INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
v. 7 · e707 · 2026 – DOI: 10.47975/ijdl.v7.1324

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

Licenciado sob uma Licença Creative Commons
Licensed under Creative Commons

International Journal of Digital Law – IJDL
DOI: 10.47975/ijdl.v7.1324

A violação da privacidade como política pública: por que a autorização de uso de *softwares* espiões hoje é equivocada

Privacy violation as public policy: why authorizing the use of spyware today is misguided

Rafaela dos Reis Baldissera*
Universidade Federal de Santa Catarina (Santa Catarina, SC, Brasil)
rafaelabaldissera@yahoo.com.br
https://orcid.org/0009-0000-7627-0806

Recebido/Received: 12.11.2025 / November 12th, 2025
Aprovado/Approved: 18.07.2026 / July 18th, 2026

Resumo: O uso massivo de aparelhos inteligentes oportuniza as investigações e o conjunto de evidências que envolvem computadores pessoais e servidores, como e-mail, arquivos apagados, decriptação de arquivos e histórico de Internet, dispositivos móveis. Alguns pontos merecem destaque no que diz respeito à proteção de dados pessoais dos usuários cujos dados são extraídos mediante essas soluções tecnológicas. O Brasil possui diversas iniciativas legislativas relacionadas ao uso de novas tecnologias, sendo o mais recente o objeto dos Projetos de Lei nº 402/2024 e 58/2024 (apensado ao PL 199/2021), nascidos após provocação da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 1143. A tentativa de regulação, seja pela ADPF, seja pelos PLs apresentados, surgiu como resposta às denúncias de espionagem ilegal na Agência Brasileira de Inteligência (ABIN) utilizando a ferramenta israelense First Mile. Com essas novas tecnologias e nova sociedade em perspectiva, questiona-se se há balizas essenciais que autorizam a regulamentação das tecnologias invasivas e se a regulamentação hoje representa uma ameaça à privacidade. A pesquisa ostenta caráter qualitativo e a técnica de pesquisa foi a de análise legislativa e revisão bibliográfica de fontes primárias e secundárias, por meio da qual se buscou material em livros temáticos, teses de doutoramento e dissertações de mestrado, assim como artigos científicos publicados em periódicos diversos e, ainda, de análise legislativa.

Como citar este artigo/*How to cite this article*: BALDISSERA, Rafaela dos Reis. A violação da privacidade como política pública: por que a autorização de uso dos *softwares* espiões hoje é equivocada. *International Journal of Digital Law*, Belo Horizonte, v7, e707, 2026. DOI: 10.47975/ijdl.v7.1324.

* Mestre em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina (Florianópolis, SC, Brasil). Pós-Graduada em Segurança Digital, Governança e Gestão de Dados pela Pontifícia Universidade Católica do Rio Grande do Sul. Pós-Graduada em Direito Público pela Fundação Universidade Regional de Blumenau. Advogada. *E-mail*: rafaelabaldissera@yahoo.com.

Palavras-chave: Privacidade. Proteção de dados. Segurança pública. Violação. Infiltração clandestina.

Abstract: The proliferation of smart devices has revolutionized the landscape of investigations and evidence collection. These devices, encompassing personal computers, servers, mobile devices, and more, provide access to a vast array of data, including emails, deleted files, decrypted files, and internet history. However, this unprecedented access to personal information raises critical concerns regarding data privacy and the potential for misuse. Brazil has taken proactive steps to address these concerns through various legislative initiatives, the most recent being Bills No. 402/2024 and 58/2024 (attached to Bill No. 199/2021). These bills were introduced in response to allegations of illegal espionage by the Brazilian Intelligence Agency (ABIN) using the Israeli tool First Mile. The emergence of these sophisticated technologies and the evolving societal landscape necessitate a careful examination of the boundaries between legitimate investigative practices and the protection of individual privacy.

Keywords: Privacy. Data protection. Public security. Violation. Clandestine infiltration.

Sumário: 1 Introdução – **2** O funcionamento dos *softwares* espiões no contexto da privacidade e proteção de dados – **3** A ADPF 1143 e os projetos de lei dela decorrentes – **4** Política Pública de Segurança Pública ou Política de Segurança Pública? – **5** Conclusão – Referências

1 Introdução

O direito fundamental à privacidade (art. 5º, X e XII, CF)[1] e, mais recentemente, o direito fundamental à proteção de dados pessoais (art. 5º, LXXIX, CF),[2] esse acrescido pela Emenda Constitucional nº 115/2022, decorrente da decisão proferida na Ação Direta de Inconstitucionalidade (ADI) nº 6393, julgada em 2020 pelo Supremo Tribunal Federal (STF),[3] deixam claro que, quanto mais grave for a intervenção estatal sobre tais aspectos da vida do indivíduo, maiores devem ser os requisitos para tanto. A regra denota uma reserva legal qualificada que, analisada sob o princípio da proporcionalidade, autoriza ou não a redução dessas garantias constitucionais.

O próprio texto do inciso XII orienta dessa forma quando condiciona a exceção tão somente por meio de "ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Em termos de segurança pública, o Brasil possui diversas iniciativas, tanto em âmbito federal quanto estadual, relacionadas ao uso de novas tecnologias, sendo

1 BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988. Disponível em: https://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-publicacaooriginal-1-pl.html. Acesso em: 2 maio 2024.

2 BRASIL. *Constituição da República Federativa do Brasil*, Brasília, DF, Senado Federal: Centro Gráfico, 1988. Disponível em: https://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-publicacaooriginal-1-pl.html. Acesso em: 2 maio 2024.

3 BRASIL. Supremo Tribunal Federal, Ação Direta de Inconstitucionalidade nº 6.393, rel. Min. Rosa Weber, Tribunal Pleno, julgada em 7 maio 2020, *DJe* nº 270, divulgação em 11 nov. 2020, publicação em 12 nov. 2020.

o mais recente o objeto dos Projetos de Lei nº 402/2024 e nº 58/2024 (apensado ao PL nº 199/2021), nascidos após provocação da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 1.143, protocolada pela Procuradoria-Geral da República (PGR), inicialmente sob forma de uma Ação Direta de Inconstitucionalidade por Omissão (ADO) nº 84.

A ADO deu-se em razão da *inertia deliberandi* em razão dos Projetos de Lei parados: PL 8045/2010, PL 276/2011, PL 480/2011, PL 6832/2013, PL 645/2015, PL 10724/2018, PL 4510/2020, PL 4939/2020, PL 199/2021, PL 465/2023, PL 3082/2023, PL 3226/2023, PL 5139/2023, PL 5302/2023, PL 6149/2023 e PL 58/2024. Pelo princípio da fungibilidade das ações constitucionais, a ADO foi transformada em ADPF. O intuito da PGR é regular as hipóteses de invasão de aparelhos de particulares com base na tecnologia.

A tentativa de regulação, seja pela ADPF, seja pelos PLs apresentados, surgiu como resposta às denúncias de espionagem ilegal na Agência Brasileira de Inteligência (ABIN) utilizando a ferramenta israelense *First Mile*. O uso ilegal do *software* resultou na Operação Última Milha, deflagrada em outubro de 2023 e desencadeou um sem-número de investigações sobre o uso da agência para fins diversos (denominada usualmente de ABIN Paralela).

O entendimento sobre privacidade que se tem positivado hoje é datado de pelo menos 35 anos atrás. A adoção do conceito de privacidade estampado no texto constitucional foi fruto das tecnologias e momentos históricos da época que, desde então, sofreram inúmeras mudanças.[4] Com essas novas tecnologias e nova sociedade em perspectiva, questiona-se se há balizas essenciais que autorizam a regulamentação das tecnologias invasivas e se a regulamentação hoje representa uma ameaça à privacidade.

Como hipótese primária tem-se que os requisitos para o uso dos *softwares* espiões, principalmente por parte do poder público, sequer deveriam ser cogitados e o que se tem hoje (sejam os PLs, seja a ADPF) é apenas uma tentativa de regular hipóteses de restrição de direitos fundamentais e não necessariamente a sua promoção e o poder público, a saber, não condiciona a regulamentação à perspectiva da privacidade e proteção de dados.

Para confirmação das hipóteses, o estudo objetiva esmiuçar o funcionamento dos *softwares* espiões, a fim de colocá-los sob a perspectiva do estudo da ética e inteligência artificial, a fim de viabilizar um debate acurado sobre a necessidade de intensificação dos direitos fundamentais à privacidade, à intimidade e à proteção de dados pessoais na era digital. Será abordado também o texto da ADPF 1143,

[4] Apenas a título exemplificativo, cita-se o advento das redes sociais, aplicativo de mensagens instantâneas, ou ainda a caracterização da "sociedade da informação", conceito esse amplamente utilizado por Manuel Castells e extraído em suas diversas obras.

bem como dos PLs 402/2024 e 58/2024 sob a perspectiva dos direitos fundamentais. Por fim, no último tópico, serão abordadas as políticas públicas existentes na área da segurança pública, e se essa movimentação legislativa de autorização do uso dessas novas tecnologias invasivas vai ao encontro da manutenção das garantias constitucionais de privacidade e proteção de dados, ou se o país está encaminhando-se para um contexto de redução de direitos individuais.

A metodologia empregada para a elaboração do presente artigo foi essencialmente a pesquisa e a sistematização da produção acadêmica especializada, visando compreender diferentes interpretações desse *corpus* bibliográfico sobre o mesmo fenômeno das ferramentas tecnológicas. Ainda que prevaleça nas fontes do artigo os trabalhos acadêmicos, utilizou-se também materiais provenientes de organizações da sociedade civil, especialmente relatórios analíticos e similares. Os dados apresentados, por sua vez, advêm de fontes secundárias, a própria bibliografia especializada, e teve a função de trazer fundamentação aos argumentos dos autores.

O método de abordagem foi o dedutivo, por meio do qual partiu-se de uma perspectiva geral de conceitualização atual do termo privacidade, com uma introdução das novas tecnologias no seio social e seus efeitos, seguindo-se por uma análise desses efeitos sob a perspectiva dos direitos fundamentais. A pesquisa ostenta caráter qualitativo, enfatizando a subjetividade das relações interpessoais com as novas tecnologias e com maior interesse pelo processo do que pelos resultados. A técnica de pesquisa foi a de análise legislativa e revisão bibliográfica de fontes primárias e secundárias, por meio da qual se buscou material em livros temáticos, teses de doutoramento e dissertações de mestrado, assim como artigos científicos publicados em periódicos diversos e, ainda, de análise legislativa.

