estágio avançado da institucionalização do hacking governamental e a relação patente com violações direitos humanos. (MARCZAK, 2018; PRIEST; TIMBERG MEKHENNET, 2021).[11]

[11] Outros notáveis casos envolvendo brechas de segurança e uso indevido de ferramentas de hacking sob responsabilidade do Estado remontam ao Vault 7, revelado pelo WikiLeaks em 2017 e cujos de-

No campo nacional, a conjuntura política igualmente traça pontos que associam a politização e a desconfiança sobre as técnicas de hacking para explicitar as correlações entre a exploração de vulnerabilidades em dispositivos com inclinações à transgressão processual e a tendências antidemocráticas. Em 2021, o filho do presidente Jair Bolsonaro, Carlos Bolsonaro, participou ativamente de tratativas para contratar softwares de espionagem, como o Pegasus, via Ministério da Justiça, em um contrato de 25 milhões de reais (após a reportagem, a NSO Group abandonou o processo de contratação) (ALVES, 2021); em agosto, foi noticiado que Carlos Bolsonaro também tentou contratar outro software de espionagem - o Sherlock - dessa vez, tendo como potenciais alvos agentes governamentais (VALENÇA, 2021a). Tais eventos se somam a outras graves revelações sobre o monitoramento e criação de dossiês, por parte do governo federal, sobre servidores públicos opositores ao governo.

OS GARGALOS DO CENÁRIO LEGISLATIVO BRASILEIRO

Ainda que em plena operação na cultura investigativa brasileira, o conjunto normativo nacional se encontra diante de uma anacronia legislativa que não prevê, efetivamente, estrita previsão legal, balizas que limitem danos aos indivíduos e sistemas afetados, tampouco mecanismos de controle nas relações da administração pública com agentes econômicos associados ao provimento de serviços de hacking para fins processuais penais. Busca-se, portanto, um breve levantamento do mosaico legislativo atinente ao tema como forma de resgatar um ponto de partida para eventual regulação específica, apontando caminhos propositivos e críticas a dispositivos legais que mereceriam um equacionalização necessária em detrimento dos direitos constitucionais postos em risco em um cenário de hacking governamental.

Enquanto alicerce à inscrição de leis que enderecem o procedimento penal estudado, a Constituição Federal (CF) consagra no art. 5º, direitos aqui elencados e que figuram no horizonte de garantias fundamentais potencialmente afetadas: a segurança e propriedade (*caput*), a vida privada (inc. X), o sigilo dos dados e comunicações (inc. XII), a liberdade de expressão (inc. IX), a livre reunião e associação (inc. XVI e XVII) o

talhes envolvem a denúncia do arsenal de spywares da Central Intelligence Agency (CIA), capazes de acionar remotamente uma TV conectada ou interceptar mensagens e ligações de um smartphone, ou o vazamento do Ethernal Blue acima mencionado, malware da National Security Agency (NSA) vazada pelo grupo Shadow Brokers, resultando em ataques de ransomware de impacto em cadeia global como o WannaCry e o NotPetya.

devido processo (inc. LIV), ampla defesa (inc. LV) e a presunção de inocência (LVII). Adicionalmente, é preliminar a observação da base principiológica do Art. 37, notadamente os critérios de legalidade, impessoalidade, moralidade, publicidade e eficiência nos processos de contratação e licenciamento de ferramentas de exploração de vulnerabilidades por parte da administração pública. Como é notável, não se está diante de fenômeno tecnológico cuja usabilidade contemple um pleno respeito às liberdades, mas antes da possibilidade de impacto transversalmente danoso a esferas íntimas, sociais, econômicas e políticas dos indivíduos. A regulação infraconstitucional deverá partir dessas garantias na eventual recepção de operações de hacking para, então, racionalizar a possibilidade de uso excepcional desse expediente.

