XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

GUSTAVO RABAY GUERRA

JOSÉ RENATO GAZIERO CELLA

JÉSSICA FACHIN

I61

Internet: dinâmicas da segurança pública internacional[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Gustavo Rabay Guerra, José Renato Gaziero Cella, Jéssica Fachin – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-285-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

No XXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, o Grupo de Trabalho - GT “Internet: Dinâmicas da Segurança Pública e Internacional”, que teve lugar na tarde de 28 de novembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Internet: Dinâmicas da Segurança Pública e Internacional”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Gustavo Rabay Guerra

Prof. Dra. Jéssica Fachin

HACKING ESTATAL COMO TÉCNICA ESPECIAL DE INVESTIGAÇÃO: (IM) POSSIBILIDADES NA LEGISLAÇÃO BRASILEIRA ATUAL

STATE HACKING AS A SPECIAL INVESTIGATION TECHNIQUE: (IM) POSSIBILITIES UNDER CURRENT BRAZILIAN LEGISLATION

Emerson Wendt [1]
Simplicio De Oliveira Leite Júnior [2]

Resumo

O uso de ferramentas tecnológicas de monitoramento de dispositivos de comunicação pessoal é uma estratégia de investigação utilizada em diversos países, cujo emprego ficou conhecido, dentre outras denominações, como Hacking Estatal. Diante da difusão dessas ferramentas, questiona-se sobre a possibilidade de, no Brasil, também ser possível o emprego do Hacking Estatal como técnica especial de investigação. Nesse sentido, este trabalho tem como objetivo analisar o ordenamento jurídico penal atualmente em vigor, verificando se há ou não autorização legislativa para que esse meio de obtenção de prova seja licitamente utilizado pelos órgãos de persecução penal. Para tanto, inicialmente, foram conceituadas as referidas ferramentas, relacionados os principais tipos, suas funcionalidades e formas de implantação. Em seguida, foram identificadas as legislações e institutos jurídicos de possíveis aplicações, assim como jurisprudências mais próximas do tema, que, neste caso, tem como marco temporal inicial a decisão proferida pelo Superior Tribunal de Justiça no ano de 2018, que, pela primeira vez, posicionou-se a respeito da técnica de "espelhamento" do aplicativo WhatsApp, fornecendo balizas jurídicas importantes para a discussão sobre a (im) possibilidade do emprego dessas novas técnicas especiais de investigação. Dessa forma, através do emprego do método dedutivo, partindo da análise de legislações, doutrinas e jurisprudências pertinentes, e tendo como metodologia a revisão bibliográfica qualitativa, esta pesquisa obteve resultados, dos quais é possível concluir, que já existem diversos parâmetros legais (e jurisprudenciais) autorizadores do uso do Hacking Estatal, de forma excepcional e com a devida autorização judicial, como técnica especial de investigação.

Palavras-chave: Cell-site simulator, Hacking estatal, Imsi catcher, Malware, Policeware

Abstract/Resumen/Résumé

The use of technological tools for monitoring personal communication devices is an investigation strategy employed in various countries, whose application has become known,

[1] Doutor e Mestre em Direito pela Universidade La Salle – Canoas/RS. Editor-revisor da revista Direito & TI, Qualis B1 Capes. Delegado de Polícia Civil do Estado do RS.

[2] Especialista em Direito Público pela Universidade Federal do Piauí - UFPI e Bacharel em Direito pela Universidade Estadual do Piauí - UESPI. Agente de Polícia Civil – PC/PE.

among other denominations, as State Hacking. Given the proliferation of these tools, questions arise about the possibility of also employing State Hacking as a special investigation technique in Brazil. In this regard, this work aims to analyze the current criminal legal framework, verifying whether or not there is legislative authorization for this means of obtaining evidence to be lawfully used by criminal prosecution agencies. To this end, initially, these tools were conceptualized, the main types were listed, along with their functionalities and implementation methods. Subsequently, the legislation and legal institutes of possible applications were identified, as well as jurisprudence closest to the topic, which, in this case, has as its initial temporal landmark the decision rendered by the Superior Court of Justice in 2018, which, for the first time, took a position regarding the "mirroring" technique of the WhatsApp application, providing important legal guidelines for the discussion about the (im)possibility of employing these new special investigation techniques. Thus, through the use of the deductive method, starting from the analysis of relevant legislation, doctrine, and jurisprudence, and using qualitative bibliographic review as methodology, this research obtained results from which it is possible to conclude that there are already various legal (and jurisprudential) parameters authorizing the use of State Hacking, exceptionally and with proper judicial authorization, as a special investigation technique.

Keywords/Palabras-claves/Mots-clés: Cell-site simulator, Imsi catcher, Malware, Policeware, State hacking

1 INTRODUÇÃO

O uso de ferramentas tecnológicas de monitoramento de dispositivos de comunicação, denominado *Hacking* Estatal, é uma prática difundida em diversos países como estratégia eficaz de investigação criminal. Diante desse quadro, questiona-se: é possível no Brasil, dentro dos marcos legais atuais, a utilização do *Hacking* Estatal como técnica especial de investigação?

Dessa forma, este trabalho tem como objetivo analisar a viabilidade jurídica do emprego do *Hakcing* Estatal, nos termos da legislação processual penal em vigor, com abordagem dos aspectos tecnológicos, normativos e jurisprudenciais. Para tanto, inicialmente, serão conceituadas as ferramentas de *Hacking* Estatal, seus principais tipos, funcionalidades e formas de implantação.

Após essa abordagem técnico-conceitual inicial, serão verificadas e analisadas as legislações e institutos jurídicos, que, como hipótese a ser testada, se os documentos normativos autorizam o uso dessas ferramentas, inserindo, neste contexto analítico, os posicionamentos teóricos da doutrina especializada.

Por fim, serão analisadas as jurisprudências do Superior Tribunal de Justiça, com o marco temporal inicial o ano de 2018 e o final de 2024, cujos desenvolvimentos teórico-práticos podem subsidiar - ou não - a aplicação do *Hacking* Estatal, nos termos da legislação atual e sua interpretação no âmbito do Judiciário brasileiro.

Esta pequisa busca, assim, contribuir na discussão sobre a viabilidade legal de soluções alternativas para o fortalecimento da atividade de investigação, especialmente, em razão da crescente sofisticação do *modus operandi* tecnológico da criminalidade organizada, preocupação delineada pelo Fórum Brasileiro de Segurança Pública.

Utiliza-se, no contexto de todo o trabalho, a metodologia da revisão bibliográfica, a partir de artigos científicos, dissertações, teses e livros jurídicos, bem como o método dedutivo, do geral para o particular, através da análise crítica e conjunta de legislações, institutos jurídicos e decisões judiciais.

2 FERRAMENTAS DE HACKING ESTATAL

"*Hacking* Estatal" é a expressão adotada nesta pesquisa por caracterizar de forma mais adequada a atividade do Estado, que durante a persecução criminal faz uso de técnicas e ferramentas próprias de *hacking*, ou seja, o acesso a dispositivos eletrônicos, sem autorização

nem conhecimento do usuário, por meio de vulnerabilidades nos sistemas de comunicação e/ou no dispositivo-alvo (Hartmann, 2024, p. 444).