O artigo está dividido em quatro partes, além desta introdução. Na primeira parte, são apresentados, brevemente, o fenômeno sobre o qual os trabalhos se debruçam e os fundamentos da abordagem dominante, caracterizada pela noção de ferramentas de tecnologia invasiva sob a perspectiva da privacidade e proteção de dados, matizando, no entanto, algumas das diferenças que existem dentro dessa literatura. Na segunda parte, abordou-se a dimensão normativa que perpassa a literatura dominante e identifica as brechas no processo legislativo, bem como a discussão jurídica em seu entorno como sendo um desvio e um risco às garantias individuais. Na terceira parte, são apresentadas as perspectivas que criticam a literatura dominante e, com isso, essas são confrontadas com os dados existentes a respeito da temática, tendo como base a noção de política pública e segurança pública. Por fim, são apresentadas algumas conclusões que emergem da comparação entre as diferentes abordagens, destacando suas limitações e potencialidades, bem como as implicações normativas de cada uma delas.

2 O funcionamento dos *softwares* espiões no contexto de privacidade e proteção de dados

O direito à privacidade não compreende mais o antigo conceito jurídico de "right to privacy",[5] ou ainda o brocardo "right to be let alone".[6] Na sociedade contemporânea,[7] porém, a noção de privacidade extravasa os conceitos de isolamento ou tranquilidade. O "right to be let alone" revela-se insuficiente em uma sociedade em que os meios de violação da privacidade caminham paralelamente aos diversos e importantes avanços tecnológicos.[8] A privacidade hoje lida com o indivíduo e suas múltiplas possibilidades de controle sobre as informações que lhe dizem respeito, deslocando a noção de privacidade para os direitos de personalidade.[9]

O uso massivo de aparelhos inteligentes oportuniza as investigações e o conjunto de evidências que envolvem computadores pessoais e servidores, como e-mail, arquivos apagados, decriptação de arquivos e histórico de Internet, dispositivos móveis (*WhatsApp*, drones, Telegram, *e-mail*, Viber, *WeChat* etc.), redes e sistema CFTV (tráfego de rede, câmeras de vigilância e reconhecimento facial), nuvem (Office 365, Dropbox, Google Suite, Sharepoint, OneDrive etc.) e Internet das Coisas.

O nível de segurança de um aparelho pode ser corrompido através de *malwares*, *softwares* maliciosos projetados para causar danos a dispositivos independentes ou conectados via rede, como, por exemplo, os *softwares* espiões. Em outras palavras, qualquer dispositivo, aplicação, protocolo de segurança, incluindo bloqueio de tela ou serviço por código PIN, senha pessoal, biometria, criptografia de disco ou de tráfego de dados, de uso pessoal ou coletivo, é passível de acesso.

Os *softwares* espiões são programas instalados em determinado dispositivo com ou sem a permissão do indivíduo que coletam informações, hábitos de navegação em rede, rastreamento inclusive de geolocalização, entre outros, e enviam a um usuário remoto. Esses programas espiões podem também baixar outros programas maliciosos e instalá-los nesse mesmo dispositivo.

Conforme explicam Manjugouda R. Patil e C. F. Mulimani,[10] os *softwares* espiões funcionam como *adware*,[11] mas geralmente é um programa separado que é

---

5 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 7-8.

6 WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, nº 5, p. 193-220, 1890.

7 A Idade Contemporânea é o período histórico que começou na Revolução Francesa e se estende até os dias de hoje.

8 DONEDA, Danilo, *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados, 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 10.

9 GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais*, v. 156, p. 353-393, jun. 2019.

10 PATIL, Manjugouda R.; MULIMANI, C. F. Pegasus: transforming phone into a spy. *Think India Journal*, v. 22, nº 14, p. 7883-7890, 2019.

11 *Adware* é um *software* não desejado projetado para jogar anúncios na sua tela.

instalado inadvertidamente quando você instala outro programa ou aplicativo do tipo *freeware*.[12] Em níveis mais avançados, esses programas podem ser instalados em dispositivos que executam determinadas versões de sistemas operacionais, assim como conseguem quebrar sistemas de comunicação criptografada.

Alguns pontos merecem destaque no que diz respeito à proteção de dados pessoais dos usuários cujos dados são extraídos mediante essas soluções tecnológicas. O primeiro deles é a respeito do acesso aos dados por empresas fabricantes. As ferramentas de tecnologia deveriam ser administradas apenas por quem tem acesso ao conteúdo de determinada diligência policial/investigativa.

A Techbiz Forense Digital é uma das maiores representantes comerciais de tecnologias invasivas sediadas no Brasil e comercializa ferramentas como *Cellebrite*, *Opentext*, *Magnetic Forensics* e Exterro/*AccessData*, todas utilizadas no campo da segurança pública brasileira.[13] O diretor comercial da empresa, Rafael Velásquez, afirma que essas tecnologias são "soluções forenses que tratam grandes volumes de dados de forma rápida, correlacionando as informações de várias fontes - tanto dos dispositivos eletrônicos como de dados armazenados na nuvem e na Internet -, para obter evidências e provas, auxiliando a elucidação de crimes".[14]

Porém, muito embora haja informações expressas de diversas empresas alegando não possuírem acesso ao material trabalhado nas operações policiais,[15] a própria publicidade dessas ferramentas indica sentido contrário.[16] A comercialização

---

12 O *freeware* é um *software* protegido por direitos autorais que está disponível sem nenhum custo para uso ilimitado.

13 Empresa fiadora e intermediária das tecnologias para fins de investigação atualmente vigentes no país, é também a principal negociadora com o poder público brasileiro para o fornecimento de ferramentas de *hacking*. Seus clientes, dentre outros, são os Ministérios Públicos e Secretarias de Segurança Estaduais, além do próprio Ministério da Justiça. A empresa possui mais de uma centena de contratos com a administração pública estadual e federal, somando mais de 100 milhões desde 2018. Sobre isso ver: 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, p. 52.

14 VELASQUEZ, Rafael. Desafios da investigação criminal tecnológica. *Techbiz Forense Digital*, 2022. Disponível em: https://techbiz.com.br/wp-content/uploads/2022/06/Artigo-Desafios-da-investigacao-criminal-tecnologica.pdf. Acesso em: 5 maio 2024.

15 Cellebrite, *Extração e desbloqueio avançados*: Cellebrite Advanced Services, 2020. Disponível em: https://cellebrite.com/en/cellebrite-announces-formation-of-ethics-integrity-committee/. Acesso em: 5 maio 2024.

16 Exemplo seria o Projeto Excel, autorizado pela Portaria nº 26/2020 que viabilizou a criação de uma base de dados constituída por dados extraídos por ferramenta própria de notícias que amplificam o acesso aos dados tratados nas operações policiais. Essas informações alimentam uma base de dados utilizada para investigações na esfera federal. Desse Projeto desencadeou a Operação Esgtrondo, no Rio Grande do Norte (RN), em que boa parte das provas que embasaram os pedidos de busca e apreensão e de prisão estão no relatório de análise dos dados extraídos de celulares apreendidos. Ou seja, apesar do Projeto Excel ter sido criado para o combate ao crime organizado, a própria portaria permite que os equipamentos para extração e análise de dados sejam utilizados sem que haja investigação criminal em curso. Sobre o tema ver: AMENO, Fernando. As planilhas de Bolsonaro: Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados, *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: 5 maio 2024; e VALENTE, Rubens, Ação sigilosa do governo mira professores e policiais antifascistas, *UOL Notícias*, 24 jul. 2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/07/24/ministerio-justica-governo-bolsonaro-antifascistas.htm. Acesso em: 5 maio 2024.

desses *softwares* se dá também pela publicidade de fazerem o trabalho de extração de dados, ou seja, de também possuírem o acesso aos dados tratados pela atividade policial. Invariavelmente, os dados obtidos por meio de investigações policiais têm necessariamente que passar pelas mãos da Cellebrite, a qual coleta, trata, compartilha e descarta dados pessoais dos usuários encontrados e seus correlatos que estejam em suas redes de conexões. Em outras palavras, é a própria empresa que realiza todo o trabalho policial envolvendo essas ferramentas tecnológicas.

Há, pois, um acúmulo de dados nas mãos dessas empresas, o que não é nada positivo se analisar as notícias que relacionam a empresa com o mercado clandestino.[17]

Outro ponto seria a respeito da possibilidade de requisição de dados aos provedores de aplicação,[18] outra informação amplamente divulgada por empresas que comercializam esse serviço.[19] Provedor de aplicação seria um intermediário na busca pelo acesso a dados em investigações e requisitar dados de provedores nada mais é do que um desvio do devido processo legal de extração de dados, colocando mais um intermediador do tratamento desses dados sob posse de informações sigilosas investigativas.

Pegando de exemplo a ferramenta contratada para auxílio tecnológico em três casos emblemáticos brasileiros — Menino Henry, Lava Jato e Marielle Franco:[20] a *Cellebrite*, essa possui, dentre outras, duas opções de extração de dados, uma manejada por algoritmo de *machine learning* para identificação de objetos e pessoas; e outra manejada por extração de dados públicos, disponíveis em redes

---

Outro exemplo que, a meu ver, se confirmar os indícios de ilegalidade a seguir elencados, vai anular toda a investigação realizada, é a ferramenta GI2, da empresa Cognyte (ex-Verint), cujo contrato é encontrado sob alçada da Polícia Civil do Pará, utilizada para espionar investigadores de esquema de corrupção na compra de respiradores durante a Covid-19. Segundo o Ministro Francisco Falcão, relator do caso do Superior Tribunal de Justiça, "confirmou-se que o dispositivo é capaz de extrair dados de aparelhos telefônicos, interceptar diálogos criptografados e fazer gravações ambientais, tudo sem autorização judicial, podendo os dados ser apagados facilmente, não deixando rastro sobre sua utilização". Sobre o tema: DANTAS, Claudio. Exclusivo: a empresa que vendeu a "maleta hacker" para o esquema de Helder Barbalho. *O Antagonista*, 2020. Disponível em: https://oantagonista.uol.com.br/brasil/exclusivo-a-empresa-que-vendeu-a-maleta-hacker-para-o-esquema-de-helder-barbalho/. Acesso em: 5 maio 2024.