Estabelecido esse condicional e tomando por referência a norma do mencionado inciso XII, o legislador admitiu a regulamentação das quebras de sigilo de comunicações telefônicas, essa, por sua vez, estabelecida na Lei nº 9.296/96 (Lei de Interceptações), a qual, em diálogo com conjunto de Resoluções da Anatel, fixa bases legais e habilidades técnicas para a interceptação (ABREU, 2018). Em contrapartida, aparelhar a referida Lei para chancelar interceptação mediante software malicioso extrapolaria os parâmetros de proporcionalidade da norma, uma vez que o acesso, por exemplo, a dispositivo móvel por meio de hacking carrega um potencial de coleta de dados muito mais amplo em detrimento das comunicações em trânsito, incluindo dados armazenados e dados produzidos em tempo real de natureza distinta das comunicações (SCHERTEL, 2015), o que demandaria atualizados testes de proporcionalidade da medida e uma proteção expandida a outros direitos além da privacidade, como a propriedade e a segurança e integridade dos sistemas.

Para além da interceptação, ainda no contexto de tipologias que operações de hacking governamental poderiam lançar mão por analogia, seria possível argumentar que o uso de software malicioso por autoridade policial configuraria uma *infiltração*? A regulação da infiltração no Brasil é setorial e pode ser traçada, de início, a partir da Lei nº 11.303/06 (Lei de Drogas) e da Lei nº 12.850/13 (Lei de Organizações Criminosas)[12].

[12] Por definição, “infiltração de agentes é uma técnica especial de investigação, mediante a qual um agente, policial ou não, devidamente selecionado e treinado, e judicialmente autorizado, infiltra-se em uma organização criminosa, simulando ser um de seus integrantes, para buscar informações e reunir provas acerca de sua estrutura, funcionamento e identificação de seus reais membros, tendo por escopo apurar crimes passados e presentes, evitar crimes futuros e desmantelar referida organização (ZANELLA, 2020)

Ainda que salvaguardados, em ambas as leis, critérios de reserva de jurisdição, necessidade e proporcionalidade, nenhuma delas traz a categoria de “infiltração virtual” (ANTONIALLI; ABREU, 2017), muito menos por meio de exploração de vulnerabilidade em sistema informático ou por código malicioso - o que demandaria necessidade de releitura de riscos e de redefinições de salvaguardas diante da multiplicidade de bens jurídicos envolvidos, tanto dos investigados quanto de terceiros eventualmente afetados pelo comprometimento da segurança de sistema informático.

A categoria de infiltração virtual, no entanto, é inaugurada pela Lei nº 13.441/2017, que altera o Estatuto da Criança e do Adolescente, para reprimir crimes contra a dignidade sexual da criança e do adolescente. A previsão legal, no entanto, não garante base legal ao uso de softwares maliciosos, invasão de dispositivo ou exploração de vulnerabilidade eletrônica *para se atingir a infiltração virtual*, uma vez que haveria uma distância comportamental considerável entre o agente infiltrado dissimular sua identidade em fórum na Internet, aplicativo de relacionamento ou rede social e acionar, manipular ou operar código malicioso com a finalidade de obter acesso não autorizado a dados e comunicações armazenadas e em fluxo em determinado dispositivo. Mais uma vez, os testes de legalidade, necessidade e proporcionalidade mereceriam dedicada releitura tendo em vista os bens jurídicos em jogo.

Contemporaneamente, a Lei Geral de Proteção de Dados (nº 13.709/18) trouxe parâmetros centrais de salvaguarda às garantias fundamentais, incluídas as interfaces entre o indivíduo e o Estado. Porém, expressamente manteve fora de seu escopo as atividades de segurança pública e investigações criminais, a serem reguladas a posteriori por legislação específica (Art. 4º, III, *a* e *d*). Enquanto bússola principiológica, pré-fixou que eventual legislação deverá observar parâmetros de legalidade, necessidade, proporcionalidade, devido processo e o regime geral de proteção de dados da LGPD (Art. 4º, §1º).