Como as técnicas e ferramentas de *hacking* são bastante diversificadas, extremamente criativas e dinâmicas, modificando-se a todo instante, buscou-se o conceito e a identificação dos tipos ferramentas de *Hacking* Estatal tendo como parâmetro a abordagem técnica e jurídica que, atualmente, é debatida no âmbito da Ação de Descumprimento de Preceito Fundamental (ADPF) de nº 1.143 (Brasil, 2024d), ingressada pela Procuradoria-Geral da República (PGR), que tramita no Supremo Tribunal Federal (STF).

2.1 Conceito e tipologias

Na referida ADPF nº 1.143, a PGR faz uma divisão a respeito das ferramentas de *Hacking* Estatal, conceituando dois tipos: (a) programas (*softwares*) de monitoramento para fins de "[...] interceptação, captação, coleta, visualização ou qualquer outra forma de acesso a dados, informações e comunicações de investigados, alvos ou pessoas em geral, contidas em aparelhos digitais de comunicação pessoal [...]" (Brasil, 2024d, p. 52); e (b) equipamentos de monitoramento "[...] do tipo *cell-site simulator* ("CSS") ou "IMSI *catcher*" – caso do PIXCELL – que simulam antenas de telefonia celular [...]" (Brasil, 2024d, p. 53).

A PGR ainda ressalta a preocupação com as particularidades técnicas de três ferramentas comerciais de *Hacking* Estatal mais difundidas atualmente:

> [...] **1) *spywares***, como o Pegasus do NSO Group, que intercepta dados ao infectar um dos dispositivos envolvidos na comunicação; **2) *Imsi Catchers***, como o Pixcell (NSO Group) e o GI2 (Cognyte/Verint), que simulam estações rádio-base capturando dispositivos próximos; **3) dispositivos que rastreiam a localização** de um alvo específico através da rede celular, como o **First Mile** (Cognyte/Verint) e o **Landmark** (NSO Group). (Brasil, 2024d, p. 55, grifos nossos).

Tendo como referência teórica essa abordagem técnica e jurídica elaborada pela PGR, podemos definir que essas ferramentas de *Hacking* Estatal consistem em:

(1) *softwares*, denominados, de forma genérica, pela doutrina como *malwares* (Barbiero, 2021, p. 101) ou *policeware* (Lai, 2024, p. 109-110), os quais possuem alta capacidade de monitoramento do dispositivo-alvo; e

(2) equipamentos, que dotados de *softwares* com finalidades *hacking*, exploram vulnerabilidades identificadas nos sistemas de telecomunicações das operadoras de telefonia e conseguem:

(2.1) através da simulação de antenas de telefonia (frequentemente, referidas como ERBs - Estações Rádio Base), detectar os dispositivos que estão em sua área de cobertura, passando a monitorar a localização e, até mesmo, interceptando os dados telemáticos e as ligações telefônicas; e

(2.2) equipamentos, que mesmo sem simular uma ERB, conseguem, por meio de algum identificador do dispositivo-alvo, monitorar sua localização em tempo real[1].

Com as definições e categorização apresentados, necessária a análise sobre as funcionalidades e meios de implantação.

2.2 Funcionalidades e meios de implantação

Em relação ao primeiro grupo de ferramentas de *Hacking* Estatal, citado pela PGR, encontram-se os *softwares* denominados *malwares* ou *policeware*[2], dentre os quais, são bastante conhecidos os *spywares*, os *trojans horses*, os *ransomwares*, os *rootkits* e as *logic bombs* (Barbiero, 2021, p. 102).

Embora haja diversos tipos de *malwares*, importa mencionar as funcionalidades dos *spywares* por englobar as dos demais. Os *spywares* possibilitam o monitoramento de todas as atividades do dispositivo-alvo, permitindo visualizar, coletar e transmitir dados remotamente (Zaniolo, 2024, p. 719), sendo, via de regra, o escopo das investigações criminais.

A implantação de *malwares/policewares* exige, em geral, a adoção de medidas que, necessariamente, fará uso de algum grau de engenharia social para que o alvo dê permissão para a instalação remota do *software* no dispositivo a ser monitorado. Porém, há *softwares* que, dada a sua alta sofisticação, exploram vulnerabilidades de dia zero, "*zero day exploid*" (Zaniolo, 2024, p. 732), ou seja, graves falhas num sistema que permitem acesso amplo às suas funcionalidades e que, neste caso, dispensariam a elaboração de planos de engenharia social contra o investigado, como ocorre nos ataques de zero clique, "z*ero-click attack*"[3].

---

[1] No Brasil, ficou muito conhecida a utilização do *First Mile* pela ABIN (Agência Brasileira de Inteligência). Disponível em: https://www.congressoemfoco.com.br/noticia/109571/veja-a-integra-do-relatorio-da-pf-sobre-a-abin-paralela/. Acesso em: 22 jun. 2025.

[2] *Policeware* (*police software*) corresponde ao *software* policial, que, para fins didáticos, tem finalidade semelhante aos *softwares* comerciais de controle parental, onde é possível monitorar toda a atividade do dispositivo-alvo, permitindo, inclusive, o acionamento de câmera, microfone e GPS. Com esse objetivo, no Brasil, são muito conhecidos os *softwares* Bruno Espião, MSpy e MobileSpy (Barbiero, 2021, p. 156).

[3] Exemplo de ataque de zero clique (z*ero-click attack)* ocorreu com a exploração de uma grave vulnerabilidade (*zero day exploit*) no recurso de chamada de voz do aplicativo WhatsApp (CVE-2019-3568, pontuação CVSS: 9,8), em 2019, no qual foi possível a instalação do *spyware* Pegasus, da empresa israelense NSO Group, no dispositivo-alvo, apenas por meio de uma chamada de voz não atendida. Disponível em: https://thehackernews.com/2024/12/us-judge-rules-against-nso-group-in.html. Acesso em: 31 jan. 2025.

Em audiência pública realizada no STF, nos dias 10 e 11 de junho de 2024, Sauvei Lai, ao defender a regulamentação do uso dessas ferramentas, citou o recurso que, atualmente, é utilizado na Alemanha - que regulamentou esse meio de obtenção de prova -, onde para a implementação do *software* de monitoramento há o envio para o dispositivo do investigado de uma mensagem dissimulada de atualização do sistema operacional. Através dessa engenharia social é que a implantação do *policeware* é executada (Brasil, 2024e, p. 158).

Em aula do curso de Pós Gradução em Investigação Digital da WB Educação[4], o professor Ritta (2024) relaciona outras formas, as quais denomina "vetores de acesso", que tornam possível a implantação de *softwares* de monitoramento no dispositivo-alvo, sendo citados o uso de *shortlinks*, QRCode, pdf *link*, *phishing site*, *cloud attack*, SIM *swap*, *brute force* e aplicativos modificados; e, ainda mencionada, a possibilidade de instalação física (não remota) por meio da inserção oculta de *pen drives* ou outros *hardwares hacking*, como os *skimmers*, utilizados em ataques cibernéticos do tipo *juice jacking*[5].

No segundo grupo de ferramentas de *Hacking* Estatal, mencionado pela PGR, encontram-se os equipamentos que, para fins didáticos, podem ser divididos em dois subgrupos, com a respectiva descrição de suas funcionalidades.