17 Uma matéria publicada na Revista Forbes demonstra o descaso com protocolos de segurança dos dados extraídos pela empresa Cellebrite, cujas ferramentas são vendidas em mercados clandestinos ainda com bancos de informações sensíveis sobre investigações realizadas. Sobre o tema: BREWSTER, Thomas. The Feds' favorite iPhone hacking tool is selling on eBay for $100 – and it's leaking data. *Forbes*, 27 fev. 2019. Disponível em: https://www.forbes.com/sites/thomasbrewster/2019/02/27/the-feds-favorite-iphone-hacking-tool-is-selling-on-ebay-for-100and-its-leaking-data/. Acesso em: 5 maio 2024.

18 O provedor de acesso à *internet* é o agente responsável por fornecer e garantir que o serviço de internet chegue até o local contratado pelo cliente. Portanto, é a empresa especializada nesse ramo e a responsável por desenvolver e manter a estrutura necessária para o acesso à internet em determinado lugar.

19 CELLEBRITE. *UFED Cloud*: product overview. 2020. Disponível em: https://cellebrite.com/wp-content/uploads/2020/05/ProductOverview_Cellebrite_UFEDCloud_web.pdf. Acesso em: 5 maio 2024.

20 G1. *Justiça autoriza empresa a extrair dados de celulares de Ronnie Lessa e Élcio Queiroz*. 1 ago. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/08/01/caso-marielle-justica-autoriza-pericia-particular-nos-celulares-de-ronnie-lessa-e-elcio-queiroz.ghtml. Acesso em: 5 maio 2024; e GI. *O que é o software usado pela polícia do Rio para investigar celulares no caso Henry Borel*. 8 abr. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/04/08/o-que-e-o-software-usado-pela-policia-do-rio-para-investigar-celulares-no-caso-henry-borel.ghtml. Acesso em: 5 maio 2024.

sociais, por exemplo. Considerando que o funcionamento da tecnologia é sigiloso (ao menos a própria empresa nunca esclareceu nada nesse sentido), tudo leva a crer que o sucesso do *software* se dá com a mescla, por exemplo, dessas duas opções, levando à conclusão de que o recurso tecnológico de uma (identificação de objetos e pessoas) é proveniente da extração de dados pessoais sensíveis de outra (armazenamento em nuvem por fontes abertas). Em ambos os casos, os dados são extraídos dos dispositivos analisados, em clara violação às bases legais para o tratamento de dados pessoais da LGPD, principalmente no que toca aos princípios da segurança, da prevenção, da responsabilização e da prestação de contas (Lei nº 13.709/2018, art. 6º, VII, VIII e X).[21]

Outros exemplos, dos quais também já foram requisitadas pelo poder público brasileiro: (i) *Pegasus*, que intercepta dados ao infectar dispositivos envolvidos em sistemas de comunicação; (ii) *Pixcell* e *GI2* (*IMSI Catchers*), que simulam estações rádio-base capturando dispositivos próximos; e (iii) o *First Mile* e *Landmark*, que rastreiam a localização de um alvo específico através da rede celular.[22]

As três ferramentas utilizam duas formas de invasão, através das tecnologias de *spyware* e *IMSI Catchers* (ou, no português, coletor de identidade de assinante móvel internacional), que, por sua vez, identifica um assinante forçando a transmissão do coletor de identidade de assinante móvel internacional (IMSI). Com a ajuda da operadora de telefonia/rede é possível determinar o número de telefone associado e, assim, permitir ao proprietário não apenas identificar, mas também grampear o telefone de saída de chamadas.[23]

No caso do *software* utilizado pela Agência Brasileira de Inteligência (ABIN), a qual justificou os projetos de lei aqui abordados, o First Mile é um *software* de monitoramento desenvolvido pela empresa israelense Cognyte (ex-Verint)[24] e adquirido

---

21 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, nº 157, p. 59-64, 15 ago. 2018.

22 Inclusive são essas as três tecnologias citadas na ADPF 1143.

23 Tradução nossa. Versão original: "The idea of an IMSI Catcher was originally to identify a subscriber by forcing to transmit the IMSI. With the help of the network operator, it is possible to determine the associated phone number. In 1997, the successor GA 900 allows the owner not only to identify, but also to tap outgoing phone calls" (STROBEL, Daehyun. *IMSI catcher*. Chair for Communication Security, Ruhr-Universität Bochum, v. 14, 2007, p. 17).

24 A Verint, incluindo suas representações locais em outros países, tem sido alvo de denúncias internacionais por fornecer tecnologias de interceptação de comunicações "em campo" para países com regime autoritário Sobre o tema ver: RAMIRO, André (Coord.); AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M. *Mercadores da insegurança*: conjuntura e riscos do *hacking* governamental no Brasil. Coordenação: André Ramiro. 1. ed. Recife: IP.rec, 2022, p. 54. O Relatório da Anistia Internacional documentou que a Israel Verint Systems Ltd, subsidiária da Verint Systems Inc., forneceu equipamentos de interceptação de comunicações ao governo do Sudão do Sul, o qual vem sistematicamente utilizando o conteúdo de comunicações interceptadas, assim como dados coletados de redes sociais, para prender arbitrariamente e constranger jornalistas e defensores de direitos humanos. Sobre o tema ver: ANISTIA INTERNACIONAL. "These walls have ears": the chilling effect of surveillance in South Sudan. London: Amnesty International, 2021. Disponível em: https://www.amnesty.org/en/documents/afr65/3577/2021/en/. Acesso em: 5 maio 2024.

pelo governo brasileiro no início de 2019, através do Contrato nº 567/2018, por dispensa de licitação e de caráter sigiloso, com início em 26/12/2018 e encerrado em 8/5/2021.[25]

De acordo com uma análise da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (Abimde),[26] o First Mile permite o rastreamento em tempo real de telefones celulares e é capaz de gerar alertas sobre a rotina de movimentação dos alvos de interesse, ou seja, avisos sobre a localização de pessoas vigiadas por meio desse programa. O *software* ainda usa sensores táticos e plataformas analíticas próprias para tratar os dados coletados.[27] O programa atua, portanto, com as duas formas de invasão tecnológica.

O que chama atenção desse *software* é seu funcionamento através das falhas de segurança quando do uso do Protocolo SS7 pelas empresas operadoras de telefonia.

Sobre o Protocolo SS7:

> The SS7 network controls many PTN features, e.g., basic call setup, management, tear down, billing and returning busy signals. It also supports advanced services such as local number portability (LNP), toll-free (800/888) and toll (900) services. Enhanced call features such as call forwarding, calling party name/number display, and threeway calling are also controlled. SS7 not only facilitates these and other new services, but also provides a more efficient and secure telecommunications network.[28]

As brechas na segurança do Protocolo SS7 permitem a entrada de ferramentas espiãs que interceptam a íntegra de mensagens de texto e chamadas de qualquer usuário, além de sua posição em tempo real. Essas ferramentas obtêm também, sem o consentimento dos usuários, informações de geolocalização e de conteúdo de dados armazenados nos dispositivos monitorados.

---

[25] PORTO, Douglas. Abin monitorou localização de pessoas pelo celular durante governo Bolsonaro. *CNN Brasil*, 14 mar. 2023. Disponível em: https://www.cnnbrasil.com.br/politica/abin-monitorou-localizacao-de-pessoas-pelo-celular-durante-governo-bolsonaro/. Acesso em: 3 maio 2024.

[26] ABIMDE. *Declaração de Não Similaridade*. 23 jul. 2021. Disponível em: https://apublica.org/wp-content/uploads/2023/10/D.N.S_011.21_COGNYTE_NOVA-Manifesto_Como-empresa-de-espionagem-israelense-alvo-da-PF-se-espalhou-pelo-poder-publico-no-Brasil.pdf. Acesso em: 3 maio 2024.

[27] Segundo o documento publicado, o *software* é um "Serviço de geolocalização de dispositivos móveis em tempo real, capaz de decodificar as identidades lógicas dos dispositivos e de gerar alertas sobre a rotina de movimentação dos alvos de interesse. Possui acesso remoto agnóstico a tipo de dispositivo e integração nativa com os sensores táticos COGNYTE (GI2), e as plataformas analíticas (Clarian). Utiliza a infraestrutura principal GMLC e Sistema de Sinalização por Canal Comum". Sobre o tema ver: ABIMDE. *Declaração de Não Similaridade*. 23 jul. 2021. Disponível em: https://apublica.org/wp-content/uploads/2023/10/D.N.S_011.21_COGNYTE_NOVA-Manifesto_Como-empresa-de-espionagem-israelense-alvo-da-PF-se-espalhou-pelo-poder-publico-no-Brasil.pdf. Acesso em: 3 maio 2024.

[28] LORENZ, G. *et al*. Securing SS7 telecommunications networks. *In*: *Workshop On Information Assurance and Security*, 2001. p. 274.

Todos os históricos, galeria de fotos e vídeos (inclusive apagados), mensagens de texto e áudio em aplicativos, histórico de geolocalização e seus metadados, entre outros, de celulares apreendidos são compartilhados com o Ministério da Justiça. Esses dados revelam uma série de informações dos investigados e das pessoas que se relacionam virtualmente com esses indivíduos investigados.

E são essas ferramentas que estão na mira do Poder Público, que permitem, através de um único acesso a um dispositivo pessoal, a possibilidade de alcance de um nível inédito de dados pessoais e comunicações, possibilitando traçar perfis de cidadãos a partir do cruzamento de inúmeros "data points" provenientes de dados de naturezas consideravelmente distintas, como localização, rastreamento de interações, buscas de pesquisa, conteúdo de comunicações, *likes*, fotos e vídeos, dados cadastrais, biometria e tantos outros. Em suma, na coleta e raspagem de dados, pode tudo e não há quaisquer limitações, regras ou premissas a serem observadas e respeitadas.

As empresas que fabricam essas tecnologias ganham voz na mídia porque os próprios veículos de comunicação auxiliam na propaganda sobre os feitos e funcionalidades retratadas por essas empresas.[29] Tudo é ainda mais alimentado com a forma midiática com que a criminalidade é retratada. A publicidade ganha a população porque gira em torno justamente de uma campanha de combate ao crime organizado através de tais ferramentas.

Em termos de proteção de dados, a regulamentação poderia iniciar seu caminho respondendo a alguns questionamentos: como seria realizada a coleta, o tratamento, o compartilhamento e o descarte dos dados pessoais provenientes de uma investigação? Quais os protocolos de segurança adotados nesses casos? Qual a segurança que se tem de vazamento desses dados nos mercados clandestinos?