Mais recentemente, uma comissão de juristas, presidida pelo Ministro do Supremo Tribunal Federal, Nefi Cordeiro, foi formada para elaborar minuta de projeto de lei que tem como escopo regular operações de tratamento de dados pessoais no contexto de investigações criminais e segurança pública, instituindo, por exemplo, princípios, direitos dos titulares e obrigações aos agentes de tratamento (SUPREMO TRIBUNAL FEDERAL, 2020). Por um lado, a proposta foi bem recebida por entidades acadêmicas e da sociedade civil especializadas em regulação de novas tecnologias (BIONI et al,

2020; LEMOS et al, 2021; REIS et al, 2021), por outro, sofreu críticas de representações de investigação criminal (URUPÁ, 2020; CONVERGÊNCIA, 2021), o que ilustra um descompasso entre a cultura investigativa e a disciplina de proteção de dados pessoais.

CONCLUSÃO

O represamento de uma regulação, tanto a nível nacional e internacional sobre o uso de tecnologias de alto risco no processo investigativo penal, incluindo o circuito de fabricação, contratação e uso de ferramentas de hacking, elevam a pressão geopolítica por respostas enérgicas ao *status* da insegurança posto. Entidades internacionais como a Relatoria Especial para Liberdade de Expressão e Opinião da ONU (UNITED NATIONS, 2019) e a Anistia Internacional (CALLAMARD, 2021) sugerem a moratória na venda e uso das tecnologias até que haja um marco regulatório suficientemente protetivo aos direitos e à segurança do ecossistema digital. Assim, os ensaios regulatórios que irão pavimentar as diretrizes legais e administrativas, deverão estabelecer os parâmetros de legalidade, necessidade e proporcionalidade às práticas, modelar procedimentos e as respostas aos usos, e seus efeitos sociais, dos softwares de hacking, atentando ao elemento social dos riscos mapeados.

Ao passo que técnicas de exploração de vulnerabilidades, intrusão e extração de dados caminham a passos largos na cultura investigativa brasileira, a literatura especializada coberta neste trabalho, aponta para o contrário: seu uso estritamente excepcional, diante de bases legais previamente consolidadas e discutidas em processos plurais e participativos. Objetivando equacionar, inclusive, a eficácia dos procedimentos investigativos, a segurança jurídica à acusação e defesa envolvidas no processo criminal e a efetiva cooperação jurídica do Brasil com agências de investigação internacionais, será preciso priorizar a tramitação de reformas regulatórias que estabeleçam regras para o tratamento de dados pessoais na esfera penal.

A desatualização regulatória põe em risco, centralmente, civis, mas, colateralmente, a própria administração pública na medida em que atrasa regras que procedimentalizem investigações mediante novas tecnologias e cria riscos de que o próprio poder público, bem com agentes econômicos, sejam alvos de incidentes de segurança envolvendo ferramentas de hacking em um cenário de cibersegurança cada vez mais globalizado e dependente de robustos protocolos de segurança. A insegurança

distribuída provocada pelo atual modelo econômico de fornecedores de ferramentas de hacking pautados pelo mercado de vulnerabilidades, em associação a política de vigilância em expansão, eloquentemente sugerem um risco iminente ao ecossistema tecnológico e de direitos humanos.

REFERÊNCIAS

ABBUD, Bruno. A chegada ao Brasil do Pegasus, estrela do submundo da espionagem. **O Globo**. Rio de Janeiro, 2019. Disponível em <https://oglobo.globo.com/epoca/brasil/a-chegada-ao-brasil-do-pegasus-estrela-do-submundo-da-espionagem-23815778 >. Acesso em: 10 set. 2021.

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

ABREU, Jacqueline. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Revista Brasileira de Políticas Públicas**, Vol 7, nº 3. 2018.

