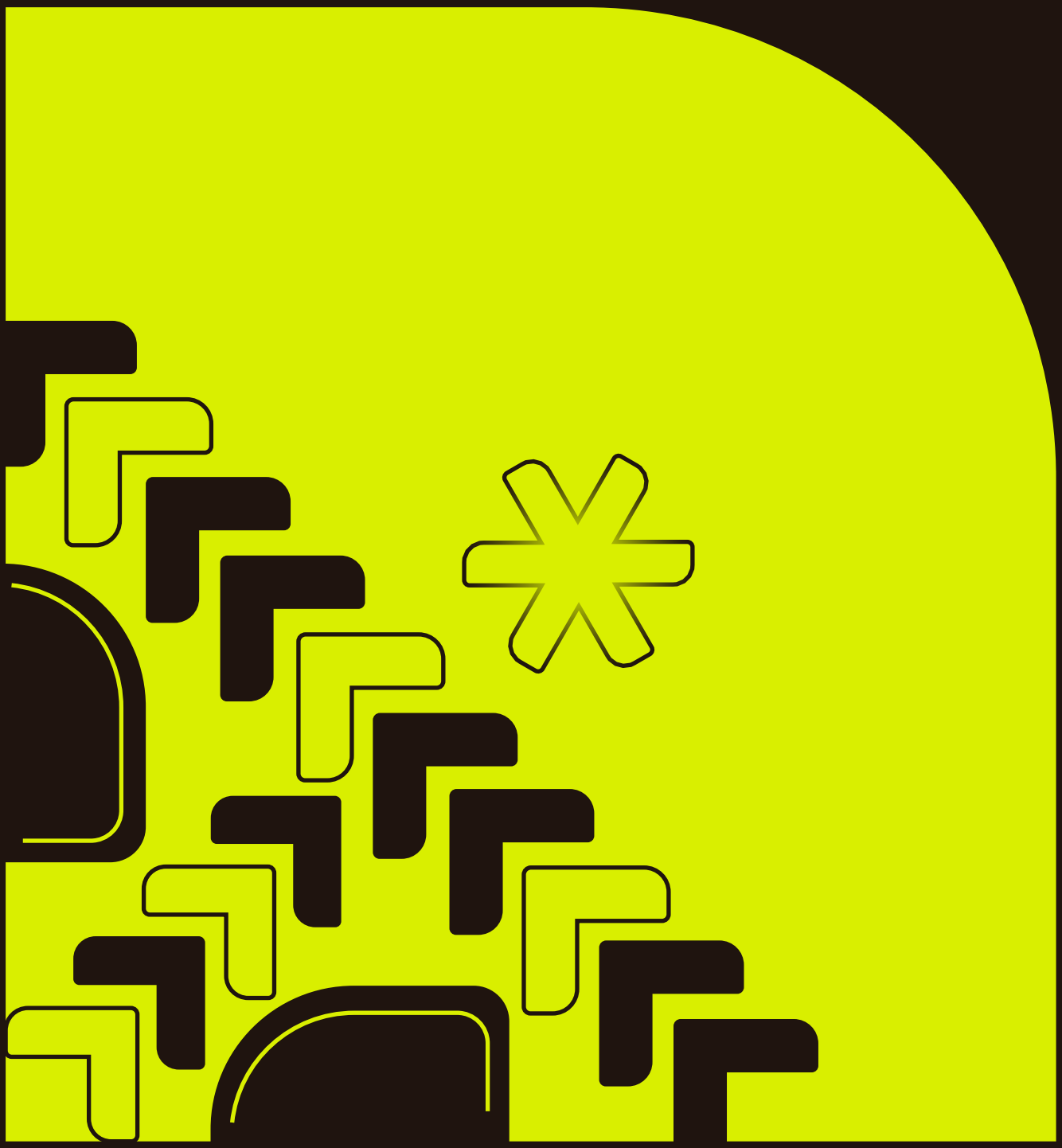
# Nota Técnica

Instituto de Pesquisa em Direito & Tecnologia do Recife

# Desafios regulatórios e diretrizes acerca do uso de ferramentas de intrusão digital no contexto brasileiro



# FICHA TÉCNICA


## Realização:

Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec

## Equipe:

### Coordenação:

Mariana Canto

### Autores:

Mariana Canto
Marcos César M. Pereira
Luana Batista

### Revisão:

Raquel Saraiva

### Projeto gráfico:

Estúdio Puya!

### Como citar:

IP.REC - INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. Nota Técnica: Desafios regulatórios e diretrizes acerca do uso de ferramentas de intrusão digital no contexto brasileiro. Recife: IP.rec, 2024.

# Nota técnica: Desafios regulatórios e diretrizes acerca do uso de ferramentas de intrusão digital no contexto brasileiro

# 1. INTRODUÇÃO

## 1.1 Contextualização e Objetivos da Nota Técnica

A presença de vulnerabilidades em dispositivos e sistemas informáticos é algo extremamente presente no cotidiano, ainda que para a maioria da população seja algo invisível ou desconhecido. Essas falhas criam brechas para que atacantes acessem informações as quais deveriam estar protegidas por camadas de segurança digital. Por vezes, a exploração dessas vulnerabilidades se dá pelo poder estatal, seja para fins de inteligência ou investigação, prática nomeada de *hacking governamental*[1].

A descoberta e exploração de vulnerabilidades pelo Estado[2] pode ser realizada por meio do próprio poder de inteligência estatal[3] ou pode ser terceirizada para empresas especializadas no cenário de vigilância. Cria-se, assim, um mercado com empresas que fomentam a insegurança cibernética para a venda de exploração para governos e empresas que desenvolvem ferramentas de intrusão a dispositivos informáticos[4].

O que se notou considerando esse panorama foi o aumento de denúncias envolvendo o abuso e infrações aos direitos humanos decorrente da utilização de ferramentas de acesso e extração de dados de dispositivos móveis. Dentre uma gama de soluções, destacou-se no cenário internacional o *spyware Pegasus*, desenvolvido pela empresa israelense NSO Group[5]. Capaz de infectar dispositivos e acessar toda a informação sem que o vigiado tenha

---

[1] DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental**: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: <https://bit.ly/3YdVcIL>. Acesso em: 02 de dezembro de 2024

[2] A prática também é conhecida na literatura como *lawful hacking*.
Cf. BELLOVIN, Steven M. et al. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. **Nw. J. Tech. & Intell. Prop.**, v. 12, p. 1, 2014.
LIGUORI, Carlos. Exploring Lawful Hacking as a Possible Answer to the'Going Dark'Debate. **Mich. Tech. L. Rev.**, v. 26, p. 317, 2019.

[3] Por exemplo, o *Vulnerabilities Equities Process* é um processo do governo dos Estados Unidos para decidir se uma vulnerabilidade descoberta será divulgada para aprimoramento da segurança cibernética ou se será utilizada de forma ofensiva para fins de inteligência. Cf. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Acesso em 02 de dezembro de 2024.

[4] Cf. AMARAL, Pedro; CANTO, Mariana; PEREIRA, César M.; RAMIRO, André (coord.). Nutrindo o Mercado de Vulnerabilidades. In: _____. Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em 02 de dezembro de 2024.

[5] MARCZAK, Bill et al. HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab, 2018. Disponível em https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in- -45-countries/. Acesso em 02 de dezembro de 2024.

conhecimento, sua utilização foi observada contra ativistas, jornalistas e dissidentes políticos em países como México[6], Espanha[7], Índia[8], Bahrein[9], entre outros.

Considerando esse cenário, esta nota técnica tem como objetivo fornecer insumos para elaboração de possíveis políticas públicas sobre tecnologias de acesso e extração de dados de dispositivos móveis. Buscaremos apresentar aqui a relevância no cenário atual do tema, os diversos tipos de ferramentas utilizadas, o contexto regulatório, boas práticas e desafios na temática.

### 1.2. Relevância do Tema no Cenário Atual

O Brasil não se encontra distante da temática. No estudo que o IP.rec realizou em 2022, intitulado "Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil"[10], identificamos 209 contratos entre o poder público e empresas privadas vendedoras de ferramentas de intrusão a dispositivos informáticos. Os dados apontaram a capilaridade de tais soluções tanto a nível federal como a nível estadual, complexificando medidas legais e de salvaguarda para o uso dessas soluções.