As perguntas aqui elencadas, as quais foram feitas apenas a título exemplificativo (porque básicas, em se tratando de proteção de dados) não são respondidas nem pela Administração Pública (via Lei da Transparência – LIA), nem pelas empresas que comercializam os softwares invasivos. Responder a esses questionamentos é primordial para se pensar em uma futura legislação que autorize o uso dessas ferramentas.

Segundo Fernando Ameno, em todos os contratos celebrados entre a Techbiz e os estados e órgãos que compõem o governo federal, não havia nenhuma cláusula sobre proteção de dados – mesmo entre aqueles firmados após a vigência da

[29] MAGNET FORENSICS. *Magnet AXIOM*: Recover and analyze your evidence in one case. 2022. Disponível em: https://go.magnetforensics.com/AXIOM_Product_Brief. Acesso em: 5 maio 2024; CELLEBRITE. *Cellebrite UFED*: Product Overview. 2020. Disponível em: https://cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf. Acesso em: 5 maio 2024.

LGPD. No contrato com o Ministério Público Federal, há menção apenas genérica e que obriga apenas a questão do sigilo quando do tratamento dos dados.[30]

Sobre o descarte, ainda, as empresas sequer informam se o praticam e se o praticam corretamente. Conforme demonstrado neste trabalho, informações de comercialização de informações supostamente descartadas no mercado clandestino tem indicado justamente o contrário.

Técnicas menos invasivas de raspagem de dados, coleta mínima e descarte de informações não essenciais não demonstram prejuízo às investigações. Até porque sequer foi realizado um estudo de impacto dessas tecnologias sobre a vida e privacidade dos indivíduos, ou ainda de que, realmente, essas ferramentas são as únicas viáveis em termos de digitalização forense e combate à criminalidade digital.

3 A ADPF 1143 e os projetos de lei dela decorrentes

Apesar de avanços na legislação para proteger a intimidade, a vida privada e a inviolabilidade do sigilo das comunicações pessoais, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD), ainda não há uma regulamentação sobre programas de infiltração virtual remota.

Em 13.12.2023, a Procuradoria-Geral da República (PGR) ajuizou uma Ação Direta de Inconstitucionalidade por Omissão (ADO nº 84) em razão da *inertia deliberandi* em razão dos Projetos de Lei parados: PL 8045/2010, PL 276/2011, PL 480/2011, PL 6832/2013, PL 645/2015, PL 10724/2018, PL 4510/2020, PL 4939/2020, PL 199/2021, PL 465/2023, PL 3082/2023, PL 3226/2023, PL 5139/2023, PL 5302/2023, PL 6149/2023 e PL 58/2024. Pelo princípio da fungibilidade das ações constitucionais, a ADO foi transformada em ADPF (ADPF nº 1.143).[31]

O intuito da PGR é regular as hipóteses de invasão de aparelhos de particulares com base na tecnologia. Ao final, a PGR postula que seja julgado procedente o pedido, para:

> (i) declarar a inconstitucionalidade da omissão parcial do Congresso Nacional em tornar plenamente efetivos os mandamentos de proteção da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da CF, por meio da regulamentação do uso, por órgãos e agentes públicos,

[30] AMENO, Fernando. As planilhas de Bolsonaro: Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados, *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: 5 maio 2024.

[31] STF. *Arguição de Descumprimento de Preceito Fundamental nº 1.143*. Relator: Ministro Cristiano Zanin. Brasília, DF, 13 dez. 2023.

> de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – smartphones, tablets e dispositivos eletrônicos similares;
>
> (ii) fixar prazo razoável para que o Congresso Nacional supra a mora legislativa; e
>
> (iii) estabelecer balizas provisórias à salvaguarda dos direitos fundamentais à intimidade e à privacidade, e à inviolabilidade do sigilo das comunicações pessoais e de dados, até que seja sanada a lacuna normativa inconstitucional.[32]

Há, ao todo, dezoito pedidos liminares de tentativa de regulamentação da matéria. O principal deles é para que as Forças Armadas e órgãos de inteligência abstenham-se de utilizar ferramentas de invasão e monitoramento sem autorização judicial e à margem das balizas requeridas nesta ADPF, tais como:

> (i) termo de responsabilidade do órgão que capta e dos órgãos que recebem as informações;
>
> (ii) indicação do número do inquérito policial ou processo em curso;
>
> (iii) certificação de que a transferência de dados respeite as normas existentes;
>
> (iv) treinamento específico para investigadores, para que eles respeitem os direitos fundamentais dos investigados;
>
> (v) controle de log dos utilizadores das ferramentas e registros guardados por 30 anos; e
>
> (vi) descarte imediato de conversas de terceiros acidentalmente captadas pela IMSI Catcher.[33]

A fundamentação é extensa. Afirma a proliferação global de ferramentas de intrusão virtual, as quais são deliberadamente utilizadas em serviços de inteligência e órgãos de repressão estatais, assim como para vigilância remota, secreta e invasiva da vida dos cidadãos, tudo sob o pretexto do combate ao crime organizado e terrorismo.

A PGR junta o relatório elaborado pelo Gabinete do Alto Comissário das Nações Unidas para os Direitos Humanos, o qual aponta a ocorrência não só de violações à garantia do sigilo de dados e de comunicações, como também às garantias da intimidade, da vida privada e do devido processo legal, e ainda à liberdade de expressão, de manifestação do pensamento e de imprensa:

---

[32] STF. *Arguição de Descumprimento de Preceito Fundamental nº 1.143*. Relator: Ministro Cristiano Zanin. Brasília, DF, 13 dez. 2023.

[33] STF. *Arguição de Descumprimento de Preceito Fundamental nº 1.143*. Relator: Ministro Cristiano Zanin. Brasília, DF, 13 dez. 2023.

> O ponto central da controvérsia que a presente ação cinge-se ao uso secreto e abusivo desses softwares e ferramentas, sem autorização judicial, tampouco limites ou salvaguardas, de forma contrária à tutela do interesse público e aos deveres de proteção dos direitos fundamentais, que se impõem em um Estado de direito.
> [...]
> Ao não estabelecer a disciplina regulamentadora da utilização, por órgãos e agentes públicos, de programas para intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – smartphones, tablets e dispositivos eletrônicos similares – o legislador nacional incide em omissão contrária à exigência imposta no art. 5º, X e XII, da CF, provocando redução arbitrária e injustificada do nível de proteção das garantias. fundamentais previstas naquelas normas constitucionais, com ofensa ao princípio da proporcionalidade, derivado do postulado do devido processo legal (art. 5o, LIV, da CF), em sua dimensão substantiva.
> [...]
> Desse panorama, entende-se que, ao menos, existem diretrizes e condicionantes relevantes na legislação brasileira de proteção de dados pessoais a serem observadas, incumbindo a esta Suprema Corte consolidar e explicitar, nesta ação direta, as balizas sistêmicas que afastem arbitrariedades no uso, por órgãos e agentes públicos em atividades de inteligência ou investigação criminal, de programas de intrusão virtual remota e/ou de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal, como smartphones,tablets e dispositivos eletrônicos similares.[34]

Como contrapesos, a ADPF exige um termo de responsabilidade; o condicionamento do uso da ferramenta à indicação do número de inquérito policial, de procedimento investigativo ou de processo judicial; a certificação de que qualquer transferência, remessa ou compartilhamento de dados respeite as regras de sigilo existentes; respeito às regras de sigilo; redação de relatório circunstanciado da utilização da ferramenta; treinamento específico; controle e transparência por sistemas eletrônicos; autorização judicial específica; controle de *logs* de acesso e entradas condicionadas; e, por fim, o estabelecimento de sistema de registro inalterável.

A PGR quer, na verdade, regular as hipóteses de invasão de aparelhos de particulares com base na tecnologia. Os contrapesos sugeridos pela PGR não parecem concretos ou factualmente aptos a contrabalancear a intrusão decorrente da tutela pleiteada.

[34] STF. *Arguição de Descumprimento de Preceito Fundamental nº 1.143*. Relator: Ministro Cristiano Zanin. Brasília, DF, 13 dez. 2023.

Há preocupações ainda não endereçadas sobre a manutenção da cadeia de custódia, uma vez que a inserção de vírus em aparelho pode corromper de tal forma o código do dispositivo invadido que não se pode garantir a cadeia de custódia do material. Há preocupações relativas à serendipidade,[35] sobretudo nos casos de *IMSI Catchers*, tecnologias que simulam estações rádio-base capturando dispositivos próximos.[36]

O pedido da PGR é que a autoridade descarte o material acidentalmente captado. Qual seria, contudo, a repercussão jurídica do não descarte? Ela é compatível com as bases da proteção de dados?

Ao que tudo indica, a ADPF está intuindo regulamentar uma legislação que limita direitos fundamentais, o que sobremaneira não é objeto de uma ADPF. Caso fosse, seria entendido como uma "ADPF às avessas", porquanto não evidencia lesão a preceito fundamental com base em ato do Poder Público, mas sim tentativa de provocar a jurisdição para justamente restringir garantias individuais, o contrário do que versaria uma ADPF.

3.1 O PL 58/2024

O PL 58/2024, do deputado federal Alberto Fraga (PL-DF), foi apresentado em 20/02/2024 e apensado ao PL 199/2021 (o qual foi apensado ao PL 4510/2020) e disciplina a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso

[35] Serendipidade é o encontro fortuito de prova relacionada a fato diverso daquele que está sendo investigado. Doutrinariamente, é também denominada de crime achado e consiste na obtenção casual de elemento probatório de um crime no curso da investigação de outro. Sobre o tema: CAPEZ, Fernando. Serendipidade: o encontro fortuito de prova. *Consultor Jurídico*, 20 maio 2021. Disponível em: https://www.conjur.com.br/2021-mai-20/fernando-capez-serendipidade-encontro-fortuito-prova/. Acesso em: 5 maio 2024.