ABREU, Jacqueline; ANTONIALLI, Dennys. Vigilância sobre as comunicações no Brasil: interceptações, quebra de sigilo, infiltrações e seus limites constitucionais. InternetLab, 2017. Disponível em: <http://www.internetlab.org.br/wpcontent/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf>. Acesso em 11 set 2021.

ALVES, Sarah. Pegasus: como funciona o programa espião defendido por Carlos Bolsonaro. **Uol Notícias**, 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/05/19/pegasus-conheca-o-software-da-crise-entre-carlos-bolsonaro-e-militares.htm>. Acesso em 11 set 2021.

AXUR. Vazamentos de Dados no Brasil 2º trimestre / 2021. São Paulo, SP: AXUR, 11 ago. 2021. Disponível em: <https://conteudo.axur.com/hubfs/Report%20Q2%202021/Vazamentos%20de%20Dados%20no%20Brasil%20-%202%20trimestre%20-%20Axur%20imprensa.pdf>. Acesso em: 11 set. 2021.

BIONI et al. Proteção de dados no campo penal e na segurança pública: Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados Pessoais para segurança pública e investigação criminal. **Data Privacy Brasil,** 2020. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-T%C3%89CNICA-PROTE%C3%87%C3%83O-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURAN%C3%87A-P%C3%9ABLICA-VF-31.11.2020.pdf>. Acesso em 11 set 2021.

BELLOVIN, Steven M. et al. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. **Northwestern Journal of Technology and Intellectual Property**, Chicago, v. 12, p. 1, 2014.

BELLOVIN, Steven; LANDAU, Susan. Encryption by Default Equals National Security. **Lawfare**, 2018. Disponível em: <https://www.lawfareblog.com/encryption-default-equals-national-security>. Acesso em 11 set 2021.

BRESSER-PEREIRA, Luiz Carlos. ESTADO, ESTADO-NAÇÃO E FORMAS DE INTERMEDIAÇÃO POLÍTICA. **Lua Nova: Revista de Cultura e Política**, São Paulo p. 155-185, 2017.

BOLTANSKI, Luc; THÉVENOT, Laurent. The sociology of critical capacity. **European journal of social theory**, v. 2, n. 3, p. 359-377, 1999.

BREWSTER, Thomas. This Powerful iPhone Hacking Tool Can Now Break Into Samsung Androids. **Forbes**, Jersey City, US, 1 fev. 2021. Disponível em: <https://www.forbes.com/sites/thomasbrewster/2021/02/01/the-powerful-graykey-iphone-hacking-tool-can-now-break-into-samsung-androids/>. Acesso em: 11 set. 2021.

BREWSTER, Thomas. Immigration Cops Just Spent A Record $1 Million On The World's Most Advanced iPhone Hacking Tech. **Forbes**, Jersey City, US, 8 maio 2019. Disponível em: <https://www.forbes.com/sites/thomasbrewster/2019/05/08/immigration-just-spent-a-record-1-million-on-the-worlds-most-advanced-iphone-hacking-tech/>. Acesso em: 11 set. 2021.

BREWSTER, Thomas. Grayshift, The Startup That Breaks Into iPhones For The Feds, Raises $47 Million. **Forbes**, Jersey City, US, 26 out. 2020. Disponível em: <https://www.forbes.com/sites/thomasbrewster/2020/10/26/grayshift-the-startup-that-breaks-into-unlocked-iphones-for-the-feds-raises-47-million/>. Acesso em: 11 set. 2021.

BREWSTER, Thomas. Mysterious $15,000 'GrayKey' Promises To Unlock iPhone X For The Feds. **Forbes**, Jersey City, US, 5 mar. 2018. Disponível em: <https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/>. Acesso em: 11 set. 2021.

BUARQUE, Gabriela Castello. Dispositivo eleva solução de crimes em Pernambuco. **Folha de Pernambuco**. Recife, 2018. Disponível em: <https://www.folhape.com.br/noticias/dispositivo-eleva-solucao-de-crimes-em-pernambuco/88930/> . Acesso em: 10/09/2021.