O uso dessas ferramentas e o tratamento dos dados coletados a partir da operacionalização é marcado por uma opacidade generalizada. A ausência de uma Lei Geral de Proteção de Dados (LGPD) para a esfera penal e de segurança nacional abre brechas para formulação de políticas públicas que levantam preocupação aos direitos fundamentais dos brasileiros. Um exemplo claro nesse campo é o Projeto Excel, da Secretaria de Operações Integradas (SEOPI), vinculada ao Ministério da Justiça e Segurança Pública, criado durante o governo do ex-presidente Jair Bolsonaro, que consistia no envio de ferramentas de extração de

---

[6] Kirchgaessner, Stephanie. Mexico: reporters and activists hacked with NSO spyware despite assurances. **The Guardian**, 04 de outubro de 2024. Disponível em https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus Acesso em 02 de dezembro de 2024.

[7] Spain: Court reopens investigation in Pegasus spying scandal. **DW**, 23 de abril de 2024. Disponível em https://www.dw.com/en/spain-court-reopens-investigation-in-pegasus-spying-scandal/a-68901546 Acesso em 02 de dezembro de 2024

[8] India still targeting high-profile journalists with Pegasus software. **Le Monde**, 28 de dezembro de 2023. Disponível em https://www.lemonde.fr/en/international/article/2023/12/28/india-still-targeting-high-profile-journalists-with-pegasus-software_6382201_4.html Acesso em 02 de dezembro de 2024.

[9] Bahrain: Devices of three activists hacked with Pegasus spyware. **Amnesty International,** 18 de fevereiro de 2022. Disponível em https://www.amnesty.org/en/latest/news/2022/02/bahrain-devices-of-three-activists-hacked-with-pegasus-spyware/ Acesso em: 02 de dezembro de 2024.

[10] AMARAL, Pedro; CANTO, Mariana; PEREIRA, César M.; RAMIRO, André (coord.). Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em 02 de dezembro de 2024.

dados de telefones celulares para as secretarias de segurança pública em troca dos dados coletados nas operações em que as ferramentas fossem utilizadas[11].

Mais recentemente, a utilização ilegal por funcionários da Agência Brasileira de Inteligência (ABIN) da solução *FirstMile*[12], desenvolvida pela Verint Systems/Cognyte, durante o governo Bolsonaro esteve em destaque nos noticiários brasileiros. O equipamento tem a capacidade de monitoramento da localização do vigiado por meio da utilização da rede 2G, 3G e 4G. Para isso, a ferramenta explora vulnerabilidades presentes nas redes de telecomunicações, simulando uma antena no qual obtém a localização do alvo[13]. Entre as listas de espionados pela chamada "Abin paralela" estão ministros do Supremo Tribunal Federal (STF), parlamentares do Congresso Federal, membros do poder executivo e jornalistas.[14]

Em decorrência desse fato político, a Procuradoria Geral da República (PGR) ingressou com uma ação no STF questionando a ausência de regulação no que concerne ao uso de ferramentas de monitoramento remoto. A Ação Direta de Inconstitucionalidade por Omissão 84, transformada em Arguição de Descumprimento de Preceito Fundamental 1143, relatada pelo Ministro Cristiano Zanin, teve audiência pública nos dias 11 e 12 de junho de 2024.

Ainda na esteira do caso, foi protocolado no Senado Federal o Projeto de Lei 402/2024[15], de autoria do Senador Alessandro Vieira (MDB/SE). O PL dispõe sobre a utilização de ferramentas de monitoramento remoto por órgãos e agentes públicos, civis e militares.

Tal conjuntura aponta para a urgência da discussão sobre o tema no Brasil, que hoje se encontra sem uma devida regulação na matéria, abrindo margem para abusos e violações aos direitos humanos.

---

[11] Ameno, Fernando. As Planilhas de Bolsonaro: Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados. **The Intercept Brasil,** Rio de Janeiro, 21 de março de 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 02 de dezembro de 2024.

[12] CNN. FirstMile: como funciona o software espião que teria sido usado pela Abin de Ramagem. **CNN Brasil.** 25 de janeiro de 2024. Disponível em https://www.cnnbrasil.com.br/politica/firstmile-como-funciona-o-software-espiao-que-teria-sido-usado-pela-abin-de-ramagem/ . Acesso em 02 de dezembro de 2024.

[13] Camporez, Patrick, Serra, Paola. 'Abin paralela': PF e Anatel explicam vulnerabilidade que permitiu acesso a localização de celulares. **O Globo,** Rio de Janeiro, 18 de julho de 2024. Disponível em https://oglobo.globo.com/politica/noticia/2024/07/18/abin-paralela-pf-e-anatel-explicam-vulnerabilidade-que-permitiu-acesso-a-localizacao-de-celulares.ghtml. Acesso em 02 de dezembro de 2024.

[14] Sales, Pedro. Lira, Renan Calheiros, Kim Kataguiri: conheça os alvos da Abin paralela. **Congresso em Foco**, 11 de julho de 2024. Disponível em https://congressoemfoco.uol.com.br/area/justica/abin-paralela-arthur-lira-renan-calheiros-kim-kataguiri/. Acesso em 02 de dezembro de 2024.

[15] https://www25.senado.leg.br/web/atividade/materias/-/materia/162146

## 2. Sobre as ferramentas de acesso e extração de dados de dispositivos móveis

### 2.1. Definição e Tipos de Tecnologias Utilizadas

Durante a pesquisa dos "Mercadores da Insegurança", realizamos uma divisão analítica para separar diferentes tipos de ferramentas de extração de dados de dispositivos móveis.

| Tipo | Descrição | Exemplos |
|---|---|---|
| **Acesso remoto** | Soluções no qual o operador acessa o dispositivo do usuário sem necessidade de ter a posse física do aparelho.<br><br>A partir da infecção do alvo, o espião terá informações diversas, a depender do nível de intrusividade do aparelho. | Pegasus (NSO Group); FirstMile, GI2 e PI2 (Verint Systems/Cognyte) |
| **Acesso com dispositivos em mãos** | Dispositivos no qual o operador necessita ter a posse física do aparelho para executar a extração de dados.<br><br>A extração se dá por meio da conexão do dispositivo com a ferramenta, que irá recuperar dados armazenados e/ou deletados do aparelho. | UFED (Cellebrite); XRY (MSAB); Magnet AXIOM (OpenText); Forensic Toolkit (Exterro/AccessData) |

Tal distinção é importante para compreender tanto os limites técnicos para o funcionamento quanto o contexto de aplicação de cada uma delas. As primeiras têm um potencial intrusivo consideravelmente superior, operando de forma remota e frequentemente infectando o dispositivo sem o conhecimento do usuário. O Pegasus, por exemplo, é capaz de infectar o dispositivo do usuário explorando vulnerabilidades em

aplicativos ou no sistema operacional. Estas falhas, quando desconhecidas pelos próprios fabricantes são denominadas vulnerabilidades de dia zero[16].

As últimas, por sua vez, necessitam da posse do aparelho físico em mãos para a extração de dados, o que diminui o poder de intrusividade, mas ainda é igualmente preocupante. Apesar dessa diferença, elas ainda são capazes de coletar dados de forma extensiva. Por serem utilizadas sobretudo em investigações criminais enquanto dispositivos forenses, a alta capacidade de extração de dados pode capturar dados que excedem o escopo investigativo, seja no tema e/ou no tempo do fato que está sendo investigado, recuperando dados deletados e criando margem para *fishing expedition* (termo que se refere à busca exploratória e indiscriminada de evidências). Isso se dá, pois, tais dispositivos operam por meio da extração de dados de três formas:

| Forma de extração | Descrição | Dados obtidos |
|---|---|---|
| **Lógica** | Método mais rápido no qual se cria cópias dos arquivos acessíveis ao usuário. | Dados básicos do dispositivo: contatos, histórico de chamadas, mensagens de texto, dados de aplicativos, mídias e documentos acessíveis. |
| **Sistema de arquivo (file system)** | Processo ainda considerado lógico, porém mais abrangente, que acessa e copia toda a estrutura do sistema de arquivos do dispositivo, recuperando inclusive arquivos ocultos e metadados do sistema. | Todos os dados da extração lógica, além de arquivos do sistema, caches de aplicativos, arquivos temporários, logs do sistema e arquivos ocultos. |
| **Física** | Método mais complexo e completo, no qual se extrai uma cópia bit por bit da memória de armazenamento do usuário, permitindo a recuperação de dados excluídos. Requer mais tempo e recursos técnicos. | Todos os dados das extrações anteriores, além de arquivos deletados e fragmentos de dados não alocados. |

[16] Pegg, David; Cutler, Sam. What is Pegasus spyware and how does it hack phones. **The Guardian**, 18 de julho de 2021. Disponível em https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones . Acesso em 03 de dezembro de 2024.

Fonte: Produção própria a partir do relatório do Privacy International (2019)[17]

No nosso estudo identificamos uma capilaridade nos órgãos de segurança pública estaduais das soluções de intrusão digital que demandam os dispositivos em mãos. Os aparelhos de intrusão remota identificados estavam, na maioria, dentro de órgãos federais, como o Ministério da Defesa. A nível estadual houve contratação de tais ferramentas, porém em menor número, não sendo possível identificar um padrão das motivações para a aquisição.