Dessa forma, há equipamentos que: (1) através da simulação de uma antena de celular, conseguem identificar todos os aparelhos telefônicos que se encontram em sua área de cobertura, podendo interceptar os dados telemáticos e chamadas telefônicas - a depender da tecnologia embarcada no equipamento utilizado para o monitoramento -, podendo ser facilmente transportados, sendo comum o uso em veículos e, mais recentemente, em *drones*; e (2) outros equipamentos/*softwares* que não utilizam o recurso de simular uma antena de celular, mas que fazem uso de falhas dos sistemas das operadoras de telefonia[6], conseguindo através de algum identificador do dispositivo-alvo obter sua localização em tempo real.

Essas ferramentas dependem da simulação de antenas de celulares ou de exploração dos sinais de telefonia bem como interação com as próprias plataformas das operadoras de telefonia, através da identificação de vulnerabilidades nos sistemas, protocolos e estruturas de

[4] Aula ministrada em 19/03/2024. Disciplina: *Investigative Hacking*: *Geofencing*, Interceptação Telemática e Informática, Módulo-8, Seção-I: Investigação Criminal Cibernética. Professor: Cristiano Ribeiro Ritta, delegado de polícia civil, PCRS, desenvolvedor de *softwares* de inteligência e investigação policial; mestrando em Direito e Ciência Jurídica pela Faculdade de Direito da Universidade de Lisboa. *Site* profissional: https://www.cristianoritta.com.br/. Currículo lattes: http://lattes.cnpq.br/0524929883108625.

[5] O *juice jacking* ocorre com a modificação de portas USB públicas (*skimmer*), possibilitando a instalação de *malwares* no dispositivo do usuário. Disponível em: https://medium.com/it-security-in-plain-english/guarding-against-juice-jacking-how-to-secure-your-devices-in-public-spaces-c609a65119aa. Acesso em: 17 mar. 2025.

[6] O *First Mile* explora vulnerabilidades no protocolo SS7 (Sistema de Sinalização nº 7) utilizado na comunicação das operadoras de telefonia no mundo inteiro. Disponível em: https://medium.com/codingrights/consultando-o-espião-de-bolso-vulnerabilidades-ss7-e-rastreamento-global-bc9920008c3c. Acesso em: 14 abr. 2025.

telecomunicações, o que, para tanto, basta, por óbvio, que as ferramentas empregadas estejam aptas a cumprirem este fim, no momento de sua utilização numa investigação, dispensando o emprego de técnicas de engenharia social contra os alvos.

3 HACKING ESTATAL NO BRASIL

Diversos países democráticos[7] fazem uso, de forma legal e legítima, de ferramentas de monitoramento, como meio de superar as tecnologias de anonimização (como o uso de VPNs e *proxies*), de recursos de criptografia e de medidas antiforenses utilizadas por criminosos para impedir que as autoridades públicas possam identificá-los e responsabilizá-los pelos delitos praticados com o uso de aparelhos pessoais de comunicação.

Na apresentação da justificativa do projeto de lei do Senador da República Alessandro Vieira (Brasil, 2024b), sobre a regulamentação do uso de ferramentas de *Hacking* Estatal, é feita referência a pesquisa realizada pelo Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), publicada em novembro de 2022, a qual destaca as contratações, por órgãos estatais brasileiros, envolvendo ferramentas de monitoramento:

> [...] **identificou, entre 2015 e 2021, 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. Segundo a pesquisa, os recursos aplicados pelos estados com essas ferramentas saltaram de R$ 522 mil, em 2015, para mais de R$ 45 milhões em 2021(Amaral et al., 2022, grifos nossos).

Em razão desse crescente interesse dos órgãos de persecução penal brasileiros na aquisição dessas ferramentas, muitos questionamentos sobre a constitucionalidade e a legalidade de sua obtenção e utilização têm surgido em nosso país, gerando muita insegurança jurídica e afetando a definição das estratégias de modernização da investigação criminal, mostrando-se, fundamental, os estudos e pesquisas sobre o tema.

3.1 Hacking Estatal na legislação brasileira atual

[7] EUA, Alemanha, França, Espanha, Itália, Finlândia, Estônia e Áustria são exemplos de democracias que regulamentaram o uso de *softwares* de monitoramento de dispositivos de comunicação pessoal, como amplamente abordado na obra de Sauvei Lai. A Espanha é citada como o país que regulamentou de forma mais abrangente o emprego destas ferramentas, sendo autorizada legalmente a sua utilização tanto na persecução criminal quanto na atividade de inteligência. Os EUA são referenciados como os primeiros a utilizarem legalmente esses meios de obtenção de provas. Já a Alemanha é destacada pelo desenvolvimento teórico-doutrinário com a inovação quanto a proteção dos direitos fundamentais da personalidade consistentes na garantia da proteção da confidencialidade e integridade dos sistemas informáticos (Lai, 2024, p.113-167).

A discussão jurídica, no Brasil, sobre o uso de recursos tecnológicos para o monitoramento de dispositivos de comunicação pessoal está inserida no contexto geral de estudos sobre o a viabilidade legal do uso de *malwares* como técnica especial de investigação.

Sobre o que sejam *malwares*, vale destacar o conceito elaborado por Barbiero (2021), no qual são apontadas as características fundamentais de um *malware*:

> [...] *malware* como sendo um programa que se instala em determinado dispositivo, eletrônico, sem o consentimento ou conhecimento de seu proprietário ou usuário, capaz de permitir, maliciosamente, não só **acesso remoto ao conteúdo armazenado** como, também, a execução de tarefas (**abertura de câmera e microfone, compilação dos dados de geolocalização ou mesmo captação das teclas acionadas no teclado físico, entre outras**) que possibilitem a obtenção de dados ou de evidências capazes de indicar determinado comportamento ou ação sobre o qual tinha o usuário **expectativa de privacidade**. Barbiero (2021, p. 102, grifos nossos).

Esse conceito de *malware* abarca tanto as características técnicas, amplamente mencionadas pela doutrina (Silva Júnior, 2021, p. 13-14; Smanio, 2022, p. 192-193), como sendo um *software* com variadas funcionalidades intrusivas, capaz de permitir o acesso e monitoramento remotos ao dispositivo eletrônico alvo da medida; como ressalta, sob o ponto de vista do Direito, o *status* jurídico do usuário enquanto sujeito de direito, que tem "expectativa de privacidade" ao fazer uso de meios tecnológicos de comunicação e armazenamento de dados pessoais.

Para os autores que defendem a tese de que o ordenamento jurídico brasileiro atual permite o emprego das ferramentas de *Hacking* Estatal mencionadas nesta pesquisa, em síntese, partem do seguinte pressuposto doutrinário (Soares, 2014):

> A simples e radical inadmissibilidade de medidas e técnicas investigativas não legalmente especificadas, não satisfatoriamente regulamentadas ou meramente nominadas (sem procedimento legalmente regulamentado) dificultaria irrazoavelmente a apuração de esquemas criminosos complexos, uma vez que esses são inevitavelmente dinâmicos e sua elucidação demanda criatividade – e, por vezes, originalidade – dos órgãos investigadores. (Soares, 2014, p. 290)

Essa premissa adota o entendimento de que em razão do dinamismo da criminalidade, não é razoável exigir que sempre haja previsão legal específica para a admissibilidade de cada técnica investigativa inédita, principalmente no contexto tecnológico.