BURGESS, Matt. UK police are buying top secret hacking tech to break into iPhones. **Wired**, Londres, UK, 19 out. 2018. Disponível em: <https://www.wired.co.uk/article/police-iphone-hacking-grayshift-graykey-uk>. Acesso em: 11 set. 2021.

CALLAMARD, Agnès. Massive data leak reveals Israeli NSO Group□s spyware used to target activists, journalists, and political leaders globally. **Anistia Internacional**, 2021. Disponível em: <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/>. Acesso em 11 set 2021.

CELLEBRITE. Cellebrite Announces Second Quarter 2021 Results. Petah Tikva, IL: CELLEBRITE, 12 ago. 2021. Disponível em: <https://investors.cellebrite.com/static-files/761a-6600-f6b4-4635-ac92-e3088d67235d>. Acesso em: 11 set. 2021.

COMEY, James B. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? **FBI**. Washington, D.C., 2014. Disponível em: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> Acesso em: 10/09/2021

CONVERGÊNCIA DIGITAL. MPF: LGPD Penal impõe restrições desproporcionais ao intercâmbio de dados. **Convergência Digital,** 2021. DIsponível em: <https://www.convergenciadigital.com.br/Seguranca/MPF%3ALGPD-Penal-impoe-restricoes-desproporcionais-ao-intercambio-de-dados-56242.html>. Acesso em: 11 set 2021.

COUTINHO, Dimítria. Ao menos oito vazamentos de dados aconteceram no Brasil em 2021; quem é punido?. **IG**, São Paulo, SP. Disponível em: <https://tecnologia.ig.com.br/2021-03-28/ao-menos-oito-vazamentos-de-dados-aconteceram-no-brasil-em-2021--quem-e-punido-.html>. Acesso em: 11 set. 2021.

COX, Joseph. Hacker Steals 900 GB of Cellebrite Data. **Vice Motherboard**, New York City, US, 12 jan. 2017. Disponível em: <https://www.vice.com/en/article/3daywj/hacker-steals-900-gb-of-cellebrite-data>. Acesso em: 11 set. 2021.

COX, Joseph. Cops Around the Country Can Now Unlock iPhones, Records Show. **Vice Motherboard**, New York City, US, 12 abril 2018. Disponível em: <https://www.vice.com/en/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police>. Acesso em: 11 set. 2021.

DOS REIS PERON, Alcides Eduardo; OLIVEIRA PAOLIELLO, Tomaz. Fear as a product, continuum as a solution: the role of private companies in the transnational diffusion of zero tolerance policing to Brazil. **Small Wars & Insurgencies**, p. 1-27, 2021.

ETHERINGTON, Darrel. Apple's Activation Lock Leads To Big Drops In Smartphone Theft Worldwide. **TechCrunch**, Bay Area, EUA, 11 fev. 2015. Disponível em: <https://techcrunch.com/2015/02/11/apples-activation-lock-leads-to-big-drops-in-smartphone-theft-worldwide/>. Acesso em 11 set. 2010.

FUREDI, Frank. **How fear works: Culture of fear in the twenty-first century**. Bloomsbury Publishing, 2018.

GASSER, Urs et al. Don't Panic: Making Progress on the" Going Dark" Debate. **Berkman Center Research Publication**, 2016.

GCHQ. The Equities Process. **GCHQ.** Cheltenham, UK, 29 novembro 2018. Disponível em: <https://www.gchq.gov.uk/information/equities-process>. Acesso em: 10 set 2021

GOMES, Ana Bárbara et al. Décalogo de Recomendações sobre Direitos Digitais e Produção de Provas. **IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife e IRIS - Instituto de Referência em Internet e Sociedade**. 2021. Disponível em: <https://obcrypto.org.br/wp-content/uploads/2021/08/Decalogo-de-recomendacoes-sobre-direitos-digitais-e-producao-de-provas-1.pdf>. Acesso em 11 set 2021.