[36] A tecnologia IMSI Catchers pode ser capaz de capturar situações desencadeadoras de outras condutas criminosas, ou potencialmente criminosas (já que aqui fala-se somente em indícios). Essa tecnologia estaria dentro do que se entende por serendipidade (ou encontro fortuito de provas?). Independentemente de ser ou não positiva a resposta da pergunta anterior, o Superior Tribunal de Justiça entende plenamente cabível o fenômeno da serendipidade porque "o fato de as medidas de quebra do sigilo bancário e fiscal não terem como objetivo inicial investigar o crime de peculato não conduz à ausência de elementos indiciários acerca do referido crime" (BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 282.096/SP. Relator: Ministro Sebastião Reis Júnior. Sexta Turma. Julgado em: 24 abr. 2014. *DJe*, 6 maio 2014), ou ainda que "o denominado encontro fortuito de provas (serendipidade) é fato legítimo, refletido, no caso concreto, na descoberta, em interceptação telefônica judicialmente autorizada, do envolvimento de pessoas diferentes daquelas inicialmente investigadas, não gerando irregularidade a macular o Decreto de custódia cautelar ou o inquérito policial" (BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 77.003/SP. Relator: Ministro Joel Ilan Paciornik. Quinta Turma. Julgado em: 23 out. 2018. *DJe*, 9 nov. 2018, p. 1730). O Supremo Tribunal Federal, de igual forma, reputa legal que "nas interceptações telefônicas validamente determinadas é passível a ocorrência da serendipidade, pela qual, de forma fortuita, são descobertos delitos que não eram objetos da investigação originária" (BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 137.438. Relator: Ministro Luiz Fux. Primeira Turma. *DJe*, 20 jun. 2017, p. 124). Todas essas situações pacificadas na jurisprudência vão ao encontro de uma serendipidade em caso de IMSI Catchers?

de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências.[37]

Esse PL procura regulamentar o uso das novas tecnologias para as atividades de inteligência, investigação criminal, de controle ou fiscalização fazendária federais (art. 1º).[38] A redação, diferentemente do PL 402/2024, garante irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos (art. 1º, parágrafo único).

A finalidade de acesso a esses dados sigilosos, ao que tudo indica, está encartada na necessidade e relevância para o cumprimento da operação de inteligência estatal ou de investigação criminal, de controle ou de fiscalização fazendária federais (art. 2º).[39] Em todos os casos, a autorização judicial é imprescindível (art. 2º, parágrafo único).[40]

Há um rol de requisitos para autorização da medida (art. 3º),[41] bem como regras de procedibilidade sobre o uso dessas ferramentas tecnológicas (art. 4º).[42] O PL faz exigir também uma transparência nas normativas internas dos órgãos que farão uso

[37] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[38] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[39] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[40] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[41] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[42] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

dessa legislação e exige que sejam realizadas auditorias e rastreamentos nessas ferramentas tecnológicas e assinatura de termos de responsabilidade (art. 5º).[43]

O PL, por fim, também cuidou de assegurar a rastreabilidade da cadeia de custódia desses dados coletados (art. 6º, parágrafo único)[44] e prevê crime a utilização desses programas sem autorização judicial:

> Art. 7º Constitui crime utilizar programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal ou quebrar segredo da Justiça referente ao seu uso, sem autorização judicial ou com objetivos não autorizados em lei.
>
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> §1º Na mesma pena incorre quem autoriza ou permite armazenamento de dados ou de informações de que trata esta lei em sistemas de empresas privadas no exterior ou de governos estrangeiros.
> §2º A pena será aplicada em dobro ao agente público que descumprir a determinação de sigilo das investigações ou das operações que envolvam o uso de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal ou corporativa ou revelar o conteúdo dos dados durante o tempo do sigilo ou da classificação.[45]

Não houve apresentação de emendas. Na justificativa há a menção expressa da ADPF 1143, motivo principal da apresentação do texto legal. Outra justificativa dada é a possibilidade de redução da garantia dos direitos individuais fundamentais para que se tenha alguma margem de atuação das instituições e dos órgãos

[43] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[44] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[45] BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

encarregados de atuar contra a criminalidade e, curiosamente, mencionada expressamente, a espionagem.[46]

3.2 O PL 402/2024

Já o PL 402/2024, do senador Alessandro Vieira (MDB-SE), apresentado em 22.02.2024, coloca nas mãos do Congresso Nacional analisar a regulamentação do uso, pelo poder público, de ferramentas de monitoramento remoto em comunicações pessoais. A iniciativa pretende disciplinar a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares.[47]

Pela leitura e descrição do PL, os órgãos de segurança pública, dentre elas a força policial e ministérios públicos (federais e estaduais), assim como dos órgãos de inteligência e das Forças Armadas terão autorização de uso das ferramentas (art. 1º).[48] A prerrogativa deverá ser sucedida de prévia autorização judicial (art. 4º)[49] e poderá contar com auxílio dos provedores de internet (art. 6º).[50] As regras valerão de igual forma para programas de extração em massa de dados, assim como aqueles que acessam dados de conexão ou de geolocalização (art. 3º, parágrafo único).[51]

O uso de monitoramento remoto de celulares, tablets, notebooks e afins sem autorização judicial será passível de punição de dois a quatro anos, mais multa.

---

46 BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

47 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

48 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

49 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

50 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

51 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

Qualquer pessoa estará sujeita à penalização, com o dobro da pena caso o agente seja funcionário público:

> Art. 8º Constitui crime realizar o monitoramento remoto de terminais de comunicações pessoais sem a prévia autorização judicial:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> Parágrafo único. O agente público, civil ou militar, que realizar o monitoramento remoto sem a prévia autorização judicial terá a pena aplicada em dobro.[52]

Em qualquer caso é vedado o uso dos *softwares* se as informações se referirem a jornalistas ou advogados no exercício profissional (art. 4º, §5º).[53] A agência fiscalizadora será a Autoridade Nacional de Proteção de Dados – ANPD (art. 7º),[54] a mesma a que diz respeito a LGPD.[55]

No processo de tramitação do texto, já há a apresentação de três emendas parlamentares, todas do Senador Mecias de Jesus (Republicanos/RR). A Emenda nº 1-T acrescenta mais vedações ao §5º do artigo 4º do PL. A justificativa é que o sigilo profissional não é só com relação aos advogados e jornalistas, mas também aos médicos e profissionais da psicologia:

> §5º Não será admitida a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais para obtenção de informações que envolvam jornalistas, advogados, médicos, psiquiatras e psicólogos, no estrito exercício das respectivas atividades profissionais.[56]

---

52 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

53 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

54 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

55 O que de pronto já se verifica um problema porque a LGPD veda expressamente a regulação de proteção de dados para fins de inteligência, segurança pública e persecução penal, sendo sua agência fiscalizadora (a ANPD), até que se entenda o contrário, igualmente incompetente.

56 BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

A Emenda nº 2-T, por sua vez, acrescenta um artigo que elenca um requisito de procedibilidade em matéria processual penal, visando a equidade entre acusação e defesa:

> Art. – A partir da apresentação da denúncia pelo Ministério Público, os dados coletados dos indivíduos alvos do monitoramento remoto deverão estar totalmente acessíveis aos indivíduos monitorados, bem como ao requerimento de que trata o §1º do art. 4º, à decisão referida no §3º do art. 4º e ao relatório circunstanciado citado no §4º do art. 4º, a qualquer tempo, bem como aos seus advogados autorizados, no mesmo formato em que coletados.[57]

E, por fim, a Emenda nº 3-T acresce o §6º ao artigo 4º, do qual afirma a importância de cumprimento dos requisitos necessários à concessão da medida de monitoramento:

> §6º O requerimento de que trata o §1º é documento essencial, sob pena de nulidade do processo, vedada decisão de ofício, estando legitimados para sua apresentação os órgãos e agentes públicos de que trata o parágrafo único do art. 1º.[58]

Na justificativa deste PL também há a menção expressa da ADPF 1143, motivo principal da apresentação do texto legal. Outra justificativa dada é através do estudo realizado pelo Instituto de Pesquisa em Direito e Tecnologia do Recife, denominado Mercadores da Insegurança: Conjuntura e Riscos do Hacking Governamental no Brasil,[59] o qual identificou a existência de 209 contratos envolvendo a compra, o treinamento de funcionários, termos aditivos, atualização de softwares e outros atos administrativos, celebrados entre fornecedores de ferramentas de vigilância remota e órgãos públicos federais e estaduais entre os anos de 2015 e 2021. Os recursos aplicados pelos estados com essas ferramentas saltaram de R$522 mil para mais de R$45 milhões. Em nível federal, há uma evolução de gastos de R$5,7 milhões em 2016 para R$54 milhões em 2020. Tudo isso sem nenhuma previsão legal expressa a respeito.

---

[57] BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[58] BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

[59] 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.

4 Política pública de segurança pública ou política de segurança pública?

Políticas públicas são conjuntos de ações implementadas pelo Estado e pelas autoridades governamentais em um sentido amplo.[60] Os problemas enfrentados pelas políticas são pensados como processos eminentemente técnicos a serem resolvidos tecnicamente, enquanto um olhar analítico tende a considerar os mesmos processos como complexos.[61]

Há quatro tipos de políticas públicas, na concepção de Eduardo C. L. Marques:[62] as políticas constitutivas, em que há uma criação e transformação das próprias regras do jogo político; as políticas regulatórias, em que o Estado estabelece regras para o funcionamento de atividades produzidas externamente; as políticas distributivas, em que se discute os recursos não finitos ou mesmo ilimitados e cuja distribuição não geraria jogos de soma zero, mas de soma positiva; e, por fim, as políticas redistributivas, em que há a distribuição de recursos finitos, com jogos de soma zero intrinsecamente muito mais conflitiva, ou seja, para um grupo receber, o outro precisa necessariamente perder.

Uma política pública visa, portanto, o bem-estar da sociedade. A função de uma política pública está relacionada a ações bem desenvolvidas e à execução nas áreas da saúde, educação, segurança, meio ambiente, entre outras. As políticas públicas são ações direcionadas a todos os setores em que o Estado atua.

Por estar inserida em áreas sensíveis da sociedade, as políticas públicas deveriam ser consideradas políticas de Estado. Entretanto, são comumente encaradas como políticas de governo. A depender de quem ocupa a cadeira da Presidência da República, haverá uma forma de interpretação das carências sociais e, com isso, a adoção de diferentes medidas.

Em um país onde as ações do poder público são centralizadas, pouco transparentes, orientadas muitas vezes pelo viés político, o que as tornam paliativas, é fundamental que se compreenda a formulação das políticas públicas. As ações são eminentemente estatais, mas a participação popular é importante.

Antigamente pensava-se em políticas públicas a partir de uma certa racionalidade. Hoje, as políticas públicas são pensadas mais a partir de uma perspectiva

---

60 MARQUES, Eduardo C. L. As políticas públicas na ciência política. *In*: MARQUES, Eduardo; FARIA, Carlos Aurélio Pimenta de (Org.). *A política pública como campo multidisciplinar*. São Paulo: Editora UNESP; Rio de Janeiro: Editora Fiocruz, 2013. p. 24.

