O MELHOR REMÉDIO É A LUZ DO DIA: TRANSPARÊNCIA E CONTROLE DA INTRUSÃO CIBERNÉTICA ESTATAL

THE BEST MEDICINE IS DAYLIGHT: TRANSPARENCY AND CONTROL STATE CYBER INTRUSION

Pedro Amaral[1]
Universidade Federal de Pernambuco, UFPE, Brasil
pedroamaral@ip.rec.br

DOI: https://doi.org/10.5281/zenodo.12207947

Resumo: Neste artigo são discutidas as capacidades de intrusão cibernética estatais, seus riscos e abusos no Brasil e no mundo, assim como a necessidade de ampliar mecanismos de transparência e controle dessas capacidades, tendo em mente a Arguição de Descumprimento de Preceito Fundamental 1.143, que se encontra no Supremo Tribunal Federal e visa abordar ferramentas de monitoramento remoto e softwares espiões. O ponto de partida é o reconhecimento de que a *internet* tem sido desenhada para viabilizar a vigilância para fins comerciais e que essas capacidades tendem a ser perseguidas ou vendidas para agências de segurança.

Palavras-chave: Vigilância; *Spyware*; *Hacking* governamental; ADPF 1.143; *Accountability*.

Abstract: This article discusses state cyber intrusion capabilities, their risks, and abuses in Brazil and around the world, as well as the need to expand transparency and control mechanisms for these capabilities, bearing in mind the Claim of Noncompliance with Fundamental Precept 1,143, which is before the Supreme Court and aims to address remote monitoring tools and spyware. The starting point is the recognition that the Internet has been designed to enable surveillance for commercial purposes and that these capabilities tend to be pursued or sold to security agencies.

Keywords: Surveillance; Spyware; Government hacking; ADPF 1,143; Accountability.

1. Introdução

Quanta informação há sobre cada um de nós na *internet*? Localidade em tempo real e do passado, histórico de busca, comunicações, atividade em redes sociais, finanças e dados pessoais, como idade, nome, gênero, entre tantas outras coisas, e biométricos, como características de face e impressões digitais. Além dos metadados dessas informações: com quem nos comunicamos, quando, como, qual frequência etc. Quanto dessa informação está acessível aos governos? Dependendo das capacidades e/ou dos recursos disponíveis, quase tudo. Craig Jarvis (2021, p. xi) argumenta que

> a habilidade histórica de governos de desenvolver capacidades de vigilância massiva sempre foi limitada pelo vasto requerimento de trabalho, que era economicamente inviável em sociedades democráticas. As tecnologias digitais removeram essa restrição.

E o *smartphone*, a "ferramenta perfeita de vigilância", é um elemento-chave da remoção desse obstáculo. Repleto de sensores e aplicativos sedentos por dados, estão quase sempre conectados à *internet* e são cada vez mais centrais para diversas atividades cotidianas, seja na educação, saúde, finanças, trabalho, lazer e comunicações privadas. Além dessa penetração na vida cotidiana, há o grau de saturação no mercado: dos 161,6 milhões de brasileiros com 10 anos ou mais que utilizaram a *internet*, 98,9% o fizeram por telefone celular móvel. Essa profundidade de alcance deve ser somada à capacidade crescente de análise de dados, especialmente com o avanço no campo da inteligência artificial, que deve acelerar nos próximos curto, médio e longo prazo.

Quando se debate *privacy by design*, devemos reconhecer que o ocorre hoje é a *surveillance by design*: a *internet*, suas aplicações, seus protocolos e dispositivos têm sido desenhados para coletar

[1] Coordenador de Projeto e Pesquisador no Instituto de Pesquisa em Direito e Tecnologia do Recife. Doutorando em Sociologia na Universidade Federal de Pernambuco. ORCID: https://www.orcid.org/0000-0002-3806-3117. Link Lattes: http://lattes.cnpq.br/5421281566504698.