Seguindo essa mesma lógica, assevera Pinho Filho (2022):

> [...] **ante a impossibilidade prática e racional de se regular o porvir, na ausência da legalidade restrita, não se pode afastar aprioristicamente o recurso** a métodos ocultos de investigação criminal, por **analogia**, enquanto **meios atípicos de obtenção de prova**, de forma excepcional e subsidiária, no contexto de evolução legislativa progressiva. Pinho Filho (2022, p. 100, grifos nossos).

Nesse sentido, a doutrina brasileira elenca cinco principais diplomas legais, os quais podem ser utilizados como legitimadores do uso das ferramentas de *Hacking* Estatal.

Como primeiro deles, podemos citar a Lei nº 9.296/1996, "Lei das Interceptações Telefônicas e Telemáticas", que regulamenta, detalhadamente, a interceptação telefônica e telemática, estabelecendo as hipóteses de cabimento (art. 2º) - indicando a proporcionalidade da medida, em razão da gravidade dos crimes e da ineficiência de outros métodos de investigação-, juntamente com normas procedimentais que garantem a transparência e auditabilidade, com observância das regras da cadeia de custódia (art. 6º), além de prever a eliminação de dados obtidos que não sejam pertinentes à finalidade da investigação (art. 9º).

No art. 4°, da referida lei, está consignado que a autoridade requerente da interceptação indicará "os meios a serem empregados" (Brasil, 1996) no procedimento; e em seu art. 6° estabelece que dará ciência ao Ministério Público, que poderá acompanhar a sua realização, prevendo, ainda, que a decisão judicial seja qualificada, fundamentando a indispensabilidade da medida, indicando a sua forma de execução e prazo (art. 5º); inclusive, prevendo tipificação penal em caso de interceptação que não ocorra dentro dos parâmetros legais (art. 10).

O segundo diploma legal a ser cotejado com a técnica do uso de *malware* é a Lei nº 12.850/2013, "Lei das Organizações Criminosas", que, em seu art. 3º, prevê diversos meios de obtenção da prova, com destaque para a ação controlada, em seus arts. 8º e 9º, a qual consiste em monitorar (até mesmo no ambiente virtual) a atividade criminosa aguardando o momento mais oportuno para tomada de medidas legais que preservem o máximo de elementos probatórios; e a infiltração virtual (art. 10-A), a qual possui amplo e consolidado quadro normativo no Capítulo II, Seção III, da citada lei (Brasil, 2013), sendo uma medida com maior potencial de interferência nos direitos fundamentais, pois a natureza da infiltração exige interação com o investigado, com participação, se necessário, da empreitada criminosa.

As técnicas especiais de investigação previstas na Lei nº 12.850/2013, quando aplicadas ao uso do *policeware*, indica que é possível o emprego desse recurso investigativo, sendo compatível com a ação controlada (monitorando a atividade criminosa) e a infiltração virtual (interagindo e colhendo informações); e, no caso da necessidade de o procedimento investigativo exigir o acionamento de microfone e câmeras do dispositivo do alvo, a medida seria equivalente a uma captação ambiental, prevista no art. 3º, inciso II, desta mesma lei, e no Art. 8º-A da "Lei das Interceptações Telefônicas e Telemáticas", inserido pela Lei nº 13.964/2019, "Pacote Anticrime" (Brasil, 2019a).

Como terceira legislação mencionada está o Estatuto da Criança e do Adolescente – ECA, o qual em seu art. 190-A, incluído pela Lei nº 13.441, de 2017, também prevê, como meio de obtenção de prova, a infiltração virtual de policiais na internet em investigações de crimes contra a dignidade sexual de crianças e adolescentes (Brasil, 2017).

Ainda no ECA, no art. 190-E, está previsto que todo o procedimento de infiltração virtual deverá ter "[...] todos os atos eletrônicos praticados durante a operação deverão ser registrados, gravados, armazenados e encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado" (Brasil, 1990), a fim de garantir a transparência, auditabilidade e controle judicial e ministerial do procedimento investigativo.

Além dessas três principais legislações, também é feita referência ao Código de Processo Penal em seu Capítulo XI, ao disciplinar o instituto jurídico da busca e apreensão, sugerindo sua aplicação ao ambiente digital, compreendendo em verdadeira "busca e apreensão virtual". Nessa perspectiva, Barbiero (2021) afirma que:

> A conclusão sobre a possibilidade de **interpretar-se extensivamente** esses institutos decorre da natureza e do resultado esperado com a utilização dos *malwares*, que podem, dependendo das necessidades do caso concreto, servir como instrumentos para operacionalização de uma **coleta digital e remota de dados, em típica ação de busca e apreensão virtual [...]**. (Barbiero, 2021, p. 162-163, grifos nossos).

O último diploma legal, mais citado pela doutrina como aplicável ao monitoramento de dispositivos de comunicação pessoal, é a Lei nº 12.965/14, "Marco Civil da Internet", que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil,.

No art. 7º, II, da Lei nº 12.965/14, está consignada a: "II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;" e o inciso III, estabelece a: "III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (Brasil, 2014). Esses dispositivos autorizam, mediante ordem judicial, a interceptação telemática das comunicações e a obtenção dos dados privados armazenados.

Além do art. 7º, II e III, o art. 10, *caput*, § 1º e § 2º, da Lei nº 12.965/14 reforça a tese da possibilidade do emprego de *malwares*, ao permitir, mediante ordem judicial, a disponibilização dos registros de conexão e de acesso a aplicações, e, principalmente, do conteúdo das comunicações privadas.

Igual disciplina normativa, prevista nas legislações analisadas, pode ser aplicada no uso das ferramentas de *Hacking* Estatal que correspondem aos equipamentos que simulando ou não antenas de celular monitoram a localização e/ou interceptam as comunicações. No

caso dos IMSI *Catchers*, *Cell-Site Simulator* e ferramentas como o *First Mile* e *Landmark,* a fundamentação legal, também, encontra repouso na "Lei das Intercepetações Telefônicas e Telemáticas", em seu art. 1º, *caput* e parágrafo único e arts. 4º, 6º e 7º, com destaque ao art. 4º, ao determinar que nos pedidos de interceptação de comunicação, a autoridade policial indicará os meios a serem empregados, autorizando, assim, o uso das ferramentas julgadas mais aptas ao fim almejado conforme a estratégia investigativa.

Essas ferramentas também podem ser utilizadas no curso de uma ação controlada (arts. 8º e 9º da Lei das Organizações Criminosas) contribuindo para o êxito da investigação. Como já destacado, o art. 6º e demais artigos correlatos da Lei nº 9.296/96 garantem a segurança jurídica e a idoneidade do emprego destas ferramentas, assegurando a confiabilidade e integralidade da prova digital obtida.

Além dessas legislações analisadas, também é importante destacar a Convenção de Budapeste (CB), promulgada no Brasil em 12 de abril de 2023, a qual prevê em seus arts. 20 e 33, a obtenção de dados de tráfego em tempo real, nos arts. 21 e 34, a interceptação de dados de conteúdo e no art. 19, a busca e apreensão de dados de computador (Wendt; Martins, 2025, p. 43), reforçando, portanto, o arcabouço jurídico legal que possibilita o emprego do *Hacking* Estatal como técnica especial de investigação.