61 MARQUES, Eduardo C. L. As políticas públicas na ciência política. *In*: MARQUES, Eduardo; FARIA, Carlos Aurélio Pimenta de (Org.). *A política pública como campo multidisciplinar*. São Paulo: Editora UNESP; Rio de Janeiro: Editora Fiocruz, 2013. p. 25.

62 MARQUES, Eduardo C. L. As políticas públicas na ciência política. *In*: MARQUES, Eduardo; FARIA, Carlos Aurélio Pimenta de (Org.). *A política pública como campo multidisciplinar*. São Paulo: Editora UNESP; Rio de Janeiro: Editora Fiocruz, 2013. p. 25.

de conveniência política do que a partir de uma racionalidade propriamente dita. Esse momento de críticas da racionalidade quando da criação de políticas públicas foi iniciado porque entendia-se que se deveria não apenas adotá-las com base em decisões racionais, mas também com base em pequenas decisões subsequentes (como forma de política incremental).

Em se tratando de racionalidade, Díez Ripollés, ao falar sobre sua teoria da decisão racional, defende que o conhecimento profundo do processo sociológico e legislativo é o que deveria conduzir as decisões no âmbito legislativo.[63] Esse conhecimento profundo é trifásico: pré-legislativa (disfunção social que pode acarretar em responsabilização penal); parlamentar (debate pela iniciativa legislativa de projetos de lei); e pós-legislativa (após sancionada, verifica-se que a lei não soluciona o problema encontrado na fase pré-legislativa). O controle deve(ria) ocupar-se de condutas que afetam diretamente a convivência social e efetivamente danosas.

É preciso ter em mente que a racionalidade política também permeia as práticas legislativas. O comportamento político tem sua própria racionalidade e é estratégico na teoria dos jogos na ciência política e na análise dos processos de cooperação e interação coletiva no âmbito do Poder Legislativo.

Uma racionalidade política não se traduz em justificação propriamente, até porque a legislação é fruto da política, seja em razão das escolhas fundamentais da Constituição, seja também porque as leis igualmente são capazes de estabelecer políticas. Deve-se prestar atenção às motivações internas ao direito. A racionalidade legislativa encontra dificuldades quando encara os cálculos mentais (prós e contras), assim como as negociações (toma-lá-dá-cá ou *quid pro quod* político — as retaliações).

Em termos de segurança pública, a situação ganha contornos ainda mais delicados. Não há consenso sobre criação de políticas públicas nas atividades da segurança pública. E tampouco há consenso sobre o que seriam essas atividades.

As atividades de segurança pública podem ser definidas como um conjunto de dispositivos e de medidas de precaução que asseguram a população de estar livre do perigo, de danos e riscos eventuais à vida e ao patrimônio, bem como um conjunto de processos políticos e jurídicos destinados a garantir a ordem pública na convivência pacífica dos seres humanos na sociedade.[64]

Hoje o Brasil conta com algumas políticas públicas que atuam na área da segurança pública, valendo-se mencionar do SUSP (O Sistema Único de Segurança Pública), instituído pela Lei nº 13.675/2018 e visa integrar os órgãos de segurança

[63] DÍEZ RIPOLLÉS, José Luis. La racionalidad legislativa penal: decisiones en un procedimiento socio-legislativo complejo. *In*: OLIVER-LALANA, A. D. (ed.). *La legislación en serio*: estudios sobre derecho y legisprudencia. Valencia: Tirant lo Blanch, 2019.

[64] VEDOVA, Daiane. O que é segurança pública. *Jusbrasil*, 2017. Disponível em: https://www.jusbrasil.com.br/artigos/o-que-e-seguranca-publica/586735267. Acesso em: 8 dez. 2023.

e inteligência; padronizar informações, estatísticas e procedimentos; entre diversas outras medidas visando a integração das forças de segurança.

Desde sua implementação, nada foi feito concretamente para que esse novo modelo de governança do sistema de segurança pública na sociedade brasileira saísse do papel. Branco[65] afirma que, por causa das peculiaridades da Segurança Pública, houve a necessidade de se criar um subsistema de inteligência dentro do SISBIN,[66] que reunisse todos aqueles que têm a Segurança Pública como missão principal.

Pensando nisso, o Decreto Presidencial nº 3.695/2000 criou o Subsistema de Inteligência de Segurança Pública (SISP).[67] O art. 1º já expõe:

> Fica criado, no âmbito do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999, o Subsistema de Inteligência de Segurança Pública, com a finalidade de coordenar e integrar as atividades de inteligência de segurança pública em todo o País, bem como suprir os governos federal e estaduais de informações que subsidiem a tomada de decisões neste campo.[68]

A intenção do legislador em criar o SISP dentro do SISBIN foi para subsidiar o processo decisório na esfera da Segurança Pública, de amplitude nacional e efetivamente integrando todos os órgãos que, de uma maneira ou outra, lidam com o tema Segurança Pública. Buscava-se, com isso, mudar uma dura realidade ainda presente nas decisões tomadas na área de Segurança Pública que afetam diretamente a segurança percebida pelos cidadãos, qual seja a de as decisões serem tomadas unicamente baseadas em experiências individuais, privilegiando-se, muitas vezes, aspectos de cunho político, sem contar com outras informações trabalhadas de maneira isenta e profissional.[69]

Nas palavras de Mingardi,[70] não há informações suficientes sobre o trabalho policial. E não se fala somente de trabalho policial, mas em toda a atividade de

---

65 CASTELLO BRANCO, André Haydt. *Doutrina nacional de inteligência de segurança pública*. Tubarão: Unisul, 2011, p. 18.

66 O Sisbin abrange o conjunto de órgãos e entidades que desenvolvem, de forma integrada e cooperativa, ações de planejamento e execução das atividades de inteligência e contrainteligência (art. 2º, parágrafo único, do Decreto nº 11.693/23).

67 A grande meta do SISP é, portanto, propiciar aos governantes condições para a tomada de decisões com base em informações trabalhadas de maneira profissional, na área da Segurança Pública.

68 BRASIL. Decreto nº 3.695, de 21 de dezembro de 2000. Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, p. 77, 22 dez. 2000.

69 BRANCO, André Haydt Castello; SCHAUFFER, Fred Harry; LENTO, Luiz Otávio Botelho. *Inteligência e segurança pública*: livro didático. Design instrucional: Marina Melhado Gomes da Silva. Palhoça: UnisulVirtual, 2014, p. 30.

70 MINGARDI, Guaracy. *A investigação de homicídios*: construção de um modelo. Relatório de pesquisa. Brasília, DF: MJ/SENASP, 2006, p. 9.

inteligência que permeia a área da segurança pública. Informações teóricas sobre e seus escopos de atuação sim, mas seu conteúdo mostra apenas o ponto de vista jurídico, jamais o operacional.

E quanto o debate adentra sobre a atuação das polícias para o enfrentamento da criminalidade (principalmente a criminalidade econômica) com o uso de técnicas que correspondem à digitalização das dinâmicas sociais, a linha tênue entre a otimização de processos por um lado e as transgressões aos direitos fundamentais e de proteção de dados de outro fica ainda mais evidente.

As rotinas de vigilância através do *hacking* governamental,[71] segundo estudos coletados pelo Fundo de Resposta Rápida da ONG *Derechos Digitales*, entre o período de 2015 e 2021 foram encontrados 209 documentos contratuais envolvendo o uso de novas tecnologias, sendo 182 estaduais e 27 federais. O gasto público dessas contratações foi, no âmbito estadual, de R$522 mil reais em 2015 para R$45 milhões de reais em 2021 e, no âmbito federal, de R$5 milhões em 2016 para R$54milhões em 2020.[72]

Esmiuçando as tecnologias contratadas, o estudo elencou que ferramentas como *Cellebrite*, cuja destinação, como já estudado neste artigo, é a extração de dados com os aparelhos em mãos, demonstram uma capilaridade significativa em órgãos de segurança pública. A inserção se dá, especialmente, em órgãos voltados para investigação, como Polícia Civil, Ministérios Públicos e setores de criminalística. Entretanto, São Paulo, Paraíba e Minas Gerais alocaram essas tecnologias na Polícia Militar, órgão que não possui função de investigação.[73]

No caso de ferramentas como a *Verint*, cuja finalidade é amplo acesso remoto em dispositivos informáticos, as soluções são adquiridas em grande maioria pelo Ministério da Defesa. Em casos como a Intervenção Federal no Rio de Janeiro, em 2016, as ferramentas que foram adquiridas não foram reveladas.[74] O estudo

---

71 Expressão ainda não utilizada neste artigo. Hacking, do ponto de vista técnico, é a exploração de uma vulnerabilidade, seja ela intencional ou não, conhecida ou não, pelo fabricante, que resulte no acesso não-autorizado a uma informação, seja comunicação ou dados em repouso ou em trânsito; e, do ponto de vista comportamental, é a exploração que envolve intencionalidade, ou seja, o propósito de alcançar aquela informação por meio do desvio do que seria um sistema de segurança. Governamental, por sua vez, é o conjunto de agências de entidades pertencentes ao corpo estatal. Sobre o tema: 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. p. 10.

72 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, p. 51.

73 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, p. 51

74 Segundo esse estudo, foram acionados por meio da Lei de Acesso à Informação, em âmbito estadual, as 27 Secretarias responsáveis por atividades de segurança pública, assim como os respectivos Ministérios Públicos estaduais. No campo federal, pelo mesmo mecanismo, foram solicitadas informações ao Ministério Público Federal e à Polícia Federal através do Ministério da Justiça e Segurança Pública, ao Ministério da Defesa, Comando do Exército (CEX), Comando da Marinha (CMAR) e ao Gabinete de Segurança Institucional. No caso das Secretarias estaduais, 5 delas não responderam aos pedidos. Já para os Ministérios Públicos

identificou que essa ausência de transparência é tratada em diversos outros portais públicos, que ou não divulgam a aquisição, ou as divulgam com informações incompletas.

O *déficit* de informações é também qualitativo, visto que, muitas vezes, sequer há descrição no contrato sobre produto ou serviço adquirido. O mesmo vale para contratos com entes federais, ficando difícil saber o quê e quanto foi adquirido.[75]

De acordo com Pedro Amaral,[76] as leis comumente usadas para negar acesso a informações solicitadas via SIC são a Lei nº 9.883/1999 (SISBIN);[77] a Lei nº 12.850/2013 (Lei das Organizações Criminosas);[78] a própria Lei nº 12.527/2011 (Lei de Acesso à Informação);[79] e, finalmente, a Política Nacional de Inteligência, instituída pelo Decreto nº 8.793/2016, regulamentando a Lei nº 9.883/99.[80] Algumas justificativas, entretanto, sequer foram embasadas em legislações vigentes, apenas afirmando ser sigilosas "por interesse do Estado".