## 2.2. Potenciais Riscos Associados a Direitos Fundamentais e Liberdades Civis

Cada uma dessas ferramentas traz consigo riscos associados aos direitos humanos, sobretudo em cenários de baixa salvaguarda. Como já destacado anteriormente, soluções de intrusão digital estão envolvidas em inúmeros casos de violações aos direitos humanos. Além do caso Pegasus, o mais conhecido, ferramentas desenvolvidas pelas empresas Verint Systems/Cognyte e Cellebrite também estão envolvidas em escândalos de violações de direitos humanos, e têm sido amplamente adquiridas pelo Estado brasileiro.

No cenário internacional, as soluções da Cognyte estiveram envolvidas na interceptação e vigilância das comunicações de cidadãos do Sudão do Sul. Durante dois anos, foram repassados para empresa mais de 760 mil dólares pelos equipamentos[18]. No Myanmar, a mesma empresa venceu um processo licitatório antes do golpe militar que ocorreu no país em fevereiro de 2021, utilizado para interceptar as telecomunicações[19].

No Brasil, para além do caso FirstMile, as soluções da Verint/Cognyte estiveram envolvidas em uma investigação da Polícia Civil do Pará contra o governador do estado, Helder Barbalho (MDB/PA). Na operação, o equipamento foi apreendido por suspeita de ter sido utilizado de forma irregular para monitorar os investigadores de um esquema de corrupção na máquina pública.[20]

---

[17] Privacy International. **A technical look at Phone Extraction.** 2019. Disponível em https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf . Acesso em 02 de dezembro de 2024.

[18] Kabir, Omer. Verint Systems supplied South Sudan with surveillance technology says Amnesty. **Calcalist**, 02 de fevereiro de 2021. Disponível em https://www.calcalistech.com/ctech/articles/0,7340,L-3891006,00.html . Acesso em 03 de dezembro de 2024.

[19] Potkin, Fanny; Mcpherson, Poppy. Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup-documents. **Reuters**. 23 de janeiro de 2023. Disponível em https://www.reuters.com/technology/israels-cognyte-won-tender-sell-intercept-spyware-myanmar-before-coup-documents-2023-01-15/ . Acesso em 04 de dezembro de 2024.

[20] O Antagonista. A empresa que vendeu a 'maleta hacker' para o esquema de Helder Barbalho. **O Antagonista,** 02 de outubro de 2020. Disponível em https://oantagonista.com.br/brasil/exclusivo-a-empresa-que-vendeu-a-maleta-hacker-para-o-esquema-de-helder-barbalho/ . Acesso em: 03 de dezembro de 2024.

Apesar de desenvolverem soluções de intrusão com dispositivos em mãos, a Cellebrite também está envolvida em escândalos similares. A ferramenta da empresa, também de origem israelense, esteve relacionada com a perseguição de jornalistas no Myanmar[21]. Outros países no qual se tem registro de utilização da solução para extração de dados de jornalistas, ativistas e/ou opositores políticos são Botswana, Gana, Nigéria, Hong Kong, Bangladesh, Indonésia, Índia, Rússia, Belarus, Venezuela, Bahrein e Arábia Saudita[22].

Nos Estados Unidos, a organização UpTurn identificou que a solução UFED, desenvolvida pela Cellebrite[23], estava capilarizada, presentes em todos os estados do país. A utilização, no entanto, havia ultrapassado o escopo de delitos de maior potencial ofensivo, sendo direcionada para crimes como pixação, furto, prostituição, batida de carros e todo tipo penal relacionado a drogas ilegais. Por causa deste último uso, o estudo aponta para uma possibilidade alta de que as extrações tenham afetado de maneira desproporcional pessoas negras e latinas.

Tal inferência também é possível de ser feita no cenário brasileiro. O Projeto Excel, mencionado anteriormente na nota técnica, distribuía aparelhos da Cellebrite para as secretarias de segurança pública estaduais. Em vídeo promocional lançado pelo Ministério da Justiça e Segurança Pública, o crime mais investigado foi o de tráfico de drogas, representando 66% dos delitos investigados. Segundo dados do Instituto de Pesquisa Econômica Aplicada (IPEA), pessoas negras são a maioria dos presos por tráfico de drogas em rondas policiais[24]. Dessa forma, é altamente provável que os dados que são enviados para os bancos de dados do Projeto Excel tenham um viés de raça, trazendo riscos para políticas de segurança pública que venham a ser desenvolvidas a partir do tratamento de tais informações.

Esses abusos apontam para os riscos associados à produção e ao uso dessas ferramentas. A existência delas pressupõe a produção e manutenção de vulnerabilidades que colocam em risco os dados e informações de diversos setores da sociedade. Tal fato dificulta a

---

[21] McLaughin, Tommy. Security-tech companies once flocked to Myanmar. One firms tools were used against two journalists. **The Washington Post**, 4 de maio de 2019. Disponível em https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html . Acesso em 04 de dezembro de 2024.

[22] Krapiva, Natália; Hinako. What spy firm Cellebrite can't hide from investors. **AccessNow**, 26 de maio de 2021. Disponível em https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/ . Acesso em 04 de dezembro de 2024.

[23] Koepke, Logan et al. **Mass Extraction**. UpTurn, 2020. Disponível em https://www.upturn.org/work/mass-extraction/ . Acesso em 04 de dezembro de 2024.

[24] G1. Negros são maioria entre presos por tráfico de drogas em rondas policiais, diz IPEA. **G1**, 13 de março de 2024. Disponível em https://g1.globo.com/politica/noticia/2024/03/13/negros-sao-maioria-entre-presos-por-trafico-de-drogas-em-rondas-policiais-diz-ipea.ghtml . Acesso em 05 de dezembro de 2024.

manutenção de um ecossistema digital seguro e estável para todos, sendo por isso necessário ter em vista essa conjuntura no desenvolvimento de qualquer política nacional de cibersegurança.

Além disso, essas soluções de intrusão de dispositivos promovem uma grave ameaça aos direitos humanos. Como foi apresentado, tais ferramentas estão sendo empregadas para a perseguição de ativistas, jornalistas, dissidentes políticos e minorias sociais. Dessa forma, para além do direito à privacidade, direitos como a liberdade de expressão, de imprensa, associação e mesmo o direito à vida podem ser ameaçados por causa de ferramentas como essas. Essa ameaça decorre não apenas da utilização das soluções contra alvos, mas também da capacidade de sua existência de inibir os cidadãos de se manifestarem livremente por medo da vigilância e repressão estatal (*chilling effect*).

Importante ainda pontuar que, uma vez feita a aquisição dessas ferramentas, o arsenal intrusivo estará disponível para uso tanto para governantes mais democráticos como mais autoritários. Da mesma forma, uma vez dentro do arcabouço estatal, sem as devidas regulações, salvaguardas e transparência, há uma enorme possibilidade de que essas soluções sofram sequestro de função (*function creep*).

Por último, mas não menos importante, a capilaridade de soluções de intrusão dentro do cenário policial brasileiro causa preocupações, sobretudo em cidades nas quais há uma alta incidência de milícias. Por isso, é necessário levar em consideração a possibilidade de que ferramentas de intrusão estejam sendo utilizadas para extrair dados de cidadãos dentro de áreas de milícias como forma de controle e vigilância do território, o que coloca em maior risco pessoas já vulneráveis socialmente.

## 3. Contexto Legal e Regulatório

### 3.1. Cenário Brasileiro Atual

#### 3.1.1. Constituição Federal

Além do direito à privacidade garantido pelo art. 5º, inciso X, da Constituição, que tem papel central na análise de direitos que podem ser restringidos com o uso de ferramentas de acesso e extração de dados, o acesso a informações de comunicações privadas também é protegido pelo inciso XII do mesmo artigo. Qualquer ação para acessar informações privadas, incluindo comunicações, deve ser conduzida por meios processuais que garantam sua legalidade, proporcionalidade e a comprovação de necessidade. Além disso, a necessidade de autorização judicial adequadamente fundamentada é essencial.

A Emenda Constitucional nº 115/2022 inseriu no art. 5º (inciso LXXIX) da carta magna brasileira o direito fundamental e autônomo à proteção de dados pessoais. Ou seja, as

normas infraconstitucionais e os instrumentos administrativos que regulamentem o uso de ferramentas de acesso e extração devem sempre considerar a proteção dos direitos fundamentais consagrados na Constituição. A observância de princípios como finalidade, necessidade, qualidade dos dados, transparência, segurança, prevenção e prestação de contas dos responsáveis pelo tratamento de dados nas operações de acesso e extração deve ser consolidada com base no direito constitucional à proteção de dados pessoais.