Para os que são contrários a utilização de *malwares/policeware* e das demais ferramentas de *Hacking* Estatal, o principal argumento está centrado na ausência de legislação específica que regulamente a autorização do uso de tais recursos; e que, a inexistência dessa lei impede completamente o emprego dessas técnicas, em face da potencialidade de alto impacto sobre uma série de direitos fundamentais do investigado (Mendes, 2018, p. 168).

Como ilustrativo do posicionamento dos doutrinadores que rejeitam a tese de aplicação do uso de *malware,* com base na legislação vigente em nosso país, Ribeiro, Cordeiro e Fumach (2022) destacam que:

> No Brasil, não é possível sustentar a existência de uma previsão para a utilização do *malware* a partir dos marcos normativos das **Leis nº 9.296/1996**, **12.850/2013** e **8.069/1990**. Por ser um meio de obtenção de prova atípico e com amplas repercussões sobre o domínio privado dos investigados, **somente uma previsão legal expressa poderia permitir o emprego dessa técnica**. A sua positivação, ademais, deve levar em conta a excepcionalidade que deve revestir o seu emprego, bem como necessidade de haver **formas rígidas de controle da sua operacionalização**. (Ribeiro; Cordeiro; Fumach, 2022, p. 1.495, grifos nossos).

Além de discordar do uso de *malwares*, a partir das leis processuais em vigor, esse posicionamento defende que sejam estabelecidos, em eventual lei sobre a matéria, rígidos controles em sua operacionalização, por considerá-lo um meio de alto impacto nos direitos

fundamentais do investigado, especialmente, a privacidade e a proteção de dados (Monteiro, 2025, p. 128); argumentação essa, que será replicada pela corrente que rechaça o uso dessas ferramentas sem a existência de uma legislação específica.

Soma-se à argumentação da necessidade de uma legislação rigorosa no controle sobre o uso do *malware*, que essa também seja uma "lei de qualidade" (*quality of law*), em razão da restrição de direitos fundamentais, conforme entendimento consagrado pelo Tribunal Europeu de Direitos Humanos (Lai, 2024, p. 169). Ou seja, a regulamentação deve ser feita elaborando-se uma lei que seja bastante detalhada, porém simples e objetiva, a fim de que qualquer cidadão possa compreender o seu sentido, limites e reflexos em seus direitos.

3.2 Hacking Estatal na jurisprudência brasileira atual

Muito recentemente, a jurisprudência brasileira apresentou algumas decisões, que abordaram a interceptação telefônica e telemática, a ação controlada e a infiltração virtual, ao decidir sobre a (im)possibilidade do "espelhamento" de aplicativos de mensageria, técnica que significa monitorar, em tempo real, a troca de mensagens no aplicativo do investigado, além de permitir o acesso às conversas armazenadas.

Há duas decisões do Superior Tribunal de Justiça (STJ) que norteiam o debate sobre a legalidade ou não da utilização do "espelhamento" como meio de obtenção de prova no direito brasileiro. A primeira decisão foi proferida em 27/11/2018, em Recurso Ordinário em Habeas Corpus (RHC 99.735/SC), Informativo nº 640 do STJ, de 15/02/2019 (Brasil, 2019b).

Nessa primeira manifestação sobre o tema "espelhamento", o STJ compreendeu ser inaplicável a interpretação analógica do instituto da interceptação telefônica, previsto na Lei nº 9.296/96, apontando, sobretudo, problemas relativos à manutenção da autenticidade, integridade e confiabilidade dos elementos de prova colhidos durante o espelhamento do aplicativo (Brasil, 2019b).

Embora sejam compreensíveis as alegações de falta de certeza e confiabilidade do material probatório que possa ser produzido, a partir da técnica do "espelhamento" da aplicação, não é forçoso imaginar que existem metodologias e técnicas forenses[8] que possam

[8] Como exemplo, podemos citar a utilização do MEDI – Materializador de Evidências Digitais e Informáticas, que consiste em um *software* gratuito desenvolvido pelo Cyber GAECO do Ministério Público do estado de Goiás - MPGO, cuja finalidade é a coleta automatizada de evidências digitais, sendo possível o registro seguro e confiável do "espelhamento" do aplicativo do investigado (Brasil, 2024a).

garantir a observância dos princípios relativos à preservação dos elementos de prova e dos procedimentos concernentes à cadeia de custódia[9].

Numa segunda oportunidade, em 17/10/2023, a 5ª Turma do STJ, conforme destacado no Informativo nº 792 do STJ, de 24/10/2023, por unanimidade, passou a admitir a técnica de "espelhamento" como compatível com o ordenamento jurídico brasileiro, deixando consignada a legalidade dessa técnica como recurso atinente à infiltração virtual, prevista no art. 10-A da Lei das Organizações Criminosas. *In verbis*:

> [...] A **lei de interceptação, em combinação com a Lei das Organizações Criminosas** outorga legitimidade (legalidade) e dita o rito (regra procedimental), a mencionado espelhamento, em **interpretação progressiva**, em conformidade com a **realidade atual**, para **adequar a norma à evolução tecnológica**. [...] Pode, desta forma, o agente policial valer-se da utilização do espelhamento pela via do Whatsapp Web, desde que respeitados os parâmetros de **proporcionalidade, subsidiariedade, controle judicial e legalidade**, calcado pelo competente mandado judicial. (Brasil, 2023b, grifos nossos).

Fica claro, portanto, diante da autorização pelo STJ do uso da técnica do "espelhamento", que o emprego de ferramentas de *Hacking* Estatal, como os *malwares/policewares*, pode ser utilizado como meio eficaz de sua implementação, contanto que, nesse caso específico, o *software* usado para a infiltração possua funcionalidade que permita o monitoramento apenas da aplicação (*WhatsApp, Telegram etc*) autorizada judicialmente, mostrando-se muito mais assertivo quando comparado ao recurso da abordagem policial e implementação dissimulada da técnica por meio do acesso físico (não remoto) ao dispositivo do alvo, além de possibilitar rigoroso registro técnico-forense do procedimento, garantindo a auditabilidade e a integralidade da prova.

Também é pertinente ressaltar, nos termos da referida decisão do STJ, que esse meio extraordinário de obtenção de prova é consentâneo com a interceptação telemática[10], conforme fundamentos expostos supra (item 3.1).

Ainda nesse contexto, cabe destacar a decisão do juízo de primeiro grau[11], reproduzida no Agravo em Recurso Especial n° 2460351/MG, que autorizou a medida de espelhamento do

[9] Sobre o conceito de cadeia de custódia, ver Freitas Júnior; Garzella; Jorge (2025, p. 157).

[10] Tal semelhança é destacada pelo professor Cristiano Ribeiro Ritta, o qual preconiza o tratamento das regras sobre monitoramento de dispositivos de comunicação pessoal no contexto da Lei nº 9.296/96, "Lei das Interceptações Telefônicas e Telemáticas", sugerindo a inserção do art. 8º-B, nos seguintes termos: "Art. 8º-B: O juiz poderá autorizar a utilização de dados de identificação e senhas de acesso, assim como a instalação de um *software* que permita a coleta de dados telemáticos ou no dispositivo monitorado, à distância e sem o conhecimento do seu titular ou utilizador do conteúdo de um computador, dispositivo eletrônico, sistema informático, instrumento de armazenamento em massa de dados informáticos ou base de dados. Parágrafo único. Aplicam-se subsidiariamente ao monitoramento remoto as regras previstas para a interceptação telefônica e telemática".