Estaduais, 5 pedidos foram inviabilizados ou seguem tramitando e sem resposta conclusiva.91 No âmbito federal, todas as instituições responderam aos pedidos. Os problemas na obtenção de respostas também incluem plataformas de difícil acesso ou mesmo completamente inacessíveis, como no caso de Alagoas, que permaneceu de meados de março até o fim de julho de 2022 fora do ar. Sobre o tema: 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, p. 51.

75 Há uma amplitude de terminologias para a mesma finalidade das ferramentas, que vão desde "dados em nuvem" e "dados de redes sociais" até "artefatos de Internet" para significar o acesso a dados pessoais de forma ampla. Ou mesmo uma variedade de terminologias para se referir à natureza da ferramenta em si, como "solução de inteligência tática", "software de perícia forense", "ciber inteligência", "software para laboratório de forense digital" ou mesmo "solução para coleta, processamento e análise de dados e informações a partir de plataformas eletrônicas portáteis". Sobre o tema: 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, p. 51.

76 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, p. 56

77 Art. 3º, parágrafo único: as atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos. Sobre o tema: BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 8 dez. 1999.

78 Art. 3º, §1º, sobre a necessidade de proteção pelo Estado de sua capacidade investigatória através da manutenção e guarda de sigilo sobre suas metodologias, recursos técnicos e atividades especializadas (BRASIL. Lei nº 12.850, de 02 de agosto de 2013. Abre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Brasília, DF. *Diário Oficial da União*, 05/08/2013).

79 A qual admite exceções à transparência com base no Art. 23, inciso VIII, apontando a exceção visando à preservação de "atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações". Sobre o tema: BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Brasília, DF. *Diário Oficial da União*, 18/11/2011).

80 Que reafirma que as "atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado" (BRASIL. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. Brasília, DF. *Diário Oficial da União,* 29/06/2016).

Utilizar as próprias regras de transparência como forma de manipulação para dar opacidade às informações solicitadas permite que os atores públicos empreguem vários níveis de arbitrariedades, além de corroborar com uma ideia de existir um poder crescente de devassa das informações e acúmulo injustificável de dados pessoais pelos agentes desse mesmo Estado. Ao negar informações essenciais sobre o tratamento dos dados pessoais, o Estado impede o controle externo de sua atividade sobre esses mesmos dados.

Essa tendência à declaração de sigilo em relação às informações requisitadas, principalmente através dos canais à disposição do cidadão (Portais da Transparência e Serviços de Informação ao Cidadão – SIC, via de exemplo), a qual refere-se para a grande maioria de informações sobre contratação, armazenamento e utilização dessas ferramentas tecnológicas, corrobora com a ideia de militarização da segurança pública.[81]

A militarização da segurança pública é um processo antigo, crescente sobretudo no período da Guerra Fria, em que as preocupações de combate à criminalidade significaram uma mudança paradigmática na forma como se percebe e se atua em temas de segurança. A narrativa da "guerra às drogas", inaugurada nos anos 1970, teria ressurgido nos anos 1990 como importante justificador da militarização das polícias e da policialização das forças armadas nos Estados Unidos.[82] Uma das principais mudanças se referiu à atuação dos militares, que, antes destinados exclusivamente à defesa do território nacional em contextos de guerra, passaram a agir e "exportar" suas práticas para o trato de temas relacionados usualmente à segurança pública.[83]

O uso de dispositivos informáticos e tecnológicos como escopo de "guerra ao crime" e "guerra às drogas", ou ainda "combate ao terrorismo", entre outros, utiliza da lógica militar de combate ao inimigo a todo custo, devendo esse ser de pronto neutralizado. Isso abre brecha para um controle operacional e informacional, por parte do poder público (e consequentemente de empresas que negociam com o poder público nesses casos), que cria assimetrias de poder e coloca o Estado como detentor de todo o conhecimento e informação existente.

---

81 Na base dessa concepção está o pressuposto de que o policiamento militarizado estaria gerando efeitos perversos à sociedade e à democracia. Militarizar a polícia e policializar as forças armadas teria como principal resultado o aumento da violência contra o cidadão, que deveria ser o foco da proteção, fragilizando as instituições democráticas e incentivando caminhos autoritários. Sobre o tema: PEREIRA, P.; VILLELA, P. Militarização do policiamento: abordagens críticas em perspectiva. 90, 1-20, 2019. p. 15. Disponível em: https://doi.org/10.17666/bib9001/2019. Acesso em 05 maio 2024.

82 PEREIRA, Paulo; VILLELA, Priscila. Militarização do policiamento: abordagens críticas em perspectiva. *BIB – Revista Brasileira de Informação Bibliográfica em Ciências Sociais*, nº 90, p. 1-20, 2019, p. 3. Disponível em: https://doi.org/10.17666/bib9001/2019. Acesso em: 5 maio 2024.

83 ANDREAS, Peter; PRICE, Richard *apud* PEREIRA, Paulo; VILLELA, Priscila. Militarização do policiamento: abordagens críticas em perspectiva. *BIB – Revista Brasileira de Informação Bibliográfica em Ciências Sociais*, nº 90, p. 1-20, 2019, p. 3. Disponível em: https://doi.org/10.17666/bib9001/2019. Acesso em: 5 maio 2024.

Ter compreensão disso é essencial para levantar questionamentos sobre a natureza do tipo de banco de dados que está sendo construído pelo poder público com o uso do *hacking* governamental. Além dos riscos envolvidos no que concerne aos direitos de privacidade, proteção de dados e também dos direitos humanos para o uso dessas ferramentas, qualquer política pública pautada nessas informações estaria comprometida, em especial aquelas que utilizam de *machine learning* como base de funcionamento (cita-se aqui justamente as ferramentas que são objeto da ADPF 1143).

5 Conclusão

O presente trabalho procurou responder ao seguinte problema de pesquisa: com essas novas tecnologias e nova sociedade em perspectiva, quais seriam as balizas essenciais que autorizam a regulamentação das tecnologias invasivas? Essas balizas existem atualmente? A regulamentação hoje representa uma ameaça à privacidade?

Considerando as tecnologias já utilizadas pelo poder público, não há nenhuma aderência aos princípios estampados na LGPD. Pelo contrário, conforme se verificou, a utilização dessas tecnologias viola pelo menos quatro princípios da lei: segurança, prevenção, responsabilização e prestação de contas (Lei 13.709/2018, art. 6º, VII, VIII e X).[84]

Isso porque, em tese, pode-se coletar toda sorte de dados pessoais e assim tratá-los, compartilhá-los e descartá-los. Sobre o descarte, a situação toma contornos ainda mais delicados: há descarte? Não se sabe. E não se sabe porque não há o dever de informação a seu respeito, tampouco há o dever de justificar sobre a necessidade, finalidade e coleta desses dados, como tudo é feito, se é feito de forma subjetiva ou se há uma lógica por trás.

Quando analisada a situação sob o contexto de políticas públicas, verifica-se um lapso e uma falta de transparência pública quanto às informações coletadas através das tecnologias contratadas para fins de segurança pública. Qualquer operação que pretenda gerar confiança acerca de sua legitimidade e integridade deve vir acompanhada de mecanismos de supervisão e controle institucional, bem como deve necessariamente passar pela garantia de publicidade aos tipos, escopo e finalidades específicas de usos de dados. Isso, no atual cenário, não existe.

A hipótese de partida é, assim, confirmada, no sentido de que não há a menor possibilidade hoje de administrar o uso dessas ferramentas sem que antes se

[84] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet. *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

crie um plano mínimo que responda a premissas básicas de segurança e proteção de dados. A administração pública deve, antes de querer regulamentar essas tecnologias a qualquer custo, iniciar uma cultura de proteção de dados (i) criando regras para produção dessas tecnologias; (ii) contratando pessoas capacitadas que saibam lidar com essas novas tecnologias, porque a terceirização desses serviços no contexto da segurança pública é forma de delegação de atos administrativos e o poder de polícia é indelegável,[85] não podendo o poder público ficar dependente das empresas que fornecem as ferramentas tecnológicas para extração e tratamento dos dados que delas se adquirem; e (iii) por fim, somente aqui, regulamentar o uso das ferramentas, dos algoritmos e demais iniciativas tecnológicas de utilização no âmbito da segurança pública.

Outro eixo relevante deve ser a especificação, via regulamentação própria, de conceitos sobre tecnologias de monitoramento; se são equipamentos, programas de computador ou sistemas informáticos; se podem ser utilizados ou implementados para o tratamento de dados pessoais captados em vídeo, imagem, texto ou áudio; se essas tecnologias são condicionadas à previsão legal específica (por exemplo, especificidade dos tipos de algoritmos) ou se será uma previsão genérica. Sobre os critérios dessas tecnologias, deve haver também previsão específica de como, quando e de que forma serão utilizadas. Deve também necessariamente a contratação de determinadas tecnologias pelo poder público vir acompanhada de análise de impacto regulatório e de relatório de impacto à proteção de dados.

Por fim, no que diz respeito à natureza dos dados envolvidos, devem ser especificadas as finalidades específicas do tratamento ou mesmo a possibilidade de tratamento discriminatório como critérios mínimos para avaliação de utilização das tecnologias.

Da mesma forma que a tecnologia permite realizar coisas que antes eram impensadas, em termos de segurança pública e dentro de um contexto de privacidade e proteção de dados (contexto esse do qual já deveria ser escopo de preocupação da Administração Pública), é possível que essa mesma tecnologia seja pensada de forma a restringir o algoritmo para pesquisa de apenas o necessário, cumprindo como devem ser cumpridos os princípios estampados na LGPD. Sabe-se que o algoritmo que hoje alcança um sem-número de informações de pesquisa pode também ser restringido a ponto de captar apenas o que interessa para determinada diligência

[85] A restrição à atribuição de atos de polícia a particulares estaria alicerçada no corretíssimo entendimento de que não se lhes pode, ao menos em princípio, cometer o encargo de praticar atos que envolvem o exercício de misteres tipicamente públicos quando em causa liberdade e propriedade. Isso porque, caso contrário, haveria um desequilíbrio entre os particulares, ao passo que o ordenamento definiria que certos entes privados teriam supremacia sobre outros. Conclui, portanto, que não há delegação de ato jurídico de polícia a particular e nem a possibilidade de que este o exerça a título contratual. Sobre o tema: BANDEIRA DE MELLO, Celso Antônio. *Curso de direito administrativo*. 32. ed. São Paulo: Malheiros, 2015, p. 863-865.

policial, basta que as empresas que desenvolvem esses produtos sejam inicialmente compelidas a pensar nessas tecnologias em um contexto de privacidade para, depois, a partir de regras predeterminadas, conduzir essas ferramentas sob uma perspectiva da privacidade e proteção de dados.