É importante notar que a proteção desses direitos vai além da esfera individual, afetando, especialmente quando se trata da coleta de dados em grande escala, serviços como e-mails, redes sociais, aplicativos de mensagens instantâneas e navegadores, abrangendo coletividades inteiras cujos dados estão sendo apreendidos. Portanto, os testes de proporcionalidade e necessidade no uso dessas ferramentas devem levar em conta o impacto sobre os direitos de outros indivíduos, que muitas vezes nem estão envolvidos em uma investigação criminal, mas terão seus direitos suspensos em virtude das rotinas investigativas e de vigilância de tal natureza.

### 3.1.2. Marco Civil da Internet (MCI)

O MCI determina que é necessária uma ordem judicial para a guarda e acesso aos registros de conexão, aplicações e conteúdos das comunicações (Art. 7º, II e III; Art. 10, §§1º e 2º; Art. 15, §1º). Ou seja, ao aplicar o MCI, há um procedimento legal que deve ser seguido pela entidade responsável pela investigação quando o acesso a dados e comunicações for intermediado por um provedor de serviços, seja ele de conexão ou de aplicação. No entanto, quando o acesso é feito diretamente ao dispositivo, sem a participação de um intermediário, o MCI não estabelece diretrizes claras e específicas, o que pode gerar espaço para arbitrariedades, insegurança jurídica e abusos no monitoramento. Em qualquer ação de coleta, armazenamento, guarda e processamento de registros, dados pessoais ou comunicações por provedores de conexão e aplicativos da internet, quando ao menos um desses atos ocorrer no Brasil, o MCI impõe a obrigação de seguir a legislação brasileira, garantindo os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e registros.

### 3.1.3. Lei Geral de Proteção de Dados (LGPD) e LGPD Penal

Embora a Lei Geral de Proteção de Dados (LGPD) estabeleça normas sobre o uso de dados pessoais tanto no setor público quanto no privado, o artigo 4º da LGPD exclui do seu alcance o tratamento de dados realizado para "fins de segurança pública, defesa nacional, segurança de Estado e investigação e repressão de infrações penais" (inciso III, alíneas “a” a “d”). Assim como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a legislação brasileira prevê exceções no âmbito da segurança pública. No entanto, ao contrário da regulação europeia, que criou uma diretiva específica para tratar da esfera penal (Diretiva 2016/680), o Brasil ainda não possui uma legislação própria que aborde esse assunto.

### 3.1.4. PL 402/2024

O Projeto de Lei Nº 402/2024, de autoria do Senador Alessandro Vieira (MDB/SE), visa regulamentar o uso de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, tanto civis quanto militares.

Um dos principais aspectos do PL é a ênfase na observância de princípios consagrados, como a legalidade, a proporcionalidade, a necessidade, a segurança, a transparência e a fiscalização, alinhados com aqueles estabelecidos na Lei Geral de Proteção de Dados (LGPD). Além disso, o PL garante que a utilização dessas ferramentas será condicionada à autorização judicial prévia. Esse requisito reforça a necessidade de proteção contra abusos.

Cabe destacar a abrangência do PL, que vai além da regulação da extração de dados de dispositivos individuais, incluindo também a coleta em massa de dados, uma questão de crescente relevância diante da evolução das tecnologias de vigilância em larga escala. Outro ponto crucial do PL é a criminalização do monitoramento sem ordem judicial, bem como a obrigação de reportar incidentes relacionados a falhas ou abusos no uso dessas ferramentas. Essas disposições representam um avanço significativo na construção de um marco legal robusto, com o objetivo de assegurar a responsabilização dos agentes públicos envolvidos e prevenir abusos de poder. Entretanto, o projeto deixa de mencionar possíveis remédios legais disponíveis às vítimas de vigilância arbitrária.

Embora o projeto apresente avanços importantes, ele também requer um aprofundamento dos debates em torno das práticas de vigilância e supervisão com a participação multissetorial. A inclusão de mais detalhes sobre a elaboração de relatórios circunstanciados visando aumentar a transparência do processo é um ponto a ser levantado. A inclusão de medidas para garantir o devido processo legal também é essencial de forma a prevenir a violação da cadeia de custódia uma vez que essas ferramentas são capazes de alterar o conteúdo de dispositivos infectados.

Finalmente, o projeto deixa de incluir uma provisão que impeça o Estado de estabelecer relações comerciais com empresas envolvidas em violações de direitos humanos, tanto nacionais quanto estrangeiras. A criação de uma lista de empresas que atendam a esses critérios e a proibição de negócios estatais com essas entidades reforçaria o compromisso do Brasil com os direitos fundamentais e com a soberania nacional.

É importante ressaltar que, embora o PL represente uma ótima oportunidade de debater a fundo esse tema, ele não supre a necessidade de uma LGPD penal, já que esta traria um arcabouço legal geral de proteção de dados pessoais no âmbito da segurança pública e da

segurança nacional e defesa do Estado, de forma que as duas propostas seriam complementares, não excludentes.

Em suma, o Projeto de Lei Nº 402/2024 representa um avanço significativo na regulação das práticas de vigilância no Brasil, oferecendo um modelo legal que visa equilibrar os direitos de privacidade com a necessidade de segurança pública. Caso implementado adequadamente, o PL pode posicionar o Brasil como líder global na proteção dos direitos digitais, inspirando legislações similares em outros países, à semelhança do que ocorreu com o Marco Civil da Internet.

### 3.1.5. Arguição de Descumprimento de Preceito Fundamental 1143

Arguição de Descumprimento de Preceito Fundamental (ADPF) 1143 trata de questionamento realizado pela Procuradoria-Geral da República (PGR) acerca da falta de regulamentação do uso desses softwares por órgãos públicos. Inicialmente, a questão chegou ao Supremo Tribunal Federal por meio da Ação Direta de Inconstitucionalidade por Omissão (ADO) 84, na qual a PGR critica a ausência de ação normativa do Congresso Nacional para regular a matéria. A PGR argumentou que essas tecnologias vêm sendo empregadas por órgãos de inteligência e de repressão do Estado para realizar vigilância remota e invasiva de dispositivos móveis, sob o pretexto de combate ao terrorismo e ao crime organizado. Posteriormente, a ação foi convertida em ADPF 1143, a pedido da própria Procuradoria-Geral da República.

No início de 2024, o Ministro Cristiano Zanin, relator da ação, pediu informações ao Congresso Nacional e enviou os autos à Advocacia-Geral da União (AGU) e à PGR. Em abril do mesmo ano, o Ministro determinou a realização de uma audiência pública, com o objetivo de reunir informações técnicas e empíricas sobre o tema, marcada para os dias 10 e 11 de junho. O IP.rec participou da referida audiência e apresentou uma série de contribuições pertinentes à discussão.

Em maio de 2024, o ministro Cristiano Zanin, do Supremo Tribunal Federal (STF), ordenou que os Tribunais de Contas da União, dos estados e dos municípios fornecessem informações sobre a existência de processos administrativos relacionados a licitações, aquisições ou contratações de software espiões para dispositivos de comunicação pessoal, como celulares e tablets. Sobre os programas de rastreamento, o ministro esclareceu que as ferramentas em questão incluem, mas não se limitam, ao Pegasus, Imsi Catchers (como o Pixcell e o G12), além de aplicativos que monitoram a localização de alvos específicos, como o First Mile e o Landmark. Até novembro de 2024 mais de 20 Tribunais de Contas encaminharam documentos à corte[25].

[25] https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814

## 3.2. Legislação e Precedentes Internacionais Relevantes
### 3.2.1. Legislações e Iniciativas

#### a) Iniciativas Estadunidenses

Em 2021, o Departamento de Comércio dos Estados Unidos anunciou a inclusão de empresas de spyware na sua "Entity List", uma lista que reúne indivíduos, empresas e organizações estrangeiras consideradas uma ameaça à segurança nacional dos Estados Unidos, sujeitando-as a restrições de exportação e requisitos de licenciamento para determinadas tecnologias e produtos. Em 2021, as empresas israelenses de spyware NSO Group e Candiru foram adicionadas à lista[26]. Em 2023, a lista foi ampliada com a inclusão das empresas Intellexa, com sede na Grécia e Irlanda, e Cytrox AD, com sede na Hungria e na Macedônia do Norte[27].