GRAYSHIFT. Record Growth and Continued Innovation in Mobile Forensics Market. **Grayshift,** Atlanta, US, 4 maio 2021. Disponível em: <https://www.grayshift.com/news-room/record-growth-and-continued-innovation-in-mobile-forensics-market/>. Acesso em: 11 set. 2021.

GREENBERG, Andy. Inside Endgame: A Second Act For The Blackwater Of Hacking. **Forbes**, Jersey City, US, 12 fev. 2020. Disponível em: <https://www.forbes.com/sites/andy-greenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/>. Acesso em: 11 set. 2021.

GUIMARÃES, Arthur et al. Polícia prende vereador Dr. Jairinho e mãe de Henry Borel pela morte do menino. **G1**. Rio de Janeiro, 2021. Disponível em <https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/04/08/operacao-henry.ghtml>. Acesso em: 10 set. 2021.

HANDEYSIDE, Hugh; et al. We Got U.S. Border Officials to Testify Under Oath. Here's What We Found Out. **American Civil Liberties Union**, New York City, US, 30 abril 2019. Disponível em: <https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/we-got-us-border-officials-testify-under>. Acesso em: 11 set. 2021.

HERPIG, Sven. A Framework for Government Hacking in Criminal Investigations. **Stiftung Neue Verantwortung,** 2018. Disponível em: <https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf>. Acesso em 11 set 2021.

COLLINS, Patricia Hill. Black feminist thought: Knowledge, consciousness, and the politics of empowerment. **Routledge**, 2002.

JAFFE, Adam. Milhões em bens apreendidos à medida que a Polícia Federal do Brasil se dedica a desmascarar chefes do tráfico de drogas. **Cellebrite**. 2021. Disponível em: <https://www.cellebrite.com/pt/milhoes-em-bens-apreendidos-a-medida-que-a-policia-federal-do-brasil-se-dedica-a-desmascarar-chefes-do-trafico-de-drogas/>. Acesso em: 10 set. 2021

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

KARROUB, Tamara. The Full Story behind the NSO Hack: The Israeli-Military-Allied Surveillance Industry and Transnational Repression. **Arab Center Washington DC**, Washington DC, US, 28 jul. 2021. Disponível em: <https://arabcenterdc.org/resource/the-full-story-behind-the-nso-hack-the-israeli-military-allied-surveillance-industry-and-transnational-repression/>. Acesso em: 11 set. 2021.

KEHL, Danielle; WILSON, Andi; BANKSTON, Kevin. Doomed to Repeat History? Lessons from the Crypto Wars of the 1990. Washington D.C: OPEN TECHNOLOGY INSTITUTE, NEW AMERICA FOUNDATION, 2015. Pág 10. Disponível em: <https://static.newamerica.org/attachments/3407--125/Lessons%20From%20the%20Crypto%20Wars%20of%20the%201990s.882d6156dc194187a5fa51b14d55234f.pdf>. Acesso em 11 set 2021.

KOEPKE, L. et. al. Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones. Washington: UPTURN, 2020. Disponível em: <https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf> Acesso em: 10 set. 2021

LEAL, David. FELIX, Yuri. O Mercado de Dados: o caso Cellebrite e a investigação digital no Brasil. **BOLETIM DO IBCCRIM** , v. 28, p. 13-15, 2020.

LEMOS et al. Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública: Tecnologia de Reconhecimento Facial. **Instituto de Tecnologia e Sociedade**, 2021. Disponível em: <https://itsrio.org/wp-content/uploads/2021/04/UK-Comentarios_LGPDPenal.pdf>. Acesso em 11 set 2021.

LIGUORI, Carlos. Exploring Lawful Hacking as a Possible Answer to the Going Dark Debate. **Michigan Technology Law Review.** Michigan, v. 26, p. 317, 2020.

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

MARLINSPIKE, Moxie. Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective. **Signal**, San Francisco, US, 21 abr. 2021. Disponível em: <https://signal.org/blog/cellebrite-vulnerabilities/> . Acesso em: 10 set. 2021

MAYER, Jonathan. Government hacking. **Yale Law Journal**, Connecticut, v. 127, p. 570, 2017.

MENN, Joseph. Exclusive: NSA infiltrated RSA security more deeply than thought. **Reuters**, 2014. Disponível em: <https://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331>. Acesso em 11 set 2021.

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

NEAL, Louis. How Israel uses NSO spyware as a diplomatic calling card. **Financial Times**, Londres, UK, 21 jul. 2021. Disponível em: <https://www.ft.com/content/24f22b28-56d1-4d66-8f76-c9020b1b5cb1>. Acesso em: 11 set. 2021.

NSO Group. Transparency and Responsibility Report. Herzliya, IL: NSO GROUP., 30 jul. 2021. Disponível em: <https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf>. Acesso em: 11 set. 2021.

NYST, Carly. El derecho a la privacidad y a la libertad de expresión: dos caras de la misma moneda. Cuestión de Derechos**. Asociación por los Derechos Civiles**, 2013. Disponível em: <https://www.apc.org/sites/default/files/ADC%20-%20Cuestion%20de%20derechos%20-%20Revista-numero4%20-%202013.pdf>. Acesso em 11 set 2021.

PARKIN, Simon. 'Every message was copied to the police': the inside story of the most daring surveillance sting in history. **The Guardian**, Londres, UK, 11 set. 2021. Disponível em: <https://www.theguardian.com/australia-news/2021/sep/11/inside-story-most-daring--surveillance-sting-in-history>. Acesso em 11 set. 2021.

PERLROTH, Nicole. How Spy Tech Firms Let Governments See Everything on a Smartphone. **The New York Times**, New York City, US, 2 set. 2016. Disponível em: <https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html>. Acesso em: 11 set. 2021.

PETERSON, BeckyThe founders of a billion-dollar Israeli spyware startup accused of helping Saudi Arabia attack dissidents are funding a web of new companies that hack into smart speakers, routers, and other devices. **Business Insider**, New York City, US, 6 set. 2019. Disponível em: <https://www.businessinsider.com/inside-the-israel-offensive-cyber-security-world-funded-by-nso-group-2019-8>. Acesso em: 11 set. 2021.

PETERSON, Becky & GAL, Shayane. Leaked financials show Israeli spyware company NSO Group is wildly profitable despite concerns over misuse of its technology. **Business Insider**, New York City, US, 6 set. 2019. Disponível em: <https://www.businessinsider.com/nso-group-financials-show-offensive-cyber-company-is-profitable-2019-9>. Acesso em: 11 set. 2021.

PFEFFERKORN, R. Security Risks of Government Hacking. Stanford: THE CENTER OF INTERNET AND SOCIETY. 2018. Disponível em: <https://cyberlaw.stanford.edu/publications/security-risks-government-hacking> Acesso em: 10 set. 2021.

RAMIRO, André. A construção de imaginários nas narrativas governamentais sobre criptografia. **Derechos Digitales**, 2019. Disponível em: <https://www.derechosdigitales.org/wp-content/uploads/A-Construcao-de-Imaginarios-nas-Narrativas-Governamentais-sobre-Criptografia-final.pdf>. Acesso em: 11 set 2021.

REUTERS STAFF. UPDATE 1-NSO Group's management buys firm from Francisco Partners. **Reuters**, Londres, UK, 14 fev. 2019. Disponível em: <https://www.reuters.com/article/nso-ma-francisco-partners-idUSL5N209642>. Acesso em: 11 set. 2021.