Hoje, além da realidade retratar um contexto de recorrentes violações a garantias individuais, já que o poder público se utiliza de ferramentas que restringem direitos sem qualquer regulamentação e regras a respeito, há uma tentativa de legalizar essas violações, de modo que seja impossível, amanhã, reclamar e reivindicar esses direitos violados. Assim como as questões ambientais hoje clamam por atenção, porque há muito não se vinha pensando a seu respeito, com a privacidade e a proteção de dados pode ser diferente se, desde já, seja realizado um plano de ação de prevenção e manutenção desses direitos.

A ADPF, que poderia ser uma ferramenta de resguardo das garantias individuais (até porque esse seria o fim precípuo de uma ADPF – ação de descumprimento de preceito fundamental), no fundo se prestaria a regular precipuamente as hipóteses de restrição de direitos fundamentais e não necessariamente a sua promoção. Os projetos de lei que seguem sua lógica, de igual forma, não garantem proteção a direitos fundamentais, mas sim autorizam sua redução e limitação.

Referências

ABIMDE. *Declaração de Não Similaridade*. 23 jul. 2021. Disponível em: https://apublica.org/wp-content/uploads/2023/10/D.N.S_011.21_COGNYTE_NOVA-Manifesto_Como-empresa-de-espionagem-israelense-alvo-da-PF-se-espalhou-pelo-poder-publico-no-Brasil.pdf. Acesso em: 3 maio 2024.

AMENO, Fernando. As planilhas de Bolsonaro: Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados. *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: 5 maio 2024.

ANISTIA INTERNACIONAL. *"These walls have ears"*: the chilling effect of surveillance in South Sudan. London: Amnesty International, 2021. Disponível em: https://www.amnesty.org/en/documents/afr65/3577/2021/en/. Acesso em: 5 maio 2024.

BANDEIRA DE MELLO, Celso Antônio. *Curso de direito administrativo*. 32. ed. São Paulo: Malheiros, 2015.

BRANCO, André Haydt Castello; SCHAUFFER, Fred Harry; LENTO, Luiz Otávio Botelho. *Inteligência e segurança pública*: livro didático. Design instrucional: Marina Melhado Gomes da Silva. Palhoça: UnisulVirtual, 2014.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988. Disponível em: https://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-publicacaooriginal-1-pl.html. Acesso em: 2 maio 2024.

BRASIL. *Decreto nº 3.695, de 21 de dezembro de 2000*. Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências. *Diário Oficial da União: seção 1*, Brasília, DF, p. 77, 22 dez. 2000.

BRASIL. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. *Diário Oficial da União: seção 1*, Brasília, DF, 30 jun. 2016.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. *Diário Oficial da União: seção 1*, Brasília, DF, 8 dez. 1999.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União: seção 1*, Brasília, DF, 18 nov. 2011.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. *Diário Oficial da União: seção 1*, Brasília, DF, 5 ago. 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD. *Diário Oficial da União: seção 1*, Brasília, DF, ano 155, nº 157, p. 59-64, 15 ago. 2018.

BRASIL. Senado Federal. *Projeto de Lei nº 58, de 2024*. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 402, de 2024*. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 5 maio 2024.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 282.096/SP. Relator: Ministro Sebastião Reis Júnior. Sexta Turma. Julgado em: 24 abr. 2014. *DJe*, 6 maio 2014.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 77.003/SP. Relator: Ministro Joel Ilan Paciornik. Quinta Turma. Julgado em: 23 out. 2018. *DJe*, 9 nov. 2018.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6.393. Relatora: Ministra Rosa Weber. Tribunal Pleno. Julgada em: 7 maio 2020. *DJe*, 12 nov. 2020.

BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 1.143*. Relator: Ministro Cristiano Zanin. Brasília, DF, 13 dez. 2023.

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 137.438. Relator: Ministro Luiz Fux. Primeira Turma. *DJe*, 20 jun. 2017.

BREWSTER, Thomas. The Feds' favorite iPhone hacking tool is selling on eBay for $100 – and it's leaking data. *Forbes*, 27 fev. 2019. Disponível em: https://www.forbes.com/sites/thomasbrewster/2019/02/27/the-feds-favorite-iphone-hacking-tool-is-selling-on-ebay-for-100and-its-leaking-data/. Acesso em: 5 maio 2024.

CAPEZ, Fernando. Serendipidade: o encontro fortuito de prova. *Consultor Jurídico*, 20 maio 2021. Disponível em: https://www.conjur.com.br/2021-mai-20/fernando-capez-serendipidade-encontro-fortuito-prova/. Acesso em: 5 maio 2024.

CASTELLO BRANCO, André Haydt. *Doutrina nacional de inteligência de segurança pública*. Tubarão: Unisul, 2011.

CELLEBRITE. *Cellebrite UFED*: product overview. 2020. Disponível em: https://cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf. Acesso em: 5 maio 2024.

CELLEBRITE. *Extração e desbloqueio avançados*: Cellebrite Advanced Services. 2020. Disponível em: https://cellebrite.com/en/cellebrite-announces-formation-of-ethics-integrity-committee/. Acesso em: 5 maio 2024.

CELLEBRITE. *UFED Cloud*: product overview. 2020. Disponível em: https://cellebrite.com/wp-content/uploads/2020/05/ProductOverview_Cellebrite_UFEDCloud_web.pdf. Acesso em: 5 maio 2024.

DANTAS, Claudio. Exclusivo: a empresa que vendeu a "maleta hacker" para o esquema de Helder Barbalho. *O Antagonista*, 2020. Disponível em: https://oantagonista.uol.com.br/brasil/exclusivo-a-empresa-que-vendeu-a-maleta-hacker-para-o-esquema-de-helder-barbalho/. Acesso em: 5 maio 2024.

DÍEZ RIPOLLÉS, José Luis. La racionalidad legislativa penal: decisiones en un procedimiento socio-legislativo complejo. *In*: OLIVER-LALANA, A. D. (ed.). *La legislación en serio*: estudios sobre derecho y legisprudencia. Valencia: Tirant lo Blanch, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais*, v. 156, p. 353-393, jun. 2019.

GI. *Justiça autoriza empresa a extrair dados de celulares de Ronnie Lessa e Élcio Queiroz*. 1º ago. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/08/01/caso-marielle-justica-autoriza-pericia-particular-nos-celulares-de-ronnie-lessa-e-elcio-queiroz.ghtml. Acesso em: 5 maio 2024.

LORENZ, G. *et al*. Securing SS7 telecommunications networks. *In*: *Workshop On Information Assurance and Security*, 2001. p. 274.

MAGNET FORENSICS. *Magnet AXIOM*: recover and analyze your evidence in one case. 2022. Disponível em: https://go.magnetforensics.com/AXIOM_Product_Brief. Acesso em: 5 maio 2024.

MARQUES, Eduardo C. L. As políticas públicas na ciência política. *In*: MARQUES, Eduardo; FARIA, Carlos Aurélio Pimenta de (Org.). *A política pública como campo multidisciplinar*. São Paulo: Editora UNESP; Rio de Janeiro: Editora Fiocruz, 2013.

MINGARDI, Guaracy. *A investigação de homicídios*: construção de um modelo. Relatório de pesquisa. Brasília, DF: MJ/SENASP, 2006.

G1. *O que é o software usado pela polícia do Rio para investigar celulares no caso Henry Borel. 2021*. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/04/08/o-que-e-o-software-usado-pela-policia-do-rio-para-investigar-celulares-no-caso-henry-borel.ghtml. Acesso em: 5 maio 2024.

PATIL, Manjugouda R.; MULIMANI, C. F. Pegasus: transforming phone into a spy. *Think India Journal*, v. 22, nº 14, p. 7883-7890, 2019.

PEREIRA, Paulo; VILLELA, Priscila. Militarização do policiamento: abordagens críticas em perspectiva. *BIB – Revista Brasileira de Informação Bibliográfica em Ciências Sociais*, nº 90, p. 1-20, 2019. Disponível em: https://doi.org/10.17666/bib9001/2019. Acesso em: 5 maio 2024.

PORTO, Douglas. Abin monitorou localização de pessoas pelo celular durante governo Bolsonaro. *CNN Brasil*, 14 mar. 2023. Disponível em: https://www.cnnbrasil.com.br/politica/abin-monitorou-localizacao-de-pessoas-pelo-celular-durante-governo-bolsonaro/. Acesso em: 3 maio 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.

STROBEL, Daehyun. *IMSI catcher*. Chair for Communication Security, Ruhr-Universität Bochum, v. 14, 2007.

VALENTE, Rubens. Ação sigilosa do governo mira professores e policiais antifascistas. *UOL Notícias*, 24 jul. 2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/07/24/ministerio-justica-governo-bolsonaro-antifascistas.htm. Acesso em: 5 maio 2024.

VEDOVA, Daiane. O que é segurança pública. *Jusbrasil*, 2017. Disponível em: https://www.jusbrasil.com.br/artigos/o-que-e-seguranca-publica/586735267. Acesso em: 8 dez. 2023.

VELÁSQUEZ, Rafael. Desafios da investigação criminal tecnológica. *Techbiz Forense Digital*, 2022. Disponível em: https://techbiz.com.br/wp-content/uploads/2022/06/Artigo-Desafios-da-investigacao-criminal-tecnologica.pdf. Acesso em: 5 maio 2024.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, nº 5, p. 193-220, 1890.

Informação bibliográfica deste texto, conforme a NBR 6023:2025 da Associação Brasileira de Normas Técnicas (ABNT):

BALDISSERA, Rafaela dos Reis. A violação da privacidade como política pública: por que a autorização de uso dos *softwares* espiões hoje é equivocada. *International Journal of Digital Law*, Belo Horizonte, v7, e707, 2026. DOI: 10.47975/ijdl.v7.1324.

Informações adicionais

Additional information

Editores responsáveis	
Editor-Chefe	Emerson Gabardo
Editor-Adjunto	Lucas Raphael de Souza Mano