Em 2024, a canadense Sandvine foi adicionada após seus produtos serem utilizados para monitoramento massivo da web, censura e ataques a ativistas de direitos humanos e dissidentes, incluindo o uso indevido de spyware comercial. No entanto, em outubro de 2024, a empresa teve seu nome retirado da lista, após adotar uma série de medidas para abordar o uso inadequado de sua tecnologia. Entre as ações tomadas estão a reestruturação corporativa e mudanças na liderança e no modelo de negócios, com foco em atender democracias comprometidas com a proteção dos direitos humanos. A empresa também se comprometeu a sair de países não democráticos, com 32 já abandonados e outros 24 em processo de saída. O governo estadunidense fala ainda em “fortalecimento de relações com a sociedade civil”, “a destinação de lucros para a proteção dos direitos”, a “inclusão de especialistas em direitos humanos na nova equipe de liderança”, “a avaliação das decisões de negócios por meio do recém-criado Comitê de Ética Empresarial” e “o monitoramento rigoroso do uso indevido de tecnologia nos países onde a empresa pretende permanecer”[28].

---

[26] U.S. Department of Commerce. Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities. 2021. Disponível em https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list Acesso em 10 de dez de 2024

[27] U.S. Department of State. The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities. 2023. Disponível em https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/ Acesso em 10 de dez de 2024

[28] Bureau of Industry and Security. Commerce Removes Sandvine from Entity List Following Significant Corporate Reforms to Protect Human Rights. 2024. Disponível em https://www.bis.gov/press-release/commerce-removes-sandvine-entity-list-following-significant-corporate-reforms-protect Acesso em 10 de dez de 2024

Em março de 2023, durante a segunda Cúpula pela Democracia, organizada pelos Estados Unidos, 11 países assinaram uma declaração conjunta reconhecendo a ameaça representada pelo uso indevido de spyware comercial. Eles destacaram a necessidade urgente de estabelecer controles rigorosos, tanto nacionais quanto internacionais, para conter a proliferação dessas ferramentas. A declaração foi posteriormente atualizada para incluir novos países que aderiram ao compromisso multilateral de combater o uso abusivo dessas tecnologias. Em março de 2024, durante a terceira Cúpula pela Democracia, países como Finlândia, Alemanha, Japão, Polônia, Irlanda e Coreia do Sul reforçaram o apoio a medidas concretas para enfrentar os riscos associados ao uso de spyware comercial[29].

A declaração enfatiza que o spyware comercial tem sido utilizado indevidamente por regimes autoritários e democracias, frequentemente para perseguir opositores políticos, intimidar dissidentes, suprimir a liberdade de expressão e violar direitos humanos. Em resposta, os países signatários se comprometeram a adotar medidas rigorosas para garantir que o uso de spyware por seus governos seja consistente com os direitos humanos, o estado de direito e as liberdades civis. Além disso, os países se comprometeram a implementar práticas robustas de controle de exportação, impedindo o envio de tecnologias para usuários que possam utilizá-las para "atividades maliciosas".

No entanto, a experiência prática tem mostrado que, muitas vezes, esses controles são facilmente burlados ou não são rigorosamente aplicados, como apontado em investigações conduzidas por membros do Parlamento Europeu[30]. Embora o compromisso com maior cooperação internacional e compartilhamento de informações sobre o uso indevido de spyware seja positivo, ainda faltam mecanismos claros e eficazes para garantir que essas medidas resultem em um impacto real na contenção da proliferação dessa tecnologia.

Em suma, embora a declaração de março de 2023 represente um avanço no reconhecimento do problema, as ações concretas até o momento não refletem a magnitude da ameaça. A administração Trump provavelmente não dará continuidade à campanha do governo Biden para limitar a proliferação de tecnologias de spyware comercial, amplamente utilizadas por regimes autoritários para perseguir jornalistas, ativistas de direitos civis e opositores políticos. Trump e seus aliados mantêm estreitas relações políticas e financeiras com dois dos maiores consumidores dessas ferramentas, Arábia

---

[29] The White House. Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. **The White House.** 2024. Disponível em https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/ Acesso em 10 de dez de 2024

[30] Sophie in 't Veld. European Parliament Draft Recommendation to the Council and the Commission pursuant to Rule 208(12) of the Rules of Procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. **European Parliament**. Disponível em https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Acesso em 10 de dez de 2024

Saudita e Emirados Árabes Unidos, demonstrando uma postura negligente em relação às violações de direitos humanos desses regimes.

Segundo Steven Feldstein, do Carnegie Endowment for International Peace, é muito provável que haja retrocessos nas políticas de controle do spyware, com a administração Trump priorizando os argumentos de contra-terrorismo apresentados pelas empresas de spyware, em detrimento das críticas dos defensores dos direitos digitais[31]. Nesse contexto, empresas como a NSO Group, que possuem vínculos estreitos com o governo israelense alinhado a Trump, devem encontrar um ambiente mais favorável para suas operações.

Veículos de mídia noticiaram que até outubro de 2024, a NSO gastou mais de 1,8 milhão de dólares com lobby, conforme documentos do *Foreign Agents Registrations Act*[32]. A empresa tem concentrado seus esforços em estabelecer conexões com legisladores republicanos e seguiu no esforço de utilizar o contexto da guerra de Israel para aumentar suas chances de retomar suas atividades. Ainda se promoveu como uma voluntária na guerra em Gaza, afirmando ajudar a localizar israelenses desaparecidos e reféns. Essa tentativa de convencer o governo americano a permitir seu retorno foi vista como uma estratégia de "limpeza de imagem" por parte da NSO.

### b) Pall Mall Process

Em fevereiro de 2024, os governos do Reino Unido e da França lançaram, em Londres, o *Pall Mall Process* (PMP), uma iniciativa voltada para o diálogo sobre a "proliferação e o uso irresponsável de capacidades comerciais de intrusão cibernética"[33]. A declaração resultante do evento inicial enfatizou princípios orientadores como *accountability*, precisão, supervisão e transparência, destacando a importância das parcerias público-privadas e da colaboração multissetorial, além de expressar preocupações com a segurança nacional, os direitos humanos e as liberdades fundamentais.

Entretanto, algumas questões críticas emergem no contexto dessa iniciativa. A limitada participação de países fora do eixo Norte Global é um aspecto relevante, já que a falta de diversidade geopolítica pode comprometer a eficácia do diálogo e a representatividade das vozes globais no debate sobre cibersegurança. Ademais, o processo de discussões, realizado

---

[31] Eric Geller. More Spyware, Fewer Rules: What Trump's Return Means for US Cybersecurity. **Wired**. 14 de novembro de 2024. Disponível em https://www.wired.com/story/trump-administration-cybersecurity-policy-reversals/ Acesso em 10 de dez de 2024

[32] Georgia Gee. Pegasus spyware maker said to flout federal court as it lobbies to get off U.S. blacklist. **The Intercept**. 21 de outubro de 2024. Disponível em https://theintercept.com/2024/10/21/pegasus-spyware-nso-israel-lobbying-republicans/ Acesso em 10 de dez de 2024

[33] Foreign, Commonwealth and Development Office. The Pall Mall Process declaration: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities. 2024. **UK government.** Disponível em https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities Acesso em 10 de dez de 2024

a portas fechadas e sem a presença de veículos de mídia, levanta questões sobre a transparência e a inclusão de diferentes atores e perspectivas. Esta falta de visibilidade pode restringir o impacto do evento e diminuir a confiança pública na integridade do processo.

Outro ponto a ser observado é a ausência de países que são grandes produtores de ferramentas de intrusão cibernética, como Israel, bem como de empresas fornecedoras desses recursos. A ausência desses atores centrais pode dificultar a implementação efetiva dos princípios estabelecidos, uma vez que a governança internacional sobre o uso de tais tecnologias depende, em grande parte, do comprometimento das partes envolvidas na produção e comercialização dessas ferramentas.

Finalmente, a limitada participação de organizações da sociedade civil representa uma lacuna significativa em um processo que se propõe a ser multissetorial. Essas organizações desempenham um papel crucial na iluminação de um mercado de cibersegurança opaco e, portanto, sua inclusão em discussões dessa natureza é essencial para garantir a transparência e a equidade nas decisões que afetam os direitos digitais e a segurança global.

Em resumo, embora o PMP apresente um avanço importante na abordagem de questões críticas relacionadas à cibersegurança, sua eficácia futura dependerá da ampliação da participação internacional, da maior transparência no processo e da inclusão ativa de todos os setores envolvidos, incluindo os atores globais e organizações da sociedade civil.

### 3.2.2. Precedentes

Embora casos judiciais possam ser fundamentados com base em informações vazadas ou em análises forenses digitais que identifiquem sinais característicos do uso de ferramentas de intrusão, a falta de um registro abrangente, acessível, confiável e completo das operações realizadas com essas tecnologias por governos dificulta tanto para as vítimas a comprovação dos fatos de suas alegações quanto para as autoridades judiciais a condução de investigações adequadas sobre todas as circunstâncias. O número de pedidos deferidos movidos por aqueles afetados pelo uso ilegal de ferramentas digitais (tanto vítimas individuais quanto empresas de tecnologia cujos sistemas foram ilegalmente invadidos) ainda é limitado na jurisdição brasileira. No entanto, nos últimos anos, têm crescido as ocorrências de julgados diretamente relacionados ao uso dessas ferramentas para monitorar e perseguir jornalistas e defensores dos direitos humanos, especialmente em diferentes tribunais regionais de proteção dos direitos humanos.