WhatsApp, a qual tem o potencial de servir de modelo para decisões, com suas devidas adaptações, de autorização de implantação de *malwares/policewares.*

Seguindo a mesma lógica jurídica que fundamentou essa decisão, aplicando a interpretação progressiva (Brasil, 2023b), autorizando o emprego de *softwares* para o acesso remoto a aplicativos de mensagens e a redes sociais dos investigados, podemos concluir pela possibilidade de uso legal das técnicas de *Hacking* Estatal, abordadas neste trabalho, notadamente, o emprego de *malwares/policewares* com o objetivo de acesso remoto ao dispositivo do investigado, restringindo-se à obtenção de provas específicas, nos termos que a decisão judicial estritamente determinar.

3.3 Consensos e tendências quanto ao emprego do Hacking Estatal

Analisadas as argumentações sobre o uso do *Hacking* Estatal, nos termos da legislação brasileira atual, podemos observar que os doutrinadores convergem sobre alguns pontos. Todos concordam que: (1) o emprego de ferramentas de monitoramento de dispositivos eletrônicos de comunicação pessoal é uma estratégia de investigação eficaz, incrementando, sobremaneira, a atuação policial, (2) o *Hacking* Estatal é imprescindível, como *ultima ratio*, na investigação de crimes graves (pedofilia, terrorismo, organizações criminosas etc), (3) a utilização do *Hacking* Estatal somente é possível por meio de ordem judicial - em razão do impacto da medida nos direitos fundamentais do investigado -, com rígido controle (transparência) sobre a operacionalização (auditabilidade) e documentação (cadeia de custódia) do procedimento, e (4) que todas as informações, eventualmente coletadas durante a aplicação da medida, que não tenham pertinência para a investigação, devem obedecer a sério controle quanto ao seu manuseio e descarte, com supervisão ministerial e judicial que garantam a proteção dos direitos fundamentais do investigado.

Também foi possível identificar, que os doutrinadores, no geral, listam uma série de medidas, as quais julgam indispensáveis para que o uso dessas ferramentas seja a mais democrática e justa possível, recomendando que sejam seguidas rigorosas regras a respeito da cadeia de custódia, tornando o procedimento transparente e auditável, com preservação da

[11] AUTORIZO o **acesso remoto** a aplicativos de mensagens e redes sociais vinculados (dados telemáticos) instalados nos terminais telefônicos, quais sejam: […], bem como IMEIS associados, especialmente no que tange à **interceptação, monitoramento, acompanhamento, escuta, gravação e degravação**, pelo prazo de (15) quinze dias por meio de espelhamento (clonagem), **em tempo real, via *softwares*** denominados *Whatsapp Web* ou *Telegram Desktop*. (Brasil, 2023a, grifos nossos).

integralidade da prova e dos direitos fundamentais. Nesse sentido, Wendt e Martins (2025), sugerem algumas soluções práticas:

> Entre as soluções apresentadas, busca-se a criação de **controle acerca de quais agentes públicos usam as ferramentas**, com registro do dia e hora de acesso (**controle de "log"**), e de quais agentes **consultam e analisam o resultado das diligências** (informações, dados e comunicações protegidas por sigilo). Ainda, que se estabeleçam regras claras sobre o **descarte de informações** e dados irrelevantes de investigados e de terceiros, que não tenham utilidade para a investigação que fundamentou o uso da ferramenta; e **rotinas de fiscalização consolidadas**, por parte de órgãos legitimados, para **prevenir e detectar eventuais abusos na utilização dos softwares**. (Wendt e Martins, 2025, p. 53, grifos nossos).

Assim, é consensual na doutrina a exigência do máximo de detalhamento possível quanto aos mecanismos de controle da operacionalização da medida, não se restringindo a mera comprovação de cumprimento dos requisitos gerais de admissibilidade do procedimento.

Nesse mesmo sentido, a PGR, na ADPF nº 1.143, propõem, até que seja editada uma lei específica, algumas balizas e condicionantes para a utilização dessas ferramentas, destacando-se a exigência de "[...] justificativa motivada da utilidade dos registros solicitados, delimitação do período dos registros, preservação do sigilo das informações, descarte de provas irrelevantes, controle de acesso e fiscalização [...]" (Brasil, 2024d).

Dessa forma, podemos constatar que há uma forte tendência na autorização do uso dessas ferramentas, nos termos do ordenamento jurídico processual penal em vigor, especialmente, quando se analisa a jurisprudência do STJ, que não tem restringido novas técnicas especiais de investigação, como no caso de espelhamento do *WhatsApp*. A propósito, destacou o STJ:

> [...] o crescimento e desenvolvimento de novas formas de atuação da criminalidade coloca o processo penal em xeque, na medida em que a persecução penal realizada nos moldes tradicionais, com métodos de investigação já comumente conhecidos, tem se mostrado insuficiente no combate à delinquência organizada moderna. (Brasil, 2023a).

Essa insuficiência dos métodos tradicionais de investigação proporcionou ao STJ a interpretação progressiva da lei, em face do descompasso temporal entre a legislação existente e as novas tecnologias disponíveis para investigação criminal (*Going Dark Problem*), Wendt e Martins (2025, p. 36), aplicando - por analogia e interpretação extensiva e integrativa da legislação processual penal -, os institutos jurídicos, analisados nessa pesquisa, condizentes com a medida pleiteada.

Tendo como objetivo contornar os impactos nos direitos fundamentais do investigado, a doutrina, em sua maioria, propõe a utilização da técnica da ponderação (ou sopesamento) de

direitos de Robert Alexy (2024, p. 94) onde, em cada caso concreto de colisão de direitos será avaliado o peso de cada um, a fim de que o máximo de cada direito seja preservado.

Além da ponderação de direitos, há forte posição doutrinária no sentido de adoção da analogia (Costa, 2024, p. 107) e da interpretação extensiva e integrativa da legislação processual penal (Barbiero, 2021, p. 148) como principais fundamentos teóricos favoráveis ao emprego de novas técnicas especiais de investigação, com aplicação das legislações em vigor - analisadas ao longo deste trabalho -, permitindo a sua admissibilidade e a valoração das provas obtidas com o uso das ferramentas de *Hacking* Estatal no processo penal brasileiro.

Como podemos perceber, o futuro do *Hacking* Estatal está sendo construído com base na jurisprudência dos tribunais, nos debates acadêmicos, com a produção cada vez maior de artigos e livros jurídicos sobre o tema, assim como na discussão parlamentar, existindo diversos projetos de leis em tramitação no Congresso Nacional, e no debate, amplamente democrático, com participação da sociedade civil e da comunidade científica em audiência pública realizada no STF, onde tramita a ADPF nº 1.143.