REIS et al. Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. **LAPIN**, 2021. Disponível em <https://lapin.org.br/2021/03/24/nota-tecnica-sobre-o-anteprojeto-de-lei-de-protecao-de-dados-para-a-seguranca-publica-e-investigacao-criminal/>. Acesso em 11 set 2021.

ROCHA, Manoel Ilson Cordeiro. Estado e governo: diferença conceitual e implicações práticas na pós-modernidade. **Revista Brasileira Multidisciplinar**, Araraquara, v. 11, n. 2, p. 140-145, 2008.

SINHORETTO, Jacqueline; MORAIS, Danilo De Souza. Violência e racismo: novas faces de uma afinidade reiterada. **Revista de Estudios Sociales**, n. 64, p. 15-26, 2018.

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

STEPANOVICH, A. et al. A Human Rights Response to Government Hacking. **ACCESS NOW**, 2016. Disponível em: <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>. Acesso em 10 set 2021

SUPREMO TRIBUNAL FEDERAL. Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. **Supremo Tribunal Federal Notícias.** Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx>. Acesso em 11 set 2021.

SWIRE, Peter; AHMAD, Kenesa. 'Going Dark' Versus a 'Golden Age for Surveillance.'. **Center for Democracy and Technology**, 2011.

UNITED NATIONS. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. **Office of the High Commissioner,** 2019. Disponível em <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736>. Acesso em 11 set 2021.

URUPÁ, Marcos. Policiais dizem que proposta da LGPD Penal poderia atrapalhar investigações. **Teletime**, 2021. Disponível em: <https://teletime.com.br/15/12/2020/policiais-dizem-que-proposta-da-lgpd-penal-poderia-atrapalhar-investigacoes/>. Acesso em 11 set 2021.

VALENÇA, Lucas. Além do Pegasus, Carlos Bolsonaro queria sistema para monitorar o Planalto. **Uol Notícias.** Brasília, 2021a. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2021/08/03/alem-do-pegasus-carlos-bolsonaro-previa-sistema-para-monitorar-planalto.htm>. Acesso em 11 set 2021.

VALENÇA, Lucas. Empresa de software espião Pegasus abandona licitação do governo. **Uol Notícias**. Brasília, 2021b. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/25/empresa-de-software-espiaopegasus-deixa-edital-que-e-rodeado-de-incertezas.htm>. Acesso em: 10 set. 2021

WERNECK, Alexandre. "Dar uma zoada","botar a maior marra": dispositivos morais de jocosidade como formas de efetivação e sua relação com a crítica. **Dados**, v. 58, p. 187-222, 2015.

WEBER, Max. A política como vocação. In: WEBER, Max. **Ensaios de Sociologia**. Rio de Janeiro: LTC, 1982, p.97-153.

YARON, Oded & GOICHMAN, Rafa. Israeli Phone-hacking Firm Cellebrite Halts Sales to Russia, Belarus in Wake of Haaretz Report. **Haaretz**, Tel Aviv, IL, 18 mar. 2021. Disponível em: <https://www.haaretz.com/israel-news/.premium-israeli-phone-hacking-firm-cellebrite-halts-sales-to-russia-after-haaretz-report-1.9633312>. Acesso em: 11 set. 2021.

ZANELLA, Everton Luiz. Infiltração de agentes. **Enciclopédia Jurídica da PUCSP,** 2020. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/442/edicao-1/infiltracao-de-agentes>. Acesso em 11 set 2021.

ZETTER, Kim. Everything We Know About How the FBI Hacks People. **Wired**. San Francisco, 2016. Disponível em: <https://www.wired.com/2016/05/history-fbis-hacking/ >. Acesso em: 10 set. 2021

ZITTRAIN, Johnatan et al (2016). Don't Panic: Making progress on the "Going Dark" debate. Berkman Klein Center, Harvard University. Disponível em: <https://cyber.harvard.edu/pubrelease/dontpanic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>. Acesso em 11 set 2021.