Em março de 2024, em um resultado histórico no caso *Membros do Coletivo de Advogados José Alvear Restrepo (CAJAR) v Colômbia*, a Corte Interamericana de Direitos Humanos identificou uma violação do direito à privacidade e enfatizou as tensões que o

desenvolvimento tecnológico e a disseminação generalizada circulação de dados traz para o domínio da proteção dos direitos humanos[34], destacando, portanto, a importância da autorização judicial, da supervisão independente das atividades de inteligência e da necessidade de soluções eficazes. A decisão também determinou que as operações de inteligência – que neste caso envolveram o uso de spyware e malware, entre outras tecnologias – só são legais e válidas quando acompanhadas de controles robustos e salvaguardas. Ecoando seu julgamento anterior em *Escher et al. vs Brasil*[35], a Corte enfatizou que proteger a privacidade e a liberdade de expressão é fundamental, e quaisquer medidas de vigilância devem ser autorizadas por uma autoridade judicial que defina seu alcance, duração e limites.

Já no continente europeu, no caso *Pietrzak e Bychawska-Siniarska e outros v. Polônia*, em maio de 2024, o Tribunal Europeu dos Direitos Humanos (CEDH) concluiu por unanimidade que a lei de vigilância da Polônia de 2016 violava o artigo 8.º da Convenção Europeia dos Direitos Humanos, que salvaguarda o direito à privacidade[36]. O Tribunal encontrou três questões-chave na lei, particularmente relacionadas à utilização de spyware comercial como o Pegasus: (i) a falta de salvaguardas adequadas, tais como a ausência de exigência de autorização judicial e recursos; (ii) retenção excessivamente ampla de dados de comunicação; e (iii) a fiscalização inadequada. Ainda na Europa, nos casos *Liberty e outros v. Reino Unido*, *Roman Zakharov v. Rússia e Pietrzak* e *Bychawska-Siniarska e outros v. Polônia*, a falta de supervisão eficaz e de soluções disponíveis ao abrigo da legislação nacional para aqueles sujeitos a ferramentas secretas de vigilância digital, como spyware por agências estatais, foi considerada uma violação do Artigo 13 da Convenção Europeia dos Direitos Humanos, ou seja, o direito a remédio eficaz em casos de violação de direitos humanos.

## Boas Práticas e Diretrizes para a Aquisição e Uso de Tecnologias pelo Governo Federal

### 4.1. Soberania Nacional e Proveniência de Tecnologias Adquiridas

Como observado pelo Comitê de Inquérito do Parlamento Europeu, que investiga o uso do Pegasus e de spyware de vigilância equivalente, países do Norte Global são vistos como

[34] CORTE INTERAMERICANA DE DIREITOS HUMANOS. Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" v. Colômbia. Sentença de 18 de outubro de 2023. Corte Interamericana de Direitos Humanos. Disponível em: https://privacyinternational.org/sites/default/files/2024-03/seriec_506_esp.pdf . Acesso em: 10 dez. 2024.

[35] CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros Vs. Brasil. Sentença de 6 de julho de 2009. Sentença de 20 de novembro de 2009. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_208_por.pdf Acesso em: 10 de dez de 2024

[36] TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Pietrzak v. Poland and Bychawska-Siniarska and others v. Poland. Disponível em https://hudoc.echr.coe.int/eng#{"itemid":["002-14333 Acesso em: 10 dez 2024

locais atrativos para as sedes de empresas de tecnologia e serviços de vigilância[37]. De acordo com estudos recentes, grandes fornecedoras de ferramentas de intrusão digital, como Cellebrite, FinFisher, Blue Coat, Hacking Team, Nexa Technologies, CyberPoint, L3 Technologies, Verint, Sandvine e NSO Group, estão sediadas em países considerados democráticos, como Estados Unidos, Itália, França, Alemanha, Canadá e Israel[38]. Ainda assim, muitas dessas empresas forneceram tecnologias tanto para regimes autocráticos quanto para o uso ilegítimo por governos democráticos ao redor do mundo.

Desde 2022, no entanto, observa-se uma mudança no discurso de diferentes governos em relação à necessidade de desenvolver um marco regulatório que vise coibir a proliferação e a ameaça representada pelo "uso indevido" de ferramentas de intrusão digital. Neste sentido, acreditamos que o Brasil precisa implementar um controle mais rigoroso sobre a importação dessas ferramentas, a fim de evitar que sejam desenvolvidas por ou adquiridas de atores que violem ou contribuam para a violação de direitos humanos, ou que coloquem em risco a sua soberania nacional.

Considerando os evidentes riscos aos direitos humanos e as dificuldades de fiscalização,o ex-Relator Especial da ONU sobre a liberdade de expressão, David Kaye, propôs uma moratória sobre o comércio de tecnologias de vigilância, com o objetivo de "permitir que os Estados desenvolvam um regime de controle e exportação e aprimorem os marcos legais que protejam a privacidade"[39]. Esse pedido foi apoiado por vários responsáveis por mandatos de Procedimentos Especiais da ONU. Em 2022, a Costa Rica se tornou o primeiro país a solicitar a implementação dessa moratória[40]. Assim, é essencial que o governo brasileiro considere a possibilidade de uma moratória na compra de certos equipamentos de vigilância privada com maior capacidade intrusiva, até que regras claras e responsáveis sejam estabelecidas. Essa medida é justificada pela gravidade dos danos causados por essas tecnologias.

---

[37] Sophie in 't Veld. European Parliament Draft Recommendation to the Council and the Commission pursuant to Rule 208(12) of the Rules of Procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. **European Parliament**. Disponível em https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Acesso em 10 de dez de 2024

[38] Steven Fieldstein. Governments Are Using Spyware on Citizens. Can They Be Stopped? **Carnegie Endowment.** 2021. Disponível em https://carnegieendowment.org/posts/2021/07/governments-are-using-spyware-on-citizens-can-they-be-stopped?lang=en Acesso em 10 de dez de 2024

[39] United Nations. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. Disponível em https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance Acesso em: 10 de dez de 2024

[40] Access Now. Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology. 2022 Disponível em https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware Acesso em 10 de dez de 2024

Finalmente, é importante observar os avanços em outras jurisdições. Empresas como Meta e Apple já processaram fornecedores de ferramentas de intrusão, como o NSO Group, devido ao uso de softwares como o Pegasus contra seus usuários[41]. O grupo israelense argumentou que, como seus produtos são utilizados por governos estrangeiros e agências de aplicação da lei, estaria protegido por imunidade soberana em solo estadunidense. No entanto, o Tribunal de Apelações do 9º Circuito rejeitou essa alegação, criando um precedente importante para a responsabilização das empresas de spyware[42]. A decisão permitiu a abertura de um processo legal contra a empresa, sendo um marco relevante para a discussão sobre a responsabilidade no uso dessas tecnologias.

### 4.2. Garantias de Transparência e Mecanismos de Monitoramento e Auditoria

Evidências, como as apresentadas em nosso estudo "Mercadores da Insegurança: Conjuntura e Riscos do Hacking Governamental no Brasil", tornam imperativo que o governo brasileiro seja transparente quanto aos seus esforços para garantir que os serviços de investigação e segurança nacional operem em conformidade com os direitos fundamentais e as liberdades civis. Durante a coleta de dados realizada por pesquisadores do IP.rec para o nosso estudo, a partir de Portais de Transparência e de pedidos fundamentados pela Lei de Acesso à Informação, foi possível constatar que o nível de transparência em relação à aquisição dessas ferramentas por órgãos públicos ainda é considerado baixo.

Além disso, órgãos responsáveis pelo escrutínio e pela supervisão, como a ANPD e tribunais de contas, não deveriam enfrentar dificuldades em obter essas informações. A supervisão independente sobre os serviços de inteligência e a aquisição de ferramentas de intrusão no Brasil é notoriamente fraca e, muitas vezes, inexistente. É fundamental que os mecanismos de escrutínio *ex-ante* e *ex-post* sejam fortalecidos. A criação de um mecanismo de supervisão independente para a utilização dessas tecnologias é urgente e necessária. Medidas como essas estabeleceriam formas mais eficazes de proteger os direitos e as liberdades civis da população.