3.4 Síntese das Possibilidades Legais de Emprego das Ferramentas de Hacking Estatal

Diante de todo o exposto nesta pesquisa, podemos verificar, de forma sistemática, no quadro 01 a seguir, as ferramentas (*softwares* e equipamentos) de *Hacking* Estatal, com seus respectivos tipos e funcionalidades, e os institutos jurídicos correspondentes, seguida da legislação aplicável em cada caso.

Importa frisar, que a síntese apresentada, não se traduz em rígido enquadramento das ferramentas e legislações, tendo como objetivo apenas ilustrar possíveis aplicações legais do *Hacking* Estatal, podendo haver combinação de tipos, funcionalidades, institutos jurídicos e legislações, em razão da necessidade da estratégia de investigação adotada.

Quadro 01 – Resumo com foco na fundamentação legal das ferramentas de *Hacking* Estatal

FERRAMENTAS	TIPOS	FUNCIONALIDADES	INSTITUTO JURÍDICO	LEGISLAÇÃO APLICÁVEL
MALWARES/ POLICEWARE (*Softwares*)	*spywares*	Monitoramento e coleta de dados	Agente Infiltrado Virtual	Art. 10-A, da Lei 12.850/13. Art. 190-A, da Lei 8.069/90.
	trojans (cavalos de Troia)	Permitir a abertura de portas (*backdoor*)	Agente Infiltrado Virtual	Art. 10-A, da Lei 12.850/13. Art. 190-A, da Lei 8.069/90.
	ransomwares e logic bombs	Encriptar arquivos	Busca e Apreensão *On-line*	Arts. 240, 243 e 245, do CPP, Art. 10, §2º, da Lei 12.965/14 e Art. 19, da CB/23.
	rootkits	Acionamento de câmera e microfone	Captação Ambiental	Art. 8°-A, da Lei 9.296/96 e Art. 3º, II, da Lei 12.850/13.

LOCALIZAÇÃO[12] (Equipamentos)	IMSI *Catchers* (como o Pixcell e o GI2) e ferramentas como o First Mile[13] e o Landmark[14]	Histórico e localização em tempo real	Interceptação Telefônica e Telemática	Arts. 1º e 7º da Lei 9.296/96, Art. 3º, IV, da Lei nº 12.850/13, e Arts. 7º, II, 10, §1°, 13, 15, §3º e 22 da Lei 12.965/14 e Arts. 20 e 21 da CB/23.
LOCALIZAÇÃO E INTERCEPTAÇÃO (Equipamentos)	CSS (*cell-site simulator*)	Histórico/Localização em tempo real e interceptação de dados e telecomunicações	Interceptação Telefônica e Telemática	Arts. 1º e 7º da Lei 9.296/96, Art. 3º, IV, da Lei nº 12.850/13, Arts. 7º, II, 10, §1°, 13, 15, §3º e 22 da Lei 12.965/14 e Arts. 20 e 21 da CB/23.

Fonte: elaborado pelo autor (2025)

4 CONSIDERAÇÕES FINAIS

Diante da exposição a respeito do que são as ferramentas de monitoramento, seus principais tipos e respectivas funcionalidades, bem como a menção a alguns meios de implantação, passando pelas discussões jurídicas (favoráveis e contrárias) e posicionamentos atuais da jurisprudência brasileira, é possível fazer algumas considerações importantes sobre a possibilidade de utilização do *Hacking* Estatal, nos termos do ordenamento jurídico brasileiro atual e em consonância com a proteção dos direitos fundamentais do investigado.

Como analisado, há uma série de dispositivos legais, que de forma abrangente, regulam diversos métodos tecnológicos de investigação criminal, como as interceptações telefônicas e telemáticas, as buscas e apreensões em ambiente virtual, a captação ambiental, o agente infiltrado virtual e as ações controladas. Esses são alguns, dentre os vários meios extraordinários de obtenção de prova, que o ordenamento brasileiro atualmente autoriza a serem utilizados em situações excepcionais envolvendo crimes graves.

Dessa forma, a pesquisa realizada demonstra que, em que pese a ausência de legislação específica regulamentando as ferramentas de monitoramento de dispositivos de comunicação pessoal, vê-se, claramente, que a legislação brasileira atual – por meio do

[12] Em razão deste trabalho abordar, estritamente, a discussão no âmbito da ADPF nº 1.143/STF, e tendo adotado como conceito de *Hacking* Estatal a exploração de vulnerabilidades em sistemas e/ou dispositivos, não foram mencionadas as ferramentas (no caso, plataformas *web*) utilizadas para a captura de dados de localização (IPs e GPS) e de identificação de um alvo (foto e áudio), as quais são, comumente, empregadas pelas polícias no Brasil (Goclick, HiSpy, Canary Tokens, IP Logger etc.) em razão de, tecnicamente, essas ferramentas não explorarem vulnerabilidades em sistemas e/ou dispositivos dos alvos e de não permitirem a instalação de nenhum *software* de monitoramento (*malware*/*policeware*), pelo menos, ao que foi verificado até a data de finalização desta pesquisa. A assertividade dessas ferramentas depende de engenharia social, na qual o alvo será persuadido a clicar em um *link* (gerado na plataforma *web*) e autorizar o uso do GPS, da câmera e/ou áudio do seu dispositivo, que, em razão do padrão da arquitetura dos navegadores *web* (*browsers*), exige-se que o acesso a estes recursos somente seja possível com autorização do usuário. Veja-se sobre em: https://developer.mozilla.org/en-US/docs/Web/API/Permissions_API (acesso em: 25 mar. 2025).

[13] O equipamento necessário para a utilização do First Mile é um computador convencional, o qual permitirá o acesso à plataforma *web*, através de *login* e senha do usuário, conforme constante no relatório da Polícia Federal, mencionado neste artigo, sobre o caso da "ABIN Paralela".

[14] Não foi possível localizar (como é comum em se tratando de ferramentas desta natureza) informações sobre o funcionamento da ferramenta Landmark, a qual foi mencionada pela PGR na ADPF nº 1.143/STF.

emprego da analogia e da interpretação extensiva e integrativa da legislação existente que versa sobre os meios extraordinários de obtenção de prova -, conduz a concluir que há diversos parâmetros legais (e, ainda jurisprudenciais) que autorizam o uso dessas ferramentas de *Hacking* Estatal.

Cabe destacar, que a autorização judicial sempre será necessária, com o estabelecimento de critérios rigorosos que garantam a observância da cadeia de custódia, além de mecanismos de auditabilidade e preservação da integralidade das provas, e com garantias de proteção dos direitos fundamentais do investigado, especialmente, o núcleo essencial dos direitos à privacidade, intimidade, sigilo das comunicações, dados pessoais, autodeterminação informativa e a confidencialidade, integridade e disponibilidade dos sistemas informáticos, caracterizando-se, assim, como uma autorização judicial qualificada, sendo deferida apenas em situações que, como *ultima ratio*, exijam o emprego de técnicas especiais de investigação com o uso de tecnologias de *Hacking* Estatal.

Por fim, em razão das controvérsias doutrinárias, observadas na pesquisa, mostra-se necessário ampliar o debate democrático sobre o incremento tecnológico da investigação criminal, sendo o parlamento brasileiro a instituição primordial para este fim, não só buscando aprimorar as leis existentes, mas reforçando a autorização do uso das ferramentas de *Hacking* Estatal e/ou elaborando uma legislação específica sobre o tema, com os respectivos debates sobre a temática, para além da ADPF nº 1.143/STF.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. 3. ed. São Paulo: Coedição Juspodivm e Malheiros Editores, 2024.

AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César Martins; RAMIRO, André (coord.). **Mercadores da Insegurança**: conjuntura e riscos do hacking governamental no Brasil. IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em: https://ip.rec.br/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 31 jan. 2025.

BARBIERO, Diego Roberto. **Implantação de Malwares em Investigações Complexas**. Curitiba: Juruá, 2021.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 9 jan. 2025.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF: Presidência da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 11 jan. 2025.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção de provas, infrações penais correlatas e o procedimento criminal. Brasília, DF: Presidência da República, 2013. Disponível em: https://planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/12850.htm. Acesso em: 10 jan. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jan. 2025.

BRASIL. **Lei nº 13.441, de 8 de maio de 2017**. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet. Brasília, DF: Presidência da República, 2017. Disponível em: https://planalto.gov.br/ccivil_03/_Ato2015-2018/2017/L13441.htm. Acesso em: 15 jan. 2025.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019a. Disponível em: https://planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/13964.htm. Acesso em: 20 jan. 2025.

BRASIL. Ministério Público do Estado de Goiás. **MEDI** – **Materializador de Evidências Digitais e Informáticas**. 2024a. Disponível em: https://www.mpgo.mp.br/portal/pagina/medi-materializador-de-evidencias-digitais-e-informaticas. Acesso em: 19 jan. 2025.

BRASIL. **Projeto de Lei n° 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, 2024b. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2460351/MG**, Relator: Ministro Reynaldo Soares da Fonseca, 5ª Turma, julgado em 18 out. 2023a, DJe 20 out. 2023. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=DTXT&livre=(ARESP+e+2460351).nome. Acesso em: 28 abr. 2025.

BRASIL. Superior Tribunal de Justiça. **Informativo nº 640, de 15/02/2019**. STJ. 6ª Turma. RHC 99.735-SC, Rel. Min. Laurita Vaz, por unanimidade, julgado em 27/11/2018, publicado no DJe em 12/12/2018. 2019b. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0640. Acesso em: 14 abr. 2025.

BRASIL. Superior Tribunal de Justiça. **Informativo nº 792, de 17/10/2023**. STJ. 5ª Turma. AREsp 2.309.888-MG, Rel. Min. Reynaldo Soares da Fonseca, por unanimidade, julgado em 17/10/2023, publicado no DJe de 30/10/2023. 2023b. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0792. Acesso em: 16 fev. 2025.

BRASIL. Superior Tribunal de Justiça. **Informativo nº 810, de 07/05/2024**. STJ. 5ª Turma. AREsp 2.318.334-MG, Rel. Min. Reynaldo Soares da Fonseca, julgado em 16/4/2024, publicado no Dje de 29/04/2024. 2024c. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0810. Acesso em: 18 mar. 2025.

BRASIL. Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental - ADPF nº 1.143**. Reautuação de Processo em 16/04/2024, referente à ADO nº 84/2023. Relator: Cristiano Zanin. 2024d. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814. Acesso em: 25 jan. 2025.

BRASIL. Supremo Tribunal Federal. **Regulação do uso de ferramentas de monitoramento secreto de aparelhos de comunicação pessoal**. Transcrições da 39ª audiência pública do Supremo Tribunal Federal – STF, ADPF 1.143. 2024e. Disponível em: https://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/AudinciaPblica39RegulaodoTranscrioaudinciapblica39.pdf. Acesso em: 20 abr. 2025.

COSTA, Diogo Erthal Alves da. **Meios Atípicos de Obtenção de Prova**: a invasão de sistemas informáticos na investigação da criminalidade organizada. São Paulo: JusPodivm, 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública**. São Paulo, 2024. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/253. Acesso em: 20 jul. 2025.

FREITAS JÚNIOR, Adair Dias de; GARZELLA, Oleno Carlos Faria; JORGE, Higor Vinicius Nogueira. **Manual de Interceptação Telefônica e Telemática** - teoria, prática e legislação. 4. ed. São Paulo: JusPodivm, 2025.

HARTMANN, Stefan Espírito Santo. **O Conteúdo do Smartphone como Prova no Processo Penal**: o excepcionalismo da tecnologia sob a óptica da proteção da privacidade. Curitiba: Juruá, 2024.

LAI, Sauvei. **Policeware**: infecção de software em sistema informático do investigado para fins de vigilância eletrônica. São Paulo: JusPodivm, 2024.

MENDES, Carlos Hélder Carvalho Furtado. **Malware do Estado e Processo Penal**: a proteção de dados informáticos à infiltração por software na investigação criminal. Orientador: Prof. Dr. Aury Lopes Jr. 2018. Dissertação (Mestrado em Ciências Criminais), Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS, Porto Alegre, 2018. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/8537. Acesso em: 17 jan. 2025.

MONTEIRO, Leonardo Max Pereira. **Persecução Criminal e o uso de Malwares**: limites e possibilidades frente aos direitos fundamentais à privacidade e proteção de dados. Dissertação (Mestrado em Direito) - Universidade do Oeste de Santa Catarina - UNOESC, 2025.

PINHO FILHO, Ossian Bezerra. **Investigação Criminal Tecnológica** - infiltração por malware nas investigações informáticas. Curitiba: Juruá, 2022.

RIBEIRO, Gustavo A. M.; CORDEIRO, Pedro Ivo R. V.; FUMACH, Débora M. O *malware* como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro.

Revista Brasileira de Direito Processual Penal, vol. 8, n. 3, p. 1463-1500, set/dez, 2022. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/723. Acesso em: 28 jan. 2025.

RITTA, Cristiano Ribeiro. **Investigative Hacking***: Geofencing*, Quebra de Sigilo e Interceptação Telemática e Informática. Aula ministrada em 19 mar. 2024. Especialização em Investigação Digital – WB Educação, Seção I: Investigação Criminal Cibernética, Módulo 8. Porto Alegre: WB Educação, 2024.

SILVA JÚNIOR, Washington Trindade da. **A Utilização de Malware em Investigações Criminais em Face do Estabelecido pelos Direitos Fundamentais**. Dissertação (Mestrado em Direito Público), Faculdade de Direito da Universidade Nova de Lisboa, 2021. Disponível em: https://run.unl.pt/bitstream/10362/142099/1/Junior_2022.pdf. Acesso em: 29 jan. 2025.

SMANIO, Gianluca Martins. **A vigilância policial em meio digital**: entre o garantismo e a eficiência. Curitiba: Juruá, 2022.

SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas**: perspectivas e limites. Tese (Doutorado em Direito Processual), Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-30112015-165420/publico/Versao_integral_Gustavo_Torres_Soares.pdf. Acesso em: 10 abr. 2025.

WENDT, Emerson; MARTINS, Tiago Misael de Jesus. Hacking Investigativo: perspectivas da legislação brasileira. In: IBRAHIN, Francini Imene Dias; LEITÃO JÚNIOR, Joaquim (org.). **Crimes Digitais**. Leme: Mizuno, 2025. p. 34-57.

ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no Direito. 6. ed. São Paulo: JusPodivm, 2024.