[*] Este artigo foi desenvolvido a partir da minha fala inicial na Roda de Conversa organizada pelo IBCCrim no dia 06/06. O artigo também aborda elementos previamente debatidos no texto "Tempestade quase perfeita?", publicado no blog do Instituto de Pesquisa em Direito e Tecnologia do Recife, e em trabalho homônimo apresentado no VII Seminário Internacional Violência e Conflitos Sociais, promovido pelo Laboratório de Estudos da Violência, em abril de 2024.

mais e mais dados para viabilizar uma economia baseada em dados ou o "capitalismo de vigilância" (Zuboff, 2018). Não surpreende, então, que governos ao redor do mundo tenham buscado ou tenham sido provocados por habilidosos vendedores a adquirir esses poderes de vigilância massiva e/ou direcionada. A *internet* é uma infraestrutura para nossa sociedade e, como tal, "facilita ou dificulta" certas coisas (Easterling, 2014). Ela tem sido desenhada para facilitar a vigilância, especialmente com a privatização das diversas de suas camadas (Tarnoff, 2023).

Capacidades de vigilância têm frequentemente sido abusadas contra grupos específicos e adversários políticos dos governantes de ocasião. Tais capacidades têm tido ou tendem a ter suas funções sequestradas (*mission creep*) para outros fins. Por exemplo, nos Estados Unidos, dados de geolocalização e de busca, tradicionalmente empregados para vigilância comercial, têm sido usados para quem busca exercer seus direitos reprodutivos ou cuidados de afirmação de gênero.

2. Na opacidade, riscos são concretizados

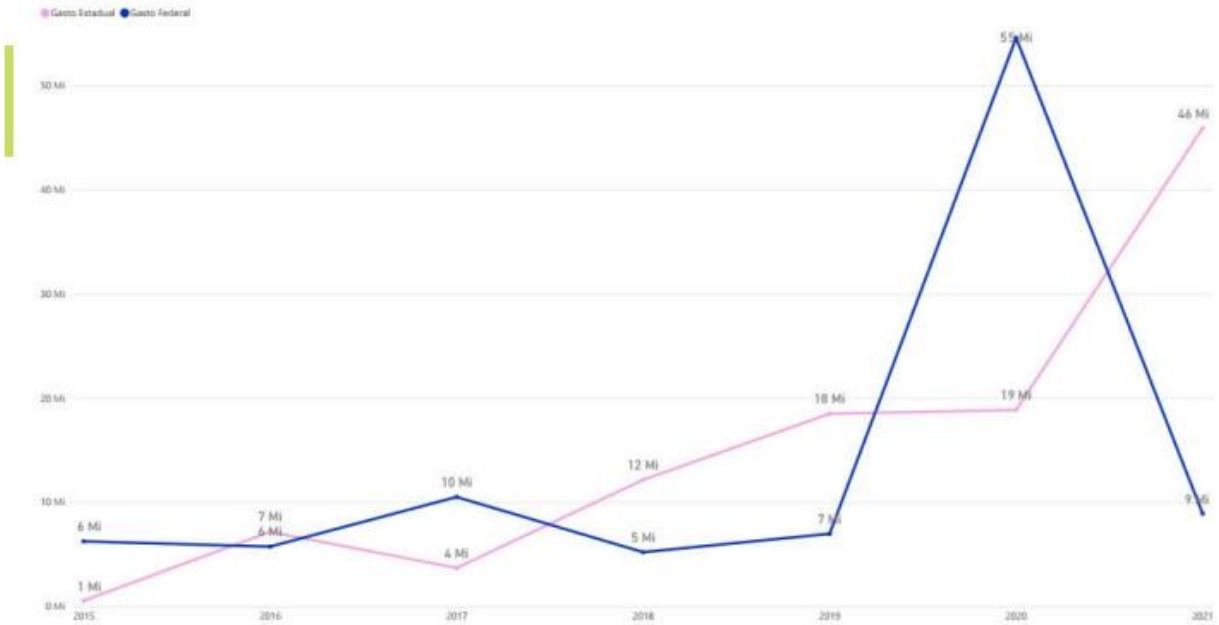
Nesse cenário, é necessário analisar as consequências negativas possíveis e já concretizadas pelo uso e abuso dessas capacidades de intrusão digital na vida privada. O uso de capacidades de intrusão cibernética pelos Estados está profundamente conectado à difusão comercial da criptografia forte, especialmente acelerada após as revelações de Edward Snowden, em 2013, sobre os programas de vigilância global realizados pela estadunidense National Security Agency (NSA).

Nesse debate, agentes de aplicação da lei ao redor do mundo têm defendido e aplicado capacidades de intrusão (ou *hacking*) em dispositivos, redes e sistemas como alternativa à escuridão que a criptografia proporciona aos agentes mal intencionados. Se inicialmente era defendida como medida excepcional, o que se vê é a difusão descontrolada dessas capacidades.

Uma vez com as capacidades instaladas e com incentivos, essas ferramentas tendem a ser usadas sem atender a tal critério. Isso foi observado nos Estados Unidos pelo estudo da Upturn, onde os usos estão relacionados a infrações de menor potencial ofensivo ou sem relação com o uso de tais dispositivos, incluindo pixação, prostituição e batidas de carro (Koepke *et al.*, 2020). O estudo confirmou a posse dessas ferramentas por todas as agências de investigação estaduais, pelas 50 maiores agências de investigação locais e todas as repartições da polícia federal daquele país.

O caso brasileiro é similar. Em 2022, o Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) publicou o estudo "Mercadores da insegurança: conjuntura e riscos do *hacking* governamental no Brasil", do qual sou um dos autores. Neste estudo mostramos a difusão de ferramentas de intrusão de dispositivos em diversos órgãos brasileiros. Tais ferramentas estão presentes em todos os estados brasileiros, além de diversos órgãos federais e das Forças Armadas (Ramiro *et al.*, 2022). É possível ver uma crescente quase constante nos gastos na Figura 1.

Figura 1 – Gastos estaduais e federais no Brasil, entre 2015 e 2021.

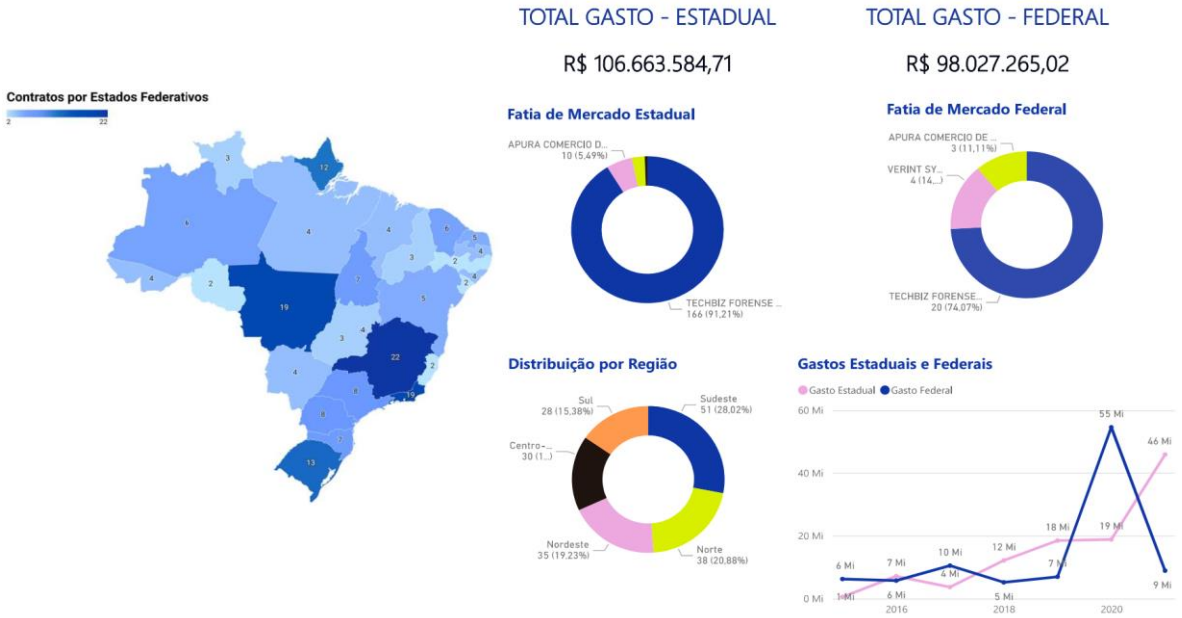


Fonte: Ramiro *et al.* (2022, p. 29).

Em nosso estudo encontramos documentos públicos de aquisição de ferramentas de intrusão em todos os estados brasileiros e em diversos órgãos federais. Foram 209 documentos contratuais, sendo 182 estaduais e 27 federais. Encontramos contratos de aquisição de ferramentas, treinamento de pessoal, aditamento de licença, atualização de *software*, entre outros. Identificamos oito fabricantes internacionais, com atuação presente ou passada no Brasil dentro do recorte temporal de 2015 a 2021, assim como 22 ferramentas ou serviços (Figura 2). A maioria das ferramentas encontradas são as Ferramentas Forense de Dispositivos Móveis (no original, *Mobile Device Forensic Tools*). Incapazes de invadir dispositivos móveis de maneira remota, essas ferramentas:

> […] são conjuntos de *hardware* e *software* utilizados em dispositivos móveis em custódia das forças policiais para desbloqueá-los e extrair dados, através de conexão física, que alcançam serviços de e-mail, armazenamento em nuvem, dados de redes sociais, histórico de localização (GPS), comunicações privadas, fotos, vídeos e, basicamente, o que mais estiver armazenado e acessível em aparelhos de celular pessoais, incluindo dados deletados pelo usuário. Sobre o conjunto de dados coletados, não é incomum ver soluções de inteligência artificial aplicadas adicionalmente, como forma de identificar padrões (Ramiro *et al.*, 2022, p. 9).

Figura 2 – Contratos por estados e gastos estaduais e federais.



Fonte: Elaborada pelos autores.

Apesar de menos intrusivas que *spywares* famosos, como o Pegasus e Candiru, as ferramentas disponíveis hoje já são problemáticas e já têm sido abusadas nesse atual vácuo legislativo. Em Santa Catarina, um dos sócios da Suntech, por exemplo, braço da Verint, fornecedora desse tipo de ferramenta, foi investigado e preso por indícios de articular o vazamento de informações de investigações aos políticos investigados. No Pará, ferramentas da mesma Verint estão envolvidas no monitoramento ilegal de agentes que investigavam um esquema de corrupção na compra de respiradores durante a pandemia da COVID-19 (Ramiro *et al.*, 2022). Allan de Abreu (2023), na Revista Piauí, revelou que foi denunciado ao Ministério Público do Amazonas que "agentes da Secretaria de Segurança estavam extorquindo comerciantes de ouro depois de monitorá-los com o GI-2 e outro programa, conhecido como Guardião". GI-2 é uma ferramenta fornecida pela Cognyte, que encontramos em nosso estudo. Esses casos evidenciam o potencial de abuso de poder facilitado pelas tecnologias já presentes nas forças de segurança pública brasileiras.

Vale lembrar que, durante o governo Bolsonaro, a extinta Secretaria de Operações Integradas do Ministério da Justiça distribuiu para as forças estaduais equipamentos da Cellebrite, por meio do Projeto Excel (Ameno, 2022). Em outubro de 2023, a Agência Pública reportou como Cognyte tem fechado contratos com vários estados (Paes; Scofield; Valente, 2023). Tatiana Dias e Paulo Motoryn (2023), no The Intercept Brasil, detalharam a acelerada adoção estatal dessas ferramentas. A imprensa tem feito um trabalho excepcional e essencial em publicizar iniciativas, as capacidades em jogo e seus riscos.

Vale destaque para o Jornal O Globo (Dantas; Camporez; Bronzatto, 2023), que denunciou um esquema de espionagem da Agência Brasileira de Inteligência (Abin) contra pessoas consideradas adversárias do governo de Jair Bolsonaro, em março de 2023. Após a denúncia, a Polícia Federal tem investigado o caso e já cumpriu diversos mandados de busca e apreensão, inclusive contra o então diretor da Abin, o agora deputado federal Alexandre Ramagem, e contra Carlos Bolsonaro. O FirstMile, ferramenta fornecida pela Cognyte, explora o Sistema de Sinalização 7 (SS7) para monitorar a localização de até 10 mil dispositivos simultaneamente. O SS7 está presente nas redes de dados móveis inferiores à 4G, que são usadas por quase todos os dispositivos móveis no Brasil.

Há algum tempo graves denúncias têm sido feitas por jornalistas, ativistas e pesquisadores de cibersegurança e provocando reação pública, incluindo regulatória. Entre a infecção de líderes pró-independência da Catalunha (Farrow, 2022), do gabinete do Primeiro Ministro do Reino Unido (Deibert, 2022), de diversos jornalistas e defensores de direitos humanos, vale destacar o caso do jornalista saudita Jamal Khashoggi, assassinado dentro do Consulado da Arábia Saudita em Istambul, Turquia, em 2018, que teria sido facilitado pelo Pegasus (Farrow, 2022). Em 2020, um consórcio de jornalismo investigativo teve acesso a uma lista de 50 mil telefones alvos do *spyware* da empresa israelense NSO Group (About [...], 2021), incluindo o presidente francês Emmanuel Macron, dentre os 600 políticos de 32 nações encontrados na lista (Pegasus [...], 2021). Após recorrentes e graves denúncias, algumas lideranças políticas têm criticado publicamente esses usos e abusos.

Um breve comentário vale também para atentar a uma outra capacidade de certas ferramentas que ganham total controle do dispositivo, alertada pelo especialista e referência em cibersegurança, Carlos Cabral: a inserção de informações nos dispositivos. Visto que as informações nos dispositivos podem ser consideradas prova, um risco adicional é a de incriminação pela inserção de, por exemplo, uma foto ou vídeo, cuja posse em si seja crime ou possa ser usada como indicativo de participação em crime.

Tal conjunto de abusos e capacidades, devemos reconhecer, assusta e deve assustar. É necessário olhar para toda a amplitude de ferramentas e capacidades disponíveis no mercado, evitando focalizar apenas nos casos mais perigosos. Nesse sentido, a ADPF 1.143 deixa de fora uma gama de ferramentas menos intrusivas e menos custosas, mas muito mais adquiridas, respectivamente, as ferramentas forenses de dispositivos móveis. Apesar de levantarem menos alarme à sociedade civil e já estarem bem mais integradas ao ferramental policial brasileiro, tais ferramentas têm seus riscos aumentados por operarem em um vácuo regulatório, como nós concluímos no relatório de pesquisa "Mercadores da Insegurança" (Ramiro *et al.*, 2022).

Em resposta ao movimento no Supremo Tribunal Federal, o Senador Alessandro Vieira (PSDB-AL) protocolou o Projeto de Lei 402/2024, que visa disciplinar a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Em contraste com a ADPF 1.143, o PL 402/2024 avança ao incluir em seu escopo os "equipamentos e programas de informática que possibilitam a extração em massa de dados dos terminais de comunicações pessoais a partir de seu controle físico", segundo artigo 3º, parágrafo único (Brasil, 2024). Ponto muito positivo.

3. Grandes poderes requerem grandes responsabilidades, certo?

As capacidades inéditas de vigilância servem a muitos objetivos e a muitos senhores, mas as tecnologias digitais também empoderam os cidadãos. Por meio delas, é possível, por exemplo, fiscalizar melhor as crescentes capacidades de vigilância estatal. Se essas capacidades estão aumentando e se transformando rapidamente, é necessário que o controle público também acompanhe. Operando em quase total sigilo, muitas agências de segurança no Brasil e no mundo têm crescentemente adquirido ou desenvolvido capacidades de intrusão digital.

Mecanismos de controle, como a transparência, devem ser fortalecidos, tanto sobre as capacidades informacionais e os *inputs* que fornecem à tomada de ação, quanto sobre o próprio processo de tomada de decisões a partir das análises recebidas. Nesse sentido, Clement (2021, p. 143, tradução livre) critica a agência de inteligência canadense Communications Security Establishment, por não reconhecer que "[...] pode haver interesse público em divulgar algumas de suas capacidades básicas". O ponto central para uma "transparência de capacidades" é reconhecer que entre a postura atual de sigilo total (presente em vários órgãos que questionamos via Lei de Acesso à Informação) e o:

> [...] sigilo que é comprovadamente necessário para a eficácia, existe um amplo meio-termo de transparência e responsabilização que vale a pena explorar, especialmente relacionado com as capacidades de vigilância doméstica (Clement, 2021, p. 143, tradução livre).

É importante, contudo, ir além do que o autor propõe e avaliar em que medida há alinhamento ou justificativa em termos de legalidade, necessidade, proporcionalidade e proteção de dados pessoais para a aquisição e uso de certas capacidades de intrusão digital. São princípios que, inclusive, estão ausentes do "*Pall Mall Process*". A transparência é uma necessidade de reduzir a assimetria de informação e, portanto, de poder, entre Estado e cidadãos. Algumas agências de segurança ao redor do mundo não parecem reconhecer ou querer reconhecer que os seus poderes devem ser acompanhados por novos deveres a fim de mitigar riscos e evitar abusos.

Acesso à informação e sua consequente disponibilização na esfera pública, argumento, têm sido condições, no âmbito das capacidades de intrusão cibernética, para avançar em mecanismos de controle e de supervisão, assim como de proporcionalidade, necessidade e proteção de dados pessoais. Estudos como o nosso "Mercadores da Insegurança" (Ramiro *et al.*, 2022) e da Upturn (Koepke *et al.*, 2020) e as investigações jornalísticas dependeram de algum nível de acesso à informação para engatilhar as conversações públicas que têm possibilitado um horizonte de controle democrático das capacidades estatais de intrusão. Por isso, devemos ampliar e aprofundar as obrigações de transparência para a aquisição e o uso de capacidades de intrusão cibernética.

Informações adicionais e declarações do autor (Integridade Científica)

Declaração de conflito de interesses: o autor confirma que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de originalidade:** o autor garantiu que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; ele também atesta que não há plágio de terceiros ou autoplágio, ressalvados os esclarecimentos anotados no rodapé inicial.

Como citar (ABNT Brasil):

AMARAL, P. O melhor remédio é a luz do dia: transparência e controle da intrusão cibernética estatal. Boletim IBCCRIM, São Paulo, v. 32, n. 380, p. 5-8, 2024. DOI: 10.5281/zenodo.12207947. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1224. Acesso em: 1 jul. 2024.

Referências

ABOUT the Pegasus Project. *Forbidden Stories*, 18 jul. 2021. Disponível em: https://forbiddenstories.org/about-the-pegasus-project/. Acesso em: 4 abr. 2024.

ABREU, Allan de. No reino da arapongagem. *Revista Piauí*, dez. 2023. Disponível em: https://piaui.folha.uol.com.br/materia/como-os-orgaos-oficiais-abriram-as-comportas-da-espionagem-ilegal-no-governo-bolsonaro/. Acesso em: 4 abr. 2024.

AMENO, Fernando. As planilhas de Bolsonaro. *The Intercept Brasil*, 21 mar. 2022. Disponível em: https://www.intercept.com.br/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/. Acesso em: 4 abr. 2024.

BRASIL. Congresso Federal. *Projeto de Lei 402/2024*. Brasília: Congresso Federal, 2024. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9551220&ts=1711466303706&disposition=inline. Acesso em: 4 abr. 2024.

CLEMENT, Andrew. Limits to secrecy: what are the communications security establishment's capabilities for intercepting Canadians' Internet communications? *In*: LYON, David; WOOD, David Murakami (Ed.). *Big data surveillance and security intelligence*: The Canadian case. UBC Press, 2021. p. 126-146.

DANTAS, Dimitrius; CAMPOREZ, Patrik; BRONZATTO, Thiago. Abin de Bolsonaro usou programa secreto para monitorar localização de pessoas por meio do celular. O Globo, Brasília, 14 mar. 2023. Disponível em: https://oglobo.globo.com/politica/noticia/2023/03/abin-de-bolsonaro-usou-programa-secreto-para-monitorar-localizacao-de-pessoas-por-meio-do-celular.ghtml. Acesso em: 4 abr. 2024.

DEIBERT, Ron. UK government officials infected with Pegasus. *Citizen Lab*, abr. 2022. Disponível em: https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/. Acesso em: 4 abr. 2024.

DIAS, Tatiana; MOTORYN, Paulo. Como o Brasil virou o paraíso da espionagem ilegal. *The Intercept Brasil*, 27 out. 2023. Disponível em: https://www.intercept.com.br/2023/10/28/brasil-virou-paraiso-da-espionagem-ilegal-com-michel-temer-jair-bolsonaro/. Acesso em: 4 abr. 2024.

EASTERLING, Keller. *Extrastatecraft*: The power of infrastructure space. Verso Books, 2014.

FARROW, Ronan. How democracies spy on their citizens. *The New Yorker*, 25 abr. 2022. Disponível em: https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens. Acesso em: 4 abr. 2024.

JARVIS, Craig. *Crypto wars*: the fight for privacy in the digital age: A political history of digital encryption. CRC Press, 2020.

KOEPKE, Logan; WEIL, Emma; JANARDAN, Urmila; DADA, Tinuola; YU, Harlan. Mass extraction the widespread power of U.S. law enforcement to search mobile phones. *Upturn*, 2020. Disponível em: https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf. Acesso em: 22 maio 2023.

PAES, Caio de Freitas; SCOFIELD, Laura; VALENTE, Rubens. Como empresa de espionagem israelense alvo da PF se espalhou pelo poder público no Brasil. *Agência Pública*, 20 out. 2023. Disponível em: https://apublica.org/2023/10/como-empresa-de-espionagem-israelense-alvo-da-pf-se-espalhou-pelo-poder-publico-no-brasil/. Acesso em: 4 abr. 2024.

PEGASUS spyware scandal: Emmanuel Macron among 14 heads of states identified as possible targets. *Euronews*, 21 jul. 2021. Disponível em: https://www.euronews.com/next/2021/07/21/pegasus-spyware-scandal-emmanuel-macron-among-14-heads-of-states-identified-as-possible-ta. Acesso em: 4 abr. 2024.

RAMIRO, André (coord.); AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M. *Mercadores da insegurança*: conjuntura e riscos do *hacking* governamental no Brasil. Recife: IP.rec, 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 4 abr. 2024.

TARNOFF, Ben. *Internet for the people*: The fight for our digital future. Verso Books, 2022.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. Nova York: Public Affairs, 2019.

Autor convidado