É imprescindível que o governo brasileiro assegure que alegações de monitoramento ilegal e abuso de ferramentas de intrusão sejam investigadas adequadamente e que os responsáveis sejam punidos quando necessário. Também devem ser estabelecidas regras

---

[41] Stephanie Kirchgaessner. Court orders maker of Pegasus spyware to hand over code to WhatsApp. **The Guardian**. 29 de fevereiro de 2024. Disponível em https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group Acesso em 10 de dez de 2024

[42] UCI Law. One step closer to holding NSO Group accountable: The U.S. Solicitor General recommended the Supreme Court deny NSO's cert petition concerning the applicability of foreign sovereign immunity to a private entity. Disponível em https://ijclinic.law.uci.edu/2022/11/22/one-step-closer-to-holding-nso-group-accountable-the-u-s-solicitor-general-recommended-the-supreme-court-deny-nsos-cert-petition-concerning-the-applicability-of-foreign-sovereign-immunity-t/ Acesso em 10 de dez de 2024

claras para limitar o uso da "segurança nacional" como justificativa para a vigilância, garantindo supervisão judicial apropriada e o respeito às liberdades e garantias fundamentais.

Cabe ainda ressaltar que as ferramentas de intrusão digital não estão isoladas nesse cenário, mas fazem parte de toda uma rede de instituições e atores. A utilização dessas ferramentas muitas vezes depende da (in)existência de medidas regulatórias, salvaguardas legais e mecanismos de supervisão. Como observado pelo Parlamento Europeu, muitas vezes, de forma intencional ou não, sistemas regulatórios foram distorcidos, total ou parcialmente, ou projetados de maneira a facilitar o uso de mecanismos altamente intrusivos de monitoramento[43]. Assim, o uso ilegítimo ou abusivo dessas ferramentas deixa de ser um incidente e passa a ser uma estratégia. Portanto, recomenda-se que o governo brasileiro fundamente a utilização dessas ferramentas em uma base legal precisa e específica, com mecanismos de escrutínio robustos.

Remédios legais também devem existir e ser eficazes diante da obstrução por parte de órgãos governamentais. Como observado por Ní Aoláin, os Estados frequentemente estabelecem sistemas judiciários separados, como "tribunais secretos", para lidar com casos de segurança nacional[44]. As atividades de vigilância realizadas pelas agências estatais dificultam os mecanismos tradicionais de responsabilização. Além disso, a transferência transnacional de tecnologia impõe desafios jurisdicionais e práticos específicos. O governo brasileiro não deve permitir que o envolvimento de entidades privadas no desenvolvimento e na operação dessas ferramentas de intrusão torne ainda mais difícil o acesso a remédios eficazes para tratar violações de direitos.

### 4.3. Capacitação e Especialização das Autoridades Responsáveis

O direito a um julgamento justo é um elemento crucial do Estado Democrático de Direito. Os Estados garantem esse direito não apenas assegurando a independência dos juízes e tribunais, mas também preservando a integridade das evidências digitais e garantindo que tanto a acusação quanto a defesa tenham acesso igualitário às informações relevantes, incluindo dados sobre a cadeia de custódia.

---

[43] Sophie in ‘t Veld. European Parliament Draft Recommendation to the Council and the Commission pursuant to Rule 208(12) of the Rules of Procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. **European Parliament**. Disponível em https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Acesso em 10 de dez de 2024

[44] Fionnuala Ní Aoláin. United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. **United Nations.** Abril de 2023. Disponível em https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

A capacitação e especialização das autoridades responsáveis pela administração da justiça e pela proteção dos direitos fundamentais são elementos essenciais para garantir a preservação da integridade do processo judicial, especialmente em um contexto em que as evidências digitais desempenham papel central. O caso *Rook v. Alemanha*, analisado pelo Tribunal Europeu de Direitos Humanos, exemplifica os desafios que surgem em razão da utilização de tecnologias digitais em processos judiciais, ao destacar a violação do direito a um julgamento justo decorrente de falhas na preservação e no acesso às evidências digitais, incluindo a cadeia de custódia[45]. A integridade dessas evidências é fundamental para assegurar que os direitos da defesa sejam respeitados e que as provas possam ser contestadas de maneira significativa, conforme enfatizado pelo Tribunal.

A questão da proteção de dados e da preservação das evidências digitais foi ainda ressaltada pelo ex-Relator Especial da ONU sobre a liberdade de expressão, David Kaye, que alertou sobre os riscos de adulteração dos registros digitais por meio do uso de ferramentas como spywares[46]. Certas ferramentas de intrusão digital, ao possibilitarem a alteração discreta de dados sem deixar vestígios, representam uma grave ameaça à imparcialidade do processo judicial e ao direito a um julgamento justo, pois podem ser utilizadas tanto por atores estatais quanto por outros agentes, para modificar informações de forma intencional ou acidental. O uso de tais ferramentas, portanto, demanda uma regulação rigorosa e a formação específica dos agentes envolvidos, a fim de mitigar os riscos de manipulação de evidências.

A evolução das tecnologias de vigilância, como o Pegasus, exige uma adaptação no quadro regulatório global. A pressão por um sistema legal mais robusto visa reconhecer que certas ferramentas de intrusão, devido às suas características inerentes, não devem ser utilizadas em processos judiciais, uma vez que sua capacidade de alterar dados sem deixar rastros compromete o princípio da integridade das evidências[47]. O Supervisor Europeu de Proteção de Dados enfatizou que a vigilância digital intensificada e as ferramentas associadas, ao mudarem a dinâmica de investigação e julgamento, necessitam de

[45] TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Rook v. Germany. 25 de julho de 2019. Disponível em https://hudoc.echr.coe.int/eng#{"itemid":["001-194614"]}. Acesso em 10 de dez de 2024.

[46] David Kaye e Sarah McKune. The Scourge of Commercial Spyware—and How to Stop It. **Lawfare**. 2023. Disponível em https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it Acesso em 10 de dez de 2024

[47] Fionnuala Ní Aoláin. United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. **United Nations.** Abril de 2023. Disponível em https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf Acesso em 10 de dez de 2024

autoridades altamente qualificadas, que possam assegurar o uso legítimo dessas tecnologias dentro dos limites do Estado de Direito[48].

Portanto, a formação técnica e a especialização das autoridades brasileiras responsáveis pela coleta, preservação e análise de evidências digitais são fundamentais para garantir que o processo judicial não seja comprometido pela utilização inadequada dessas ferramentas. A colaboração internacional entre o Brasil e diferentes jurisdições, visando à troca de conhecimentos e boas práticas, é igualmente necessária para que as autoridades possam responder de forma eficaz aos desafios impostos pela vigilância digital e pela integridade das evidências, preservando assim os direitos humanos e o Estado Democrático de Direito.

### 4.4. Participação da Sociedade Civil e Especialistas no Tema

Nos últimos anos, a participação ativa da sociedade civil tem sido essencial para trazer à tona as implicações éticas e os abusos relacionados ao uso de ferramentas de intrusão digital. Organizações não governamentais, jornalistas e ativistas têm sido os principais responsáveis por expor a utilização indevida dessas tecnologias, muitas vezes em regimes autoritários ou para fins de vigilância indiscriminada em democracias. No entanto, apesar de sua contribuição crucial para a visibilidade do problema, a sociedade civil continua sendo marginalizada nas discussões que envolvem a regulamentação e a responsabilização desses atos, muitas vezes em detrimento de uma abordagem mais técnica e transparente.

A ausência de uma participação efetiva da sociedade civil e de especialistas na área compromete o processo de formulação de políticas públicas que visem à proteção de direitos fundamentais, como a privacidade e a liberdade de expressão. Especialistas no campo da tecnologia, direitos humanos e segurança digital têm alertado para a necessidade de criar um ambiente regulatório mais inclusivo e participativo, onde diferentes vozes possam ser ouvidas. Dessa forma, a participação da sociedade civil e de especialistas é imprescindível para garantir um equilíbrio entre segurança e liberdade, além de assegurar que as normas adotadas estejam alinhadas com os princípios democráticos e os direitos humanos.

A contribuição de especialistas em áreas como direitos digitais é crucial para garantir que a regulamentação do uso de ferramentas de intrusão digital seja fundamentada em conhecimento técnico robusto e em uma abordagem de direitos fundamentais. No Brasil, um debate interdisciplinar e transparente é essencial para que o processo de formulação de políticas públicas não seja dominado exclusivamente por interesses econômicos ou de

[48] European Data Protection Supervisor. EDPS Preliminary Remarks on Modern Spyware. 2022. Disponível em https://www.edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en Acesso em 10 de dez de 2024.

segurança, mas também considere os impactos sociais e individuais do uso dessas tecnologias. A criação de um ambiente regulatório inclusivo e participativo assegura que as normas adotadas estejam alinhadas com os princípios democráticos e direitos humanos, evitando abusos e excessos no uso de ferramentas de intrusão digital, que podem ser facilmente mal utilizados para fins de vigilância indiscriminada como constatado pelo trabalho do IP.rec, jornalistas e outros representantes da sociedade civil. A colaboração entre sociedade civil e autoridades públicas é, portanto, essencial para a construção de um sistema de controle mais justo e eficaz sobre o uso dessas tecnologias no Brasil.

## 5. Desafios e Considerações Finais

Há um desafio constante de como equilibrar a proteção dos cidadãos com os direitos humanos garantidos. Por vezes, o Estado utiliza da narrativa de proteção para introduzir equipamentos de intrusão e vigilância, quando na realidade eles causam mais riscos e insegurança.

O desenvolvimento tecnológico de soluções digitais cria falhas técnicas. Ainda que de forma não intencional, o surgimento de novas vulnerabilidades cria maiores áreas de ataques para atores mal intencionados. Por muita das vezes, essas próprias falhas são desconhecidas pelo time de desenvolvimento, que só toma conhecimento tempos depois. Consequentemente, empresas de intrusão e *bug bounties* irão explorar comercialmente essas falhas, enquanto os Estados irão utilizar para fins de inteligência.

Nesse sentido, para as correções,  fazem-se necessários avanços em cibersegurança, campo esse que avança em pesquisa de novas técnicas de proteção, oferecendo cada vez mais níveis superiores de segurança. Contudo, do lado oposto, as soluções de intrusão também avançam, desenvolvendo e identificando novas formas de burlar mecanismos de defesa, gerando um cenário circular de insegurança, que parece crescer cada vez mais.

Por isso que frente ao rápido desenvolvimento tecnológico, são necessárias atualizações constantes nas políticas de cibersegurança e de regulação de ferramentas de intrusão digital. Todos os incrementos devem levar em consideração essa conjuntura para que seja criado um ambiente mais seguro para os usuários.

Em face desses desafios e avanços tecnológicos, é fundamental que o Brasil adote uma abordagem proativa para proteger seus cidadãos, promovendo a transparência nas operações de vigilância e assegurando que qualquer uso de ferramentas de intrusão digital seja monitorado adequadamente.

O fortalecimento de marcos legais, mecanismos de supervisão e a inclusão de diferentes setores da sociedade, incluindo especialistas e organizações civis, são cruciais para assegurar que o uso dessas tecnologias seja transparente, responsável e alinhado com

princípios democráticos. No Brasil, é essencial que o governo adote medidas rigorosas para controlar a importação e o uso dessas ferramentas, garantindo que não sejam empregadas na violação de direitos fundamentais ou ameacem a soberania nacional.

Além disso, a capacitação das autoridades responsáveis pela investigação e análise de evidências digitais, a transparência nas aquisições de tecnologias de vigilância e a implementação de um controle efetivo sobre sua utilização são fundamentais para garantir que os direitos da população sejam protegidos, e que o uso de tecnologias digitais esteja em conformidade com o Estado Democrático de Direito.

## 6. Recomendações

**Promoção da transparência em processos licitatórios**: Recomenda-se uma maior transparência no processo de licitação pública em relação à aquisição de produtos e à contratação de serviços de intrusão digital com empresas do setor privado, observando potenciais questões relacionadas à segurança pública e nacional, assim como aos direitos humanos.

**Garantia de transparência na utilização de ferramentas de intrusão digital**: Recomenda-se que, em caso de utilização de ferramentas de intrusão digital, seja promovida total transparência, a fim de garantir a conformidade com as normas legais e éticas, além de preservar a confiança pública e a proteção dos direitos fundamentais e liberdades civis.

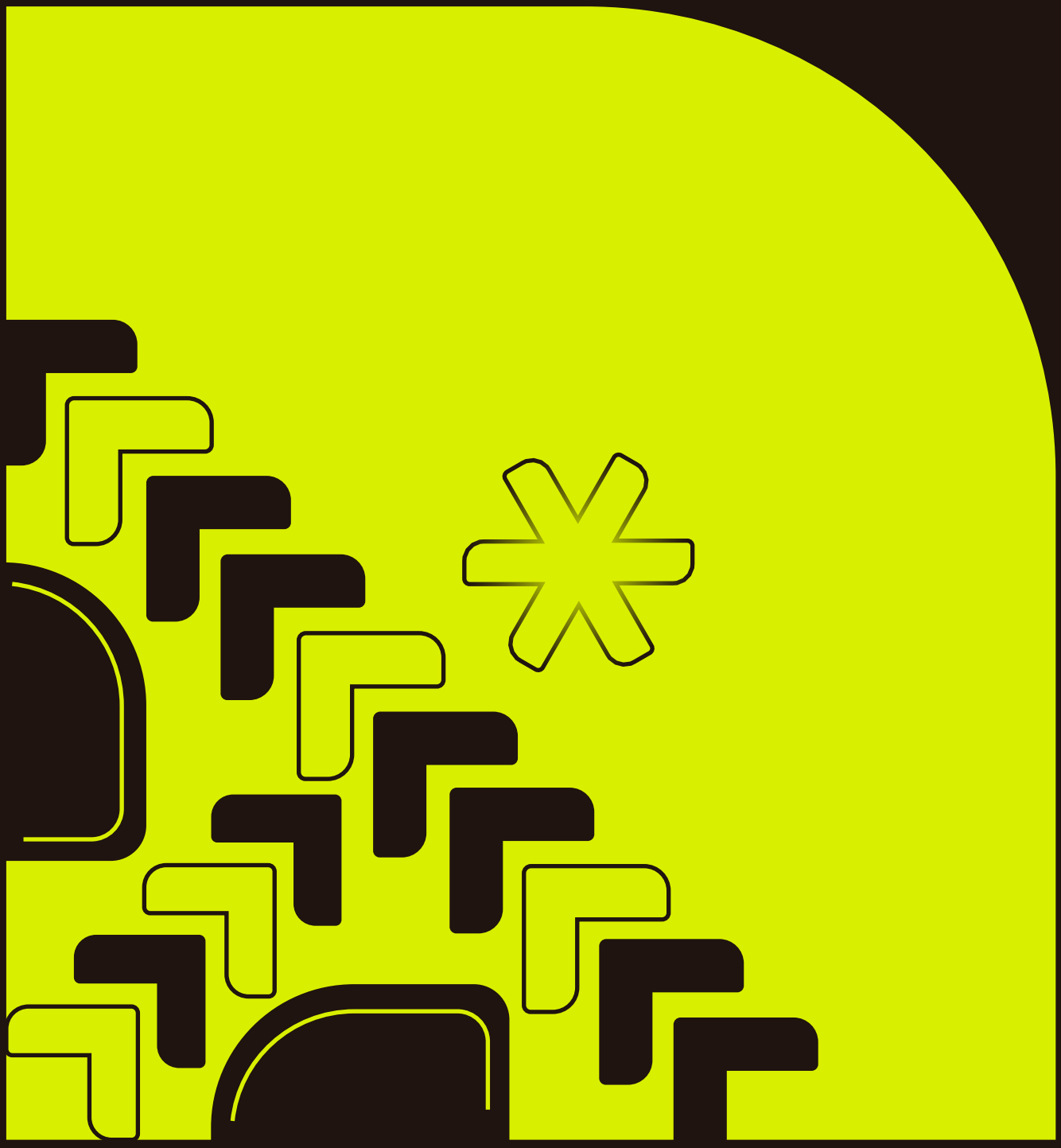
**Observância de direitos humanos por empresas contratadas**: Recomenda-se a não negociação com empresas envolvidas no monitoramento e coleta de informações sobre ativistas, acadêmicos, jornalistas, dissidentes, figuras políticas ou membros de organizações não governamentais ou comunidades marginalizadas, com o objetivo de limitar liberdades de expressão ou possibilitar abusos aos direitos humanos ou supressão das liberdades civis.

**Banimento de ferramentas de intrusão sem critérios de confiabilidade**: Recomenda-se o banimento do uso de ferramentas de intrusão digital (sobretudo as remotas) que não possuam características de auditabilidade, transparência e especificidade, como é o caso do Pegasus.

**Implementação de moratória sobre ferramentas de alta capacidade intrusiva**: Recomenda-se a implementação de uma moratória relacionada ao uso e aquisição de ferramentas digitais com alta capacidade intrusiva até a construção de uma regulação adequada para a matéria.

**Aprovação da Lei Geral de Proteção de Dados Penal**: Faz-se essencial a aprovação de uma Lei Geral de Proteção de Dados para fins de segurança pública, defesa nacional e

inteligência, com o objetivo de garantir a proteção da privacidade e dos direitos individuais.



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife