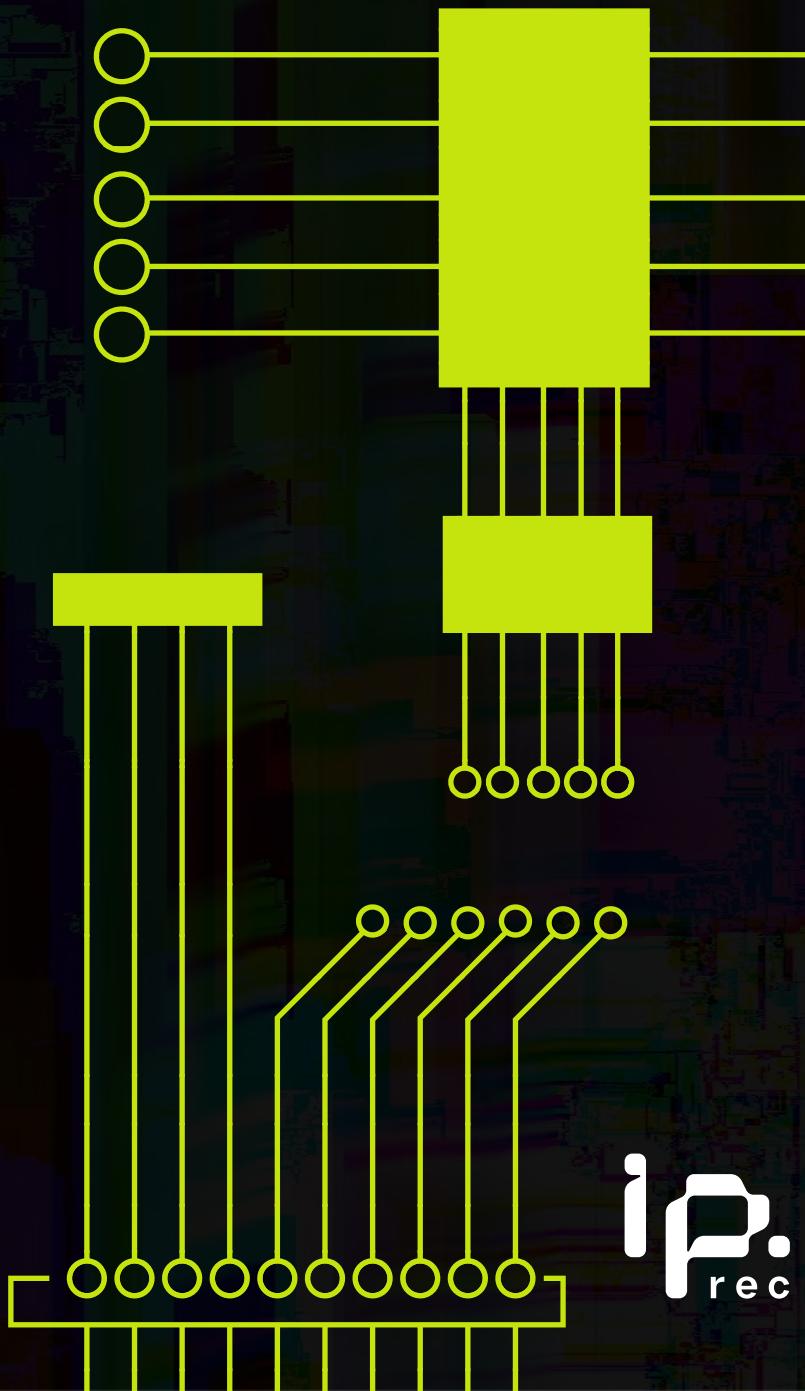
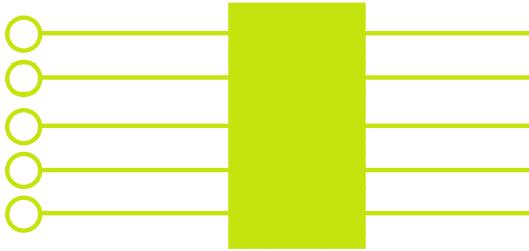


Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil.

Novembro, 2022

André Ramiro (coord.)
Pedro Amaral
Mariana Canto
Marcos César M. Pereira





Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil.

Autores:

André Ramiro (coord.)
Pedro Amaral
Mariana Canto
Marcos César M. Pereira

Revisão:

Raquel Saraiva

Realização:

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

Design e Diagramação:

Clara Guimarães



Índice

SUMÁRIO EXECUTIVO.....	1
1. INTRODUÇÃO.....	3
2. HACKING GOVERNAMENTAL: conceito e um breve balanço do debate global.....	6
2.1. Definição.....	6
2.2. Escalabilidade e crescente protagonismo das ferramentas de hacking.....	7
2.3. DESVIOS À CRIPTOGRAFIA: a ofensiva policial enquanto atalho aos pedidos de acesso à comunicações privadas.....	11
2.3.1. A criptografia vai ao STF: bloqueios ao WhatsApp e o Tratado de Assistência Legal Mútua (MLAT).....	11
2.3.2. Cortando o intermediário: o acesso a dados de forma direta.....	12
2.4. NUTRINDO O MERCADO DE VULNERABILIDADES.....	14
2.5. VAZAMENTO DE FERRAMENTAS, ABUSOS E DESVIOS DE FINALIDADE.....	18
3. INSEGURANÇA DISTRIBUÍDA: negociando a exploração de vulnerabilidades enquanto cultura investigativa no Brasil	20
3.1. O circuito internacional: importação e negociações entre Brasil e países exportadores de tecnologias de vigilância	20
3.2. Ferramentas de hacking no Brasil, em números	28
3.3. Distribuição de contratos no Brasil.....	30
3.4. Panorama geral dos achados	47
3.4.1. Olhando de perto: o caso da Cellebrite e Techbiz Forense Digital.....	48
3.4.2. Olhando de perto: o caso da Verint Systems (Cognyte/Suntech).....	50
3.5. Muito a esconder: a cultura do sigilo sobre as ferramentas de hacking.....	51
3.5.1. Recursos empregados para negar acesso às informações.....	52
3.5.2. Olhando de perto: o Projeto Excel.....	65
4. CONJUNTOS REGULATÓRIOS	68
4.1. Um breve panorama internacional	68
4.2. Quadro regulatório atual no Brasil: na omissão há permissão?	72
4.3. Perspectivas regulatórias	74
4.4. Princípios norteadores.....	76
5. CONCLUSÃO	80

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Amaral, Pedro

Mercadores da insegurança [livro eletrônico] :
conjuntura e riscos do hacking governamental no
Brasil / Pedro Amaral, Mariana Canto, Marcos
César M. Pereira ; coordenação André Ramiro. --

1. ed. -- Recife, PE : IP.rec, 2022.

PDF.

Bibliografia.

ISBN 978-65-995947-5-5

1. Acesso à informação 2. Administração pública
3. Aplicativos - Programas de computador 4. Dados -
Proteção - Brasil 5. Direitos fundamentais 6. Governoeletrônico 7. Proteção de
dados - Leis e legislação
8. Proteção de dados pessoais I. Canto, Mariana.
II. Pereira, Marcos César M. III. Ramiro, André.
IV. Título.

22-132314

CDD-320.02850981

Índices para catálogo sistemático:

1. Brasil : Governo eletrônico 320.02850981

Aline Grazielle Benitez - Bibliotecária - CRB-1/3129



Sumário Executivo

Em políticas públicas, o debate sobre como as técnicas de investigações criminais devem responder à digitalização das dinâmicas sociais tem se sobressaído e caminha em uma linha tênue entre otimização dos processos administrativos e possíveis transgressões em relação aos direitos fundamentais de pessoas que sejam alvo de investigações e rotinas de vigilância. Nesse sentido, técnicas de hacking governamental, ou seja, de superação de recursos de segurança em dispositivos pessoais e aplicações, vem ganhando uma escalabilidade crescente e envolve a multiplicação de fabricantes, revendedores e contratos com a administração pública, ao passo em que seus efeitos colaterais aos direitos fundamentais, sobretudo em relação à sociedade civil, vêm sendo denunciados internacionalmente.

A fabricação e venda de ferramentas de hacking para uso inicialmente “legítimo” por autoridades públicas envolve um percurso de exploração de vulnerabilidades em sistemas de segurança. Quer dizer, para que as ferramentas cumpram seu propósito, é necessário que brechas de segurança sigam sendo descobertas e mantidas desatualizadas pelos provedores, excluindo-os de uma dinâmica de melhoria de seus serviços. Como argumentamos, a competitividade entre certos programas de recompensa (bug bounties) ilustra uma lógica lucrativa que, fundamentalmente, afasta a atualização de sistemas de segurança, beneficiando, com informações privilegiadas sobre brechas de segurança, fabricantes de ferramentas de hacking e, consequentemente, programas de vigilância e investigação de autoridades públicas que os contratam.

Enquanto o uso de ferramentas de hacking tem sido problematizado internacionalmente, no Brasil é incipiente a incidência política e as pesquisas dedicadas sobre o tema. Como forma de oferecer dados concretos e fomentar, assim, o debate público e propostas regulatórias, realizamos levantamento de contratos de fabricantes e representantes comerciais com a administração pública no Brasil, envolvendo pedidos via Lei de Acesso à Informação às 27 Secretarias Estaduais responsáveis pelas atividades de segurança pública, incluindo o Distrito Federal; aos 27 Ministérios Públicos Estaduais, incluindo o Distrito Federal; ao Ministério Público Federal e à Polícia Federal através do Ministério da Justiça e Segurança Pública; ao Comando do Exército (CEX), ao Comando da Marinha (CMAR) e ao Ministério da Defesa; e ao Gabinete de Segurança Institucional (GSI). Em paralelo, foi realizada pesquisa nos Portais de Transparência dos 26 Estados, do Distrito Federal e do Governo Federal. A partir do recorte temporal entre 2015 e 2021, o resultado foi o levantamento de 209 documentos contratuais a nível estadual e federal, compreendendo compra, treinamento de funcionários, termos aditivos, atualização de software e outros atos administrativos que comprovam que determinadas ferramentas de hacking estão e/ou estiveram em uso no país. O levantamento se deve, na grande maioria dos casos, a documentações constantes nos Portais de Transparência, enquanto as respostas aos pedidos de acesso à informação, com raras exceções, tendiam à negativa das informações com base em justificativas de sigilo ou à simples alegação de inexistência de tais contratos.

O conjunto de fabricantes encontrados inclui Cellebrite, Micro Systemation AB (MSAB), OpenText, Magnet Forensics, Exterro/AccessData e Verint Systems/Cognyte/Suntech, dois principais representantes comerciais no Brasil - a Techbiz Forense Digital e a Apura Comércio de Softwares e Assessoria em Tecnologia da Informação - e 20 diferentes soluções fornecidas às entidades públicas. Os achados envolvem o acesso a ferramentas de hacking pela totalidade dos Estados da federação e pelo Governo Federal, além de uma relativa tendência de crescente orçamentária de investimento público no acesso às ferramentas. Além da análise quantitativa, foi possível traçar correlações entre empresas de maior notoriedade no mercado, como Cellebrite e Verint/Cognyte/Suntech, com fatos políticos nacionais e internacionais que notadamente sugerem os riscos aos direitos humanos colaterais envolvidos no uso indiscriminado e não supervisionado de tais ferramentas, incluindo denúncias de corrupção,



vazamento de informações sigilosas e envolvimento das ferramentas na perseguição à sociedade civil.

Adicionalmente, a partir de um levantamento de legislação pertinente ao tema, analisamos a insuficiência do conjunto regulatório nacional vigente para endereçar esses expedientes, uma vez que, além de não contarem com base legal específica, não levam em consideração testes de necessidade e proporcionalidade diante dos níveis inéditos de violação aos direitos fundamentais derivados do acesso indiscriminado a dados pessoais que proporcionam. Propomos, então, um conjunto de 7 princípios como forma de guiar futuras propostas legislativas que busquem regular a atividade.

Concluímos que o uso de ferramentas de hacking por autoridades brasileiras se encontra em estágio surpreendentemente avançado de assimilação e, basicamente, qualquer recurso de segurança em dispositivos pessoais é superado pelas suas capacidades. A conjuntura sugere um momento de inflexão sobre a proteção a direitos fundamentais associados à proteção de dados e ao sigilo das comunicações, bem como ao cenário de insegurança colocado pela presença da indústria e do circuito comercial de ferramentas de hacking no Brasil, “legitimada” pelas demandas governamentais por tecnologias forenses.

O IP.rec entende que é urgente a qualificação do debate sobre os efeitos dessa prática ao ecossistema de direitos e segurança no país. Ensaios regulatórios já se encontram no horizonte legislativo nacional e devem ser endereçados com prioridade - antes que o status quo a partir do qual iremos refletir sobre permissões e limites no uso dessas ferramentas seja pautado por sua indústria, e não pelo processo de formulação de políticas públicas verdadeiramente democrático, multissetorial e centrado nos usuários finais das tecnologias.

Por fim, agradecemos as fundamentais colaborações dos consultores técnicos Jacqueline Abreu (Universidade de São Paulo) e Carlos Cabral (Tempest Security), assim como as valiosas contribuições de Bruno Morassuti (Fiquem Sabendo).

Boa leitura.



I. Introdução

A disponibilidade de canais relativamente facilitados de acesso à dados derivados do uso de dispositivos pessoais, como computadores, smartphones, dispositivos IoT e outros fenômenos tecnológicos, não somente inauguram um ecossistema de serviços governamentais e empresariais baseado nos altos níveis conectividade e digitalização, mas também abrem brechas de acesso à coleta de dados para finalidades avessas ao interesse do indivíduo e da coletividade. Essas fissuras, resultantes não somente de modelos de negócio que as mantêm disponíveis, mas também da exploração de vulnerabilidades nesses sistemas, são constantemente aproveitadas tanto por agentes maliciosos, como também por entidades governamentais de inteligência e investigação.

No Brasil, são relativamente recentes as problematizações dedicadas ao aparato de ferramentas de extração de dados e acesso remoto por autoridades investigativas, ainda que, muito possivelmente, acordos comerciais já estivessem estabelecidos há muitos anos para municiar agências governamentais. Além disso, enquanto alguns poucos fornecedores estiveram sob os holofotes das denúncias de organizações defensoras dos direitos humanos, como FinFisher,¹ NSO Group² ou Cellebrite³, outros agentes econômicos, menos conhecidos no circuito político, também poderiam estar viabilizando uma variedade de instrumentos de hacking para autoridades brasileiras. Essas foram, portanto, as duas principais hipóteses que nortearam o desenvolvimento desta pesquisa.

Por um lado, argumenta-se que os parâmetros inéditos oferecidos por protocolos de segurança da informação em dispositivos pessoais têm, a um só tempo, elevado a segurança econômica e relativa aos dados pessoais de usuários finais desses dispositivos, fomentando a cadeia de confiança entre usuários, infraestruturas críticas e serviços. Por outro, também têm iniciado um novo capítulo sobre como investigações são conduzidas. Afinal, interceptações telefônicas já não seriam mais tão pertinentes, dada a migração das comunicações para aplicações de mensageria instantânea criptografadas; o cumprimento de mandados de busca e apreensão em domicílios também se depara com protocolos de segurança em dispositivos apreendidos, desde seu bloqueio ao armazenamento de dados com criptografia ou em serviços de nuvem localizados em outras jurisdições; ou mesmo a necessidade de que expedientes de infiltração alcancem círculos também protegidos por protocolos de segurança e anonimato, como grupos em plataformas de comunicação ou fóruns da deep web.

Essa narrativa capitaneou um discurso articulado por parte de agências de investigações que buscam, portanto, por mais recursos de vigilância: argumentam que são afetadas pelo obscurecimento das capacidades investigativas.⁴ Como resultado, sob a chave da “modernização” dessas capacidades, foi percebida uma janela de oportunidade para a fabricação e fornecimento, pelo setor privado, de tecnologias que exploram vulnerabilidades em dispositivos para extração em massa de dados pessoais e para acesso e monitoramento remoto. Com efeito, operam uma forma de hacking em sua grande maioria legitimado pelo Estado, colocando autoridades investigativas no pólo ativo/ofensivo de uma dinâmica que depende, fundamentalmente, de falhas de segurança e inauguram novas perguntas do ponto de vista da ética, da segurança da coletividade e do devido processo investigativo.

1 MARQUIS-BOIRE, Morgan et al. You Only Click Twice: FinFisher's Global Proliferation. Monk School of Global Affairs, 2013. Disponível em <https://web.archive.org/web/20140809015927/https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/>. Acesso em 22 de julho de 2022.

2 ANISTIA INTERNACIONAL. Op. cit.

3 Ver ACCESS NOW. Going public? Cellebrite's tech is incompatible with human rights, investors must make a stand. 2021. Disponível em <https://www.accessnow.org/cellebrite-human-rights-investors/>. Acesso em 22 de julho de 2022.

4 ZITTRAIN, Jonathan et al. Don't Panic: Making Progress on the “Going Dark” Debate. Berkman Klein Center for Internet and Society, 2016. Disponível em https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1&isAllowed=y. Acesso em 22 de julho de 2022.



Ainda que esses expedientes não sejam recentes, apenas há alguns anos vêm se destacando na grande mídia. Muitas vezes, em razão do vazamento de ferramentas das mãos de agências governamentais, resultando no comprometimento de segurança de milhões de computadores, como no caso do WannaCry⁵ e do NotPetya,⁶ ou por seu uso por figuras antidemocráticas, em perseguição a ativistas, dissidentes políticos, ou mesmo por spywares fabricados por agentes econômicos legitimados no mercado global serem encontrados em dispositivos pessoais de liderança políticas.⁷ Os fatos políticos revelam, portanto, um efeito colateral de extremo risco não somente ao ecossistema de segurança, mas também à privacidade da coletividade, ao exercício dos direitos políticos derivados, como a liberdade de expressão e opinião, bem como à integridade física⁸ de indivíduos em situações políticas antidemocráticas.

Sendo assim, buscamos, inicialmente, uma pesquisa empírica baseada no levantamento de acordos comerciais envolvendo autoridades investigativas e fornecedores privados em duas frentes: uma delas a partir de pedidos via Lei de Acesso à Informação às 27 Secretarias Estaduais responsáveis pelas atividades de segurança pública, incluindo o Distrito Federal; aos 27 Ministérios Públicos Estaduais, incluindo o Distrito Federal; ao Ministério Público Federal e à Polícia Federal, ao Ministério da Justiça e Segurança Pública; ao Ministério da Defesa; Comando do Exército (CEX); Comando da Marinha (CMAR); e ao Gabinete de Segurança Institucional (GSI). Em paralelo, foi realizado levantamento nos Portais de Transparência dos 26 Estados, do Distrito Federal e do Governo Federal.

No primeiro caso, as perguntas envolveram os seguintes tópicos: licitações e contratos para aquisição das ferramentas de extração, desbloqueio e acesso remoto; protocolos ou regras de segurança da informação; cadeia de custódia e de condições processuais para uso dessas ferramentas; prioridades de uso das ferramentas em termos de tipos de crimes; e, quando relevante, a existência de ferramentas de desenvolvimento próprio das entidades. Foram 8 perguntas para a maioria dos destinatários, exceto para a Polícia Federal, que recebeu duas questões adicionais. Num momento posterior, uma segunda rodada de pedidos de informação buscou sanar informações incompletas coletadas nos Portais da Transparência e, também, aprofundar em tópicos específicos que surgiram ao longo do levantamento de dados, como o Projeto Excel, capitaneado pela Diretoria de Inteligência da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública.

Na busca nos Portais de Transparência, fizemos a busca nominal por 32 empresas a partir de levantamento prévio de fornecedores conhecidos no mercado relativo às ferramentas de hacking usadas por agências de investigação e vigilância nacional e mundialmente. Essa escolha foi feita frente à enorme variação dos termos empregados como objeto dos contratos, como “extração de dados”, “monitoramento”, “interceptação”, “análise de dados”, “acesso remoto”, entre várias outras expressões empregadas, que eram muito abrangentes para abranger o conjunto de específico de serviços investigados aqui ou pouco precisos para identificar os contratos com as mais diversas descrições de objeto.

Adicionalmente, a partir de uma abordagem teórica, com base em revisão de literatura derivada de publicações de organizações não-governamentais, acadêmicas, de veículos de imprensa, bem como relatórios e conjuntos regulatórios governamentais, para desenvolver a análise dos resultados do levantamento, assim como do contexto brasileiro e internacional em que se insere o debate. Para qualificar o entendimento sobre os achados e sobre o contexto tecnológico, processual e político no Brasil relativo

5 KARSPERSKY. Ransomware WannaCry: all you need to know. 2022. Disponível em <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>. Acesso em 22 de julho de 2022.

6 GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired, 2018. Disponível em <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. Acesso em 22 de julho de 2022.

7 CORERA, Gordon. Pegasus: French President Macron identified as spyware target. BBC, 2021. Disponível em <https://www.bbc.com/news/world-europe-57907258>. Acesso em 20 de julho de 2022.

8 FAIFE, Corin. New analysis further links Pegasus spyware to Jamal Khashoggi murder. The Verge, 2021. Disponível em <https://www.theverge.com/2021/12/21/22848485/pegasus-spyware-jamal-khashoggi-murder-nso-hanan-elatr-new-analysis>. Acesso em 20 de julho de 2022.



ao tema de pesquisa, foram conduzidas entrevistas com pesquisadores, ativistas, advogados, jornalistas e especialistas em segurança da comunidade tecnológica.

Cabe notar que este estudo não inclui, como objeto de pesquisa, tecnologias e serviços de inteligência em fontes abertas (open source intelligence, ou “OSINT”) e suas empresas fornecedoras.^{9¹⁰} Ainda que muito próximos, os instrumentos de análise são razoavelmente distintos daqueles utilizados para compreender técnicas de hacking com base em extração ou acesso remoto a dados armazenados. Reconhece-se, no entanto, a importância crescente do escrutínio sobre empresas que fornecem ferramentas de OSINT, sobretudo do ponto de vista do direito à proteção de dados pessoais, recentemente declarada direito fundamental estabelecido na Constituição Federal e que acoberta, também, dados disponíveis em fontes abertas e devem atender a princípios como o da finalidade e da necessidade no uso de dados pessoais.

Por fim, objetivou-se lançar luz sobre a avançada capilaridade das ferramentas de hacking na estrutura organizacional investigativa no Brasil, tanto a nível dos Estados quanto a nível Federal, incluindo suas funcionalidades e os riscos que colocam ao arcabouço de proteção à privacidade e proteção de dados não somente dos indivíduos, mas de coletividades. A partir da apresentação de um “status quo” sobre as ferramentas de hacking no país, também objetiva-se conferir insumos à formulação de políticas públicas que busquem regular essas atividades antes que se estabeleça uma cultura forense cujas regras são ditadas por entidades privadas enraizadas em práticas de instituições públicas, o que tornaria mais difícil a devida reparação.

Foi possível chegar a uma diversidade de atores do setor privado que fornecem essas ferramentas para as forças de investigação e vigilância no país, atores cujos contratos chegam a remontar dez anos atrás, com sucessivas renovações, aditamentos e licenciamentos de novos produtos. Também se comprova o estado regulatório e procedural imaturo, permitindo que atividades sejam conduzidas sem bases legais padronizadas, com importantes variações, como a existência ou não de mandado judicial, abrindo claras margens para arbitrariedades. Finalmente, também foi notável o sigilo sobre as informações administrativas contratuais e programas governamentais dedicados à capacitação de agentes investigativos em técnicas de hacking, dificultando o escrutínio da sociedade civil. Ou seja, as notícias que vêm à superfície da grande mídia são, efetivamente, apenas a “ponta do iceberg”.¹¹

Quando se observa a quantidade e qualidade de informações que dispositivos pessoais podem conter, esse ganho de capacidade investigativa pelo Estado deve ser criticamente avaliado e, logo, necessariamente limitado em seus usos, a fim de evitar abusos. Os ganhos de capacidade e alcance sobre informações pessoais, por parte do Estado, são cada vez mais possibilitados pelas parcerias com entes privados, mas que, longe de inevitáveis, são frutos de um conjunto de práticas e de “filosofias”, isto é, “discursos que são ativados na operação dos sistemas e instituições existentes e das formas de ação penal que os compõem”.¹² Assim, é necessário avaliar criticamente os recursos discursivos empregados na justificação da expansão, qualitativa e quantitativa, das capacidades policiais, considerando os fins alegados, mas também aqueles concretamente alcançados nas políticas de segurança pública e de segurança nacional.

9 MENDES, Lucas. TCU suspende licitação de sistema espião pelo Ministério da Justiça. Poder 360, 2021. Disponível em <https://www.poder360.com.br/governo/tcu-suspende-liticacao-de-sistema-espiao-pelo-ministerio-da-justica/>. Acesso em 21 de julho de 2022.

10 Apesar de não terem sido consideradas para fins de análise, durante o processo de coleta de dados foi encontrada uma quantidade considerável de ferramentas de OSINT em atuação no Brasil.

11 Também chega a essa conclusão a Anistia Internacional. Ver ANISTIA INTERNACIONAL. Uncovering the iceberg: the digital surveillance crisis wrought by States and the private sector. 2021. Disponível em <https://www.amnesty.org/en/wp-content/uploads/2021/07/DOC1044912021ENGLISH.pdf>. Acesso em 20 de julho de 2022.

12 SPARKS, Richard; GACEK, James. Persistent puzzles: The philosophy and ethics of private corrections in the context of contemporary penalty. Criminology & Public Policy, v. 18, n. 2, p. 379-399, 2019.



2. HACKING GOVERNAMENTAL: conceito e breve balanço do debate global

2.1 Definição



O conjunto global de tecnologias forenses instrumentalizadas em investigações é significativamente amplo para caber dentro de uma mesma “caixa” terminológica. Reduzindo o escopo apenas para o que consideramos hacking governamental, ainda é preciso fazer recortes conceituais, ou seja “o que” e “por que” dada técnica seria considerada “hacking”, bem como justificar por que se considerariam “governamentais”.

Para fins deste estudo, o que será considerado hacking diz respeito dois atributos: primeiro, do ponto de vista técnico, a exploração de uma vulnerabilidade, seja ela intencional ou não, conhecida ou não, pelo fabricante, que resulte no acesso não-autorizado a uma informação, seja comunicação ou dados em repouso ou em trânsito; em segundo lugar, do ponto de vista comportamental, essa exploração envolve intencionalidade, ou seja, o propósito de alcançar aquela informação por meio do desvio do que seria um sistema de segurança. Adicionalmente, optamos por usar a terminologia “governamental” por duas razões. Certos autores denominam o campo dessas atividades como “lawful hacking”¹³ (“hacking legal”) ou mesmo “law enforcement hacking”¹⁴ (“hacking investigativo”). No entanto, uma vez que não delimitamos bases que confirmam legalidade evidente à prática no Brasil e que, do ponto de vista político, ferramentas dessa natureza vêm sendo associadas à atividades de perseguição a dissidentes políticos, denominar a prática de “legal” demanda um amadurecimento legislativo muito mais avançado. Depois, como forma de ressoar boa parte da literatura internacional que opta por “government hacking”,¹⁵ a adoção do termo também busca um alinhamento com o debate global para significar a agência de entidades pertencentes ao corpo estatal.¹⁶

13 BELLOVIN, Steven et al. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. 12 Northwestern Journal of Technology & Intellectual Property 1, 2014. Disponível em <https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/>. Acesso em 20 de julho de 2022; HENNESSEY, Susan. Lawful hacking and the case for a strategic approach to Going Dark, Brookings, 2016. Disponível em <https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/>. Acesso em 22 de julho de 2022.

14 QUINLAN, Sayako; WILSON, Andi. A brief history of law enforcement hacking in the United States. New America, Cybersecurity Initiative, 2016. Disponível em https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf. Acesso em 22 de julho de 2022.

15 HERPIG, Sven. A Framework for Government Hacking in Criminal Investigations. Stiftung Neue verantwortung, 2018. Disponível em https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf; PFEFFERKORN, Riana. Security Risks of Government Hacking. Center for Internet and Society, Stanford, 2018. Disponível em <http://cyberlaw.stanford.edu/publications/security-risks-government-hacking>; MAYER, Jonathan. Government Hacking . Yale Law Journal, Vol 127, nº 3, 2018. Disponível em <https://www.yalelawjournal.org/article/government-hacking>. STEPANOVITCH, et al. A human rights response to government hacking. Access Now, 2016. Disponível em <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>. Internet Society. Government hacking: What is it and when should it be used? 2020. Disponível em <https://www.internetsociety.org/wp-content/uploads/2020/05/Government-Hacking-Fact-Sheet.pdf>. Todos acessados em 22 de julho de 2022

16 A título de comentário, também caberia definir a atividade como “hacking estatal”. O Estado moderno pode ser concebido enquanto uma instituição que possui papel de coordenar atividades sociais, além de ter aparelhos de poder públicos exclusivos, incluindo políticos, militares e polícias. Em versão moderna, separa-se o Estado do governante que ocupa a cadeira deliberativa, mantendo o monopólio do uso legítimo da força no território que administra. O Governo, por sua vez, é sobretudo o grupo político que está comandando um Estado. As forças de segurança relacionam-se mais fortemente com o conceito de Estado que de governo, ainda



Optamos por abranger, quanto hacking governamental, duas subcategorias: i) o acesso a dados e comunicações a partir do controle físico do aparelho (por exemplo, um celular apreendido), possibilitando a extração em massa de dados do dispositivo. Esse cenário poderia envolver tanto a quebra de criptografia em aplicações e em discos de armazenamento, ou mesmo o desvio a outros sistemas de segurança, como senhas alfanuméricas, padrões ou autenticação mediante biometria para desbloqueio do dispositivo ou acesso a aplicações; e ii) o acesso remoto a dispositivos, normalmente a partir da exploração de uma vulnerabilidade ainda não conhecida pelo fabricante do sistema vulnerável e que permita o acesso total ou parcial ao aparelho. Para este último caso, também incluímos o uso de ferramentas para interceptação direta do tráfego de informações em redes móveis a partir de uma relativa proximidade do dispositivo alvo.¹⁷

A partir dessas duas chaves de classificação também seria possível determinar o grau de risco de uma determinada ferramenta, uma vez que o acesso remoto permite um potencial de vigilância e interferência sobre a autenticidade das provas consideravelmente mais amplos. São categorias que deverão ser observadas de perto por iniciativas regulatórias que busquem delimitar permissões, restrições e procedimentos relativos à contratação ou mesmo à fabricação doméstica de ferramentas para fins de hacking governamental.

2.2. Escalabilidade e crescente protagonismo das ferramentas de hacking



A prática de explorar vulnerabilidades em sistemas informáticos carrega, fundamentalmente, uma ambivalência: tanto pode ser explorada por agentes privados mal intencionados, constituído crime tipificado em ordenamentos jurídicos, quanto pode ser “legitimamente” utilizada por autoridades policiais como forma de produzir provas em investigações criminais ou para fins de atividades de inteligência. Partindo da segunda categoria, o hacking governamental constitui rotina de agências governamentais e vem sendo enquadrada como “modernização” tecnológica do aparato das “forças da lei”.¹⁸

À primeira vista, a sofisticação do cometimento de crimes, bem como o ocultamento de provas sob robustos sistema de segurança da informação - incorporados por padrão, em grande medida, ao mercado de tecnologias - seria motivação suficiente para que fossem adotadas ferramentas que superassem tais barreiras, tornando eficaz a atividade de segurança pública. No entanto, o investimento contínuo - em termos econômicos e políticos - em formas de superar recursos de segurança gera uma cultura de busca e preservação de vulnerabilidades em sistemas conectados que tem entre suas consequências ora o desvio de finalidade e/ou o uso sem necessidade comprovada por parte de agentes governamentais, ora incidentes de segurança que têm como consequência o vazamento de ferramentas e informações que que, por vezes, tais aparelhos estatais sejam instrumentalizados por governos específicos a fim de seguirem suas diretrizes e interesses políticos. Dessa forma, seria possível argumentar que o uso de ferramentas hacking por partes de forças de segurança, pela qual o Estado tem como desempenha sua força, poderia ser caracterizado como “hacking estatal”. Ver BRESSER-PEREIRA, Luiz Carlos. Estado, Estado-Nação e formas de intermediação política. *Lua Nova: Revista de Cultura e Política*, São Paulo, p. 155-185, 2017; WEBER, Max. A política como vocação. In: WEBER, Max. *Ensaios de Sociologia*. Rio de Janeiro: LTC, 1982, p.97-153; e ROCHA, Manoel Ilson Cordeiro. Estado e governo: diferença conceitual e implicações práticas na pós-modernidade. *Revista Brasileira Multidisciplinar*, Araraquara, v. 11, n. 2, p. 140-145, 2008.

17 Para fins desta pesquisa, consideramos hacking tanto técnicas de extração de dados mediante superação de sistemas de segurança quanto técnicas de acesso remoto a dados e comunicações pessoais, sobretudo a partir da chave da intencionalidade do agente que opera a ferramenta e, também, em função de uma didática que propõe a pesquisa para fomento ao debate público. Uma moldura regulatória, no entanto, deverá buscar qualificações sobre a natureza das ferramentas a partir da gama de potencialidades e riscos que oferecem.

18 POLÍCIA CIENTÍFICA DE SANTA CATARINA. IGP inicia entrega dos equipamentos israelenses Cellebrite. 2021. Disponível em <https://www.policiacientifica.sc.gov.br/noticias/igp-inicia-entrega-dos-equipamentos-israelenses-cellebrite/>. Acesso em 20 de julho de 2022.



são aproveitadas por atores maliciosos.¹⁹

Mas mais recentemente, o uso do Pegasus,²⁰ spyware²¹ desenvolvido pela empresa israelense NGO Group, tornou-se mundialmente notório por ter como alvo jornalistas e defensores dos direitos humanos. Ainda em 2016, denúncia do Citizen Lab expôs que houve tentativa de infectar o iPhone de Ahmed Mansoor, conhecido defensor dos direitos humanos, com o spyware. Evidências indicam que o governo dos Emirados Árabes estava por trás do ataque, bem como de outros tendo como alvo o ativista.²² Em 2017, investigação da mesma entidade expôs cientistas mexicanos envolvidos com campanha de saúde pública anti-obesidade e para a taxação de refrigerantes no país também foram alvos de tentativas de infecção de seus celulares pelo Pegasus.²³ Em 2018, foi revelado que pelo menos 45 países apresentavam registro de operações com o Pegasus, incluindo países com amplo histórico de perseguir a sociedade civil.²⁴ E em 2021, a rede de jornalistas Forbidden Stories denunciou que pelo menos 180 jornalistas em variadas partes do mundo foram alvos em potencial do mesmo spyware, para citar apenas alguns casos.²⁵

No Brasil, também registram-se consecutivos sinais e tentativas de se adquirir o Pegasus:

- Foi reportado que, em 2018, durante evento do encontro Sistema Nacional de Prevenção e Repressão a Entorpecentes, com entusiasmo foi anunciado por um delegado da Polícia Federal que o spyware havia sido oferecido para a entidade por 2.7 milhões de reais;²⁶
- Também em 2018, relatório do Citizen Lab encontrou suspeitas de que havia sinal de dispositivo infectado com o programa no país desde 2017;²⁷
- Em 2021, a defesa de Luís Inácio Lula da Silva denunciou que o Ministério Público Federal haveria negociado a aquisição do Pegasus no âmbito da operação Lava-Jato;
- E, no mesmo ano, Carlos Bolsonaro teria tentado intervir em licitação do Ministério da Justiça (MJ) para adquirir o Pegasus como forma de municiar um aparato de inteligência paralelo à Agência Brasileira de Inteligência (ABIn), sob a alcada do MJ.²⁸ No entanto, até o momento, não há documentação que ateste registros públicos de contratação da ferramenta por agências de investigação ou inteligência brasileiras.

19 Ver, por exemplo, LARSON, Quincy. The CIA just lost control of its hacking arsenal. Here's what you need to know. FreeCodeCamp, 2017. Disponível em <https://www.freecodecamp.org/news/the-cia-just-lost-control-of-its-hacking-arsenal-heres-what-you-need-to-know-ea69fc1ce38c/>. Acesso em 20 de julho de 2022.

20 PEGG, David; CUTLER, Sam. What is Pegasus spyware and how does it hack phones? The Guardian, 2021. Disponível em <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>. Acesso em 21 de julho de 2022.

21 Em linhas gerais, definido como um software malicioso construído para invadir um computador, móvel ou não, pessoal ou não, com o objetivo de coletar dados e enviar a uma parte terceira sem o consentimento do titular dos dados. Ver, por exemplo, KASPERSKY. What is a spyware. 2022. Disponível em <https://www.kaspersky.com/resource-center/threats/spyware>. Acesso em 21 de julho de 2022.

22 MARCZAK, Bill; SCOTT-RAILTON, Johan. The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Citizen Lab, 2016. <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nsogroup-uae/>. Acesso em 20 de julho de 2022.

23 HAILTON-SCOTT, John et al. Bitter Sweet Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links. Citizen Lab, 2017. Disponível em <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>. Acesso em 22 de julho de 2022.

24 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 22 de julho de 2022.

25 RUECKERT, Phineas. Pegasus: the new global weapon for silencing journalists. Forbidden Stories, 2021. Disponível em <https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/>. Acesso em 22 de julho de 2022.

26 ABBUD, Bruno. A chegada ao Brasil do Pegasus, estrela do submundo da espionagem. O Globo, 2019. Disponível em <https://oglobo.globo.com/epoca/brasil/a-chegada-ao-brasil-do-pegasus-estrela-do-submundo-da-espionagem-23815778>. Acesso em 22 de julho de 2022.

27 MARCZAK, Bill et al. Op. cit.

28 VALENÇA, Lucas. Carlos Bolsonaro intervém em compra de aparelho espião e cria crise militar. UOL Notícias, 2021. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-organos-de-inteligencia.htm>. Acesso em 22 de julho de 2022.



No campo das ferramentas de extração em massa de dados de celulares, também são registrados, de forma ainda mais marcante, altos níveis de escalabilidade que tornam cotidiano o uso de técnicas de hacking por forças policiais. Normalmente chamados de MDFTs (mobile device forensic tools), são conjuntos de hardware e software utilizados em dispositivos móveis em custódia das forças policiais para desbloqueá-los e extrair dados, através de conexão física, que alcançam serviços de e-mail, armazenamento em nuvem, dados de redes sociais, histórico de localização (GPS), comunicações privadas, fotos, vídeos e, basicamente, o que mais estiver armazenado e acessível em aparelhos de celular pessoais, incluindo dados deletados pelo usuário. Sobre o conjunto de dados coletados, não é incomum ver soluções de inteligência artificial aplicadas adicionalmente, como forma de identificar padrões.²⁹

Ainda que sugira usos mais pontuais em determinados dispositivos - aqueles apreendidos - permitem uma coleta desproporcional em relação à finalidade: sob uma lógica de acúmulo de informações, uma autoridade investigativa teria acesso a um leque de dados pessoais muito maior do que o necessário para conduzir uma investigação e produzir evidências. A amplitude da coleta de dados - inclusive de pessoas próximas que simplesmente se comuniquem e interajam com os investigados, sem qualquer relação com o interesse investigativo - colocam um grau de intrusividade, violação da privacidade e suspensão do direito ao sigilo como jamais antes expedientes, por exemplo, de interceptação telefônica ou busca e apreensão em domicílios poderiam oferecer.

No cenário internacional, não somente agências de investigação federais adquiriram MDFTs ou essas são usadas na investigação de crimes graves, como se poderia supor. Nos Estados Unidos, foi constatado que todas as agências de investigação de nível estadual, bem como as 50 maiores agências de investigação locais, além de todas as repartições do Federal Bureau of Investigation (FBI) as possuem. Seus usos estão relacionados a infrações de menor potencial ofensivo ou mesmo sem nenhuma relação clara com o uso de celulares, como pixação, prostituição e batidas de carro, o que significam que são usadas como uma "ferramenta para propósito geral".³⁰

A recepção de tecnologias de extração de dados em expedientes investigativos no Brasil já é noticiada há quase dez anos.³¹ No contexto de grandes eventos ocorridos no Brasil, como a Copa do Mundo de 2014, por exemplo, já era relatado o [treinamento de oficiais brasileiros](#) para o uso de tecnologias da Cellebrite.³² No entanto, os últimos anos foram marcados por sucessivas notícias que enquadram ferramentas do gênero por um ângulo tecno-otimista ou tecno-solucionista,³³ como nos casos do assassinato de Henry Borel ou em grandes operações de combate ao crime organizado, como na Operação Enterpise³⁴ e a Lava-Jato.³⁵

Além disso, as recentes estratégias institucionais do sistema investigativo brasileiro vêm revelando um planejamento verdadeiramente ilustrativo do nível de entrada das ferramentas de extração de dados no país. A esse respeito, o The Intercept Brasil detalhou alguns termos do Programa Excel, política

29 https://cellebrite.com/wp-content/uploads/2020/08/ProductOverview_Cellebrite_Pathfinder.pdf

30 KOEPKE, Logan et. al. Mass Extraction The Widespread Power of U.S. Law Enforcement to Search Mobile Phones. Upturn, 2020. Disponível em <https://www.upturn.org/work/mass-extraction/> Acesso em 22 de julho de 2022.

31 Um levantamento detalhado sobre a capilaridade atual de ferramentas de hacking, incluindo MDFTs, na estrutura investigativa da administração pública brasileira é apresentado no Capítulo 3.

32 VIANA, Natalia. Estados Unidos treinaram policiais brasileiros para conter manifestações na Copa do Mundo. Opera Mundi, 2014. Disponível em <https://operamundi.uol.com.br/politica-e-economia/35641/estados-unidos-treinaram-policiais-brasileiros-para-conter-manifestacoes-na-copa-do-mundo#:~:text=Desde%202012%2C%20o%20governo%20americano,Academi%2C%20novo%20nome%20da%20empresa>. Acesso em 22 de maio de 2022.

33 Ref com quote de elogio exacerbado

34 JAFFE, Adam. Milhões em bens apreendidos à medida que a Polícia Federal do Brasil se dedica a desmascarar chefes do tráfico de drogas. Cellebrite, 2021. Disponível em <https://cellebrite.com/pt/milhoes-em-bens-apreendidos-a-medida-que-a-policia-federal-do-brasil-se-dedica-a-desmascarar-chefes-do-trafico-de-drogas/>. Acesso em 22 de maio de 2022.

35 BIT MAGAZINE. Polícia Federal adota Cellebrite para investigação da Lava Jato. Bit Magazine, 2015. Disponível em <https://www.bitmag.com.br/policia-federal-adota-cellebrite-para-investigacao-da-lava-jato/>. Acesso em 22 de maio de 2022.

criada no âmbito do Ministério da Justiça que propõe o seguinte arranjo: o Ministério provê às forças policiais estatais MDFTs da Cellebrite (que, em sua maioria, podem variar entre 100 ou 200 mil reais) e, como contrapartida, as polícias alimentariam uma base dados do Ministério composta pelos dados extraídos dos celulares.³⁶ Ou seja, para além de uma finalidade investigativa pontual e demarcada por ordem judicial, dados pessoais são acumulados pela máquina pública com o fundamental auxílio das MDFTs, uma lógica que aprofunda o sistema de vigilância estatal e permite usos colaterais dos dados pessoais.

Em outras palavras, de dados um elemento verdadeiramente fiador das capacidades tecnológicas de investigação, inclusive no Brasil.³⁷ Isso não somente apresenta riscos do ponto de vista da transparência e auditabilidade das ferramentas, muitas vezes protegidas por segredo industrial, como também massifica seu uso, tendo como consequência a perda de sua natureza de excepcionalidade - ou de ser um expediente de ultima ratio - facilitando uso indiscriminado por agências governamentais e seu acesso por atores privados, abrindo margem a amplos riscos aos direitos humanos.

Isso se agrava quando seu uso se aproxima, cada vez, mais de usos diretamente ligados à perseguições políticas em variadas partes do mundo: uma série de levantamentos confirmam, por exemplo, que o uso de MDFTs da Cellebrite foi identificado para incriminar jornalistas da Reuters e do Botswana People's Daily News, além de um ativista pró-democracia em Hong Kong; a Cellebrite também vendeu aparelhos e treinou agentes ligados a "esquadrões da morte" em Bangladesh, para citar apenas alguns casos.³⁸ E quando, em 2021, a Cellebrite anunciou suas intenções de abrir seu capital, a empresa reconheceu, entre os "riscos-chave", que alguns dos seus produtos podem ser percebidos, pelas cortes de justiça, como uma violação à privacidade e às leis relacionadas. Também atestam que certos produtos poderiam ser utilizados por clientes de forma incompatível com os direitos humanos. Tal percepção poderia afetar negativamente sua reputação, lucro e resultados de suas operações.³⁹

Fica evidente, portanto, uma inevitável escalabilidade sobre o uso de tais ferramentas, que naturalmente passam da excepcionalidade e restrição para o uso corriqueiro por parte dos agentes estatais. Sob a chave da "legitimidade", a exploração de vulnerabilidades se torna prática corriqueira, facilitada por um mercado crescente de fabricação e fornecimento de ferramentas de vigilância e, invariavelmente, caem nas mãos de atores indesejados. Para Bruce Schneier "uma capacidade militar ultra-secreta de ontem se torna, hoje, uma tese de doutorado e, amanhã, uma ferramenta de hacking".⁴⁰

O estágio de regulação e de estabelecimento de estritos procedimentos no Brasil é incipiente, o que permite a massificação do uso e a consolidação de uma cultura investigativa de risco ao ecossistema de segurança e de direitos fundamentais. O cenário, portanto, tem o condão de colocar o país na retaguarda das regulações guiadas pelos princípios da privacidade, proteção de dados e das políticas nacionais de cibersegurança quando se tratando do hacking governamental.

36 AMENO, Fernando. As planilhas de bolsonaro: Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados. Disponível em <https://theintercept.com/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/>. Acesso em 26 de maio de 2022.

37 Segundo release da Sun Corporation - empresa-irmã da Cellebrite, líder global do mercado - MDFTs da Cellebrite estão presentes em mais 60.000 agências de investigação, cobrindo mais de 150 países. SUN CORPORATION. Overseas bases. Sun Corporation 2022. Disponível em <https://www.sun-denshi.co.jp/company/abroad/>. Acesso em 22 de maio de 2022.

38 KRAPIVA, Natalia; SUGIYAMA, Hinako. What spy firm Cellebrite can't hide from investors. Access Now, 2021. Disponível em <https://www.accessnow.org/what-spy-firm-cellebrite-can't-hide-from-investors/>. Acesso em 22 de maio de 2022.

39 CELLEBRITE. Investor Presentation. Cellebrite, 2021. Disponível em <https://sec.report/Document/0001213900-21-020888/>. Acesso em 22 de maio de 2022.

40 SCHNEIER, Bruce. Click here to kill everybody: security and survival in a hyperconnected world. New York: W. W. Norton & Company, 2018. Seria possível ainda continuar as possíveis consequências, como a presença de ferramentas de hacking para fácil aquisição no eBay. Ver https://br.ebay.com/b/Cellebrite-Cell-Phone-Accessories/9394/bn_77061199.



2.3. DESVIOS À CRIPTOGRAFIA: a ofensiva policial enquanto atalho aos pedidos de acesso às comunicações privadas

Ferramentas de hacking governamental normalmente compartilham uma transversal em comum: são impulsionadas como possível alternativa que viabilize desvios à criptografia⁴¹ e, portanto, acesso a dados protegidos por sistemas de segurança. A narrativa do obscurecimento das forças de investigação,⁴² ou seja, a suposta dificuldade técnica em obter dados protegidos por criptografia, atraiu a consideração de possíveis soluções de acesso ofensivo direto aos dispositivos. Uma abordagem estratégica que demandaria novos procedimentos administrativos e previsões regulatórias.⁴³

Nessa esteira, o enfrentamento político às técnicas de criptografia tem sido palco de amplos debates judiciais, especialmente no Brasil, sobre a legalidade de aplicações usarem protocolos de criptografia que impeçam o cumprimento de ordens judiciais. Sendo assim, essa conjuntura tem sido combustível para a adoção de técnicas de hacking.

2.3.1. A criptografia vai ao STF: bloqueios ao WhatsApp e o Tratado de Assistência Legal Mútua (MLAT)

Do ponto da prática investigativa, o conjunto normativo brasileiro referente à requisição e acesso a dados pessoais fundamentalmente envolve, pelo menos, dois desafios: um de natureza técnica e outro de natureza jurisdicional, tendo a criptografia como um dos centros gravitacionais no cenário político brasileiro. Como resultado, o Supremo Tribunal Federal tem sido palco, nos últimos anos, de debates paradigmáticos sobre a legalidade da interpretação da criptografia ponta-a-ponta e, consequentemente, sobre a necessidade de requisição internacional de acesso à dados para fins de investigações, envolvendo outras jurisdições.

Entre 2015 e 2016, a aplicação WhatsApp foi alvo de quatro ordens judiciais que determinavam seu bloqueio em território nacional, das quais três foram efetivamente cumpridas, tendo todas elas sido revertidas em instâncias superiores.⁴⁴ Em linhas gerais, as ordens judiciais determinavam medidas concretivas em detrimento da impossibilidade técnica - entendida pelo juízo como mera "negativa" - da plataforma ceder a representações investigativas o conteúdo de conversas privadas em função da criptografia de ponta-a-ponta utilizada pelo serviço. Entre as interpretações legais levadas à frente pelos juízos que determinaram os bloqueios, estaria a leitura de que o Art. 12, inciso III, do Marco Civil da Internet permitiria o bloqueio de aplicações em face do descumprimento de ordens judiciais. Como resultado, duas ações diretas de controle de constitucionalidade foram propostas perante o Supremo Tribunal Federal: a Ação Direta de Inconstitucionalidade (ADI) nº 5.527 e a Ação de Descumprimento de Preceito Fundamental (ADPF) nº 403. Após a realização de Audiência Pública para oitiva setores de interesse e dos votos preliminares dos Ministros Edson Fachin e Rosa Weber lançando luz sobre a importância da criptografia para conjuntos de direitos fundamentais e, consequentemente, contra a possibilidade de

41 KERR, Orin S, SCHNEIER, Bruce. Encryption Workarounds. Georgetown Law Journal, 2017. Disponível em <https://ssrn.com>.

42 COMEY, James. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Brookings Institution, 2014. Disponível em <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.

43 HENNESSEY, Susan. Lawful hacking and the case for a strategic approach to Going Dark, Brookings, 2016. Disponível em <https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/>. Acesso em 22 de ju-

44 Ver BLOQUEIOS.INFO. InternetLab e Instituto de Referência em Internet e Sociedade (IRIS). Disponível em <http://bloqueios.info>.

bloqueio da plataforma,⁴⁵ as ações seguem inconclusas até a data de publicação deste estudo.

O aspecto jurisdicional se assenta sobre instrumentos de assistência mútua entre agências investigativas de países distintos, notadamente os MLATs (Mutual Legal Assistance Treaties), acordos de cooperação motivados pela necessidade de produção de provas que estejam inacessíveis no âmbito doméstico de um dado país. Alguns elementos, inicialmente, são postos nesta seara como peças que interagem entre si e colocam os MLATs como pontos de tensão: o aumento da dependência de agências de investigação sobre dados armazenados em servidores localizados outros países, portanto em outras jurisdições; a natureza vagarosa e burocrática notadamente percebido na ativação de um procedimento administrativo internacional desta espécie, podendo afetar a eficiência de um processo penal; e a mínima relação de confiança entre provedores de serviços multinacionais e usuários na guarda e proteção de dados pessoais, estabelecendo barreiras procedimentais quanto à cessão de dados ao Estado.⁴⁶ O tema também é objeto de ação perante o STF, a Ação de Declaração de Constitucionalidade (ADC) nº 51, a qual requer determinação, entre outros pedidos, de que o Decreto nº 3810/2001 (que estabelece o MLAT em matéria penal no Brasil) é constitucional e, portanto é aplicável ao fluxo de requisição de dados armazenados em outras jurisdições.

Arguimos, portanto, que esses fatores têm sido motivadores conjunturais que deságiam na adoção de novas técnicas que simplificam o acesso a dados e comunicações - associados a um mercado de ferramentas forenses em expansão e esquivos à regulação. Note-se, ao mesmo tempo, que não concluímos que esses fatores justificam a expansão de expedientes de hacking governamental, mas que compõem um pano de fundo de ordem tecnológica, política e jurisdicional.

2.3.2. Cortando o intermediário: o acesso a dados de forma direta

O movimento de bypass dos intermediários, como os provedores de aplicações, por meio de técnicas de extração e acesso remoto a dispositivos pessoais, vem cortando os intermediários e os procedimentos burocráticos investigativos tradicionais. Como resultado, a cooperação dos intermediários passa a ser um elemento excluído, cada vez mais, da equação que resulta no acesso a dados e comunicações pessoais.

No debate global, autores sustentam que a exploração de vulnerabilidades seria um caminho “meio-termo”⁴⁷ entre os pólos opostos que seriam inserir portas clandestinas⁴⁸ (backdoors) em sistemas de criptografia e, de outro lado, não prover qualquer meio de acesso a dados em investigações. Argumentos consideram que o hacking governamental seria uma alternativa viável em relação à restrição de criptografia,⁴⁹ explorando gargalos de segurança que já existem⁵⁰ e provendo, portanto, uma vigilância

45 SUPREMO TRIBUNAL FEDERAL. Relatora entende que aplicativos de mensagens não podem ser obrigados a fornecer dados criptografados. 2020. Disponível em <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444265&ori=1>. Acesso em 22 julho de 2022.

46 ABREU, Jacqueline de Souza. Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience. Revista de Informação Legislativa: RIL, v. 55, n. 220, 2018. Disponível em https://www12.senado.leg.br/ril/edicoes/55/220/ril_v55_n220_p233. Acesso em 20 de julho de 2022.

47 HOAITHI, Nguyen. Lawful hacking; toward a middle-ground solution to the going dark problem. Naval Postgraduate School, 2017.

48 RENÁ, Paulo. “Portas clandestinas: uma tradução mais precisa para debatermos backdoors em criptografia”. Instituto de Referência em Internet e Sociedade (2022). Disponível em <https://irisbh.com.br/portas-clandestinas-uma-traducao-mais-precisa-para-debatermos-backdoors-em-criptografia/>. Acesso em 20 de julho de 2022.

49 LIGUORI, Carlos. Exploring Lawful Hacking as a Possible Answer to the “Going Dark” Debate. Michigan Technology Law Review (2020). Disponível em <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1019&context=mtlr>. Acesso em 20 de julho de 2022.

50 BELLOVIN, Steven et al. Op. cit.

“sob medida” em detrimento de programas de vigilância em massa.⁵¹ Afinal, argumentam, vulnerabilidades não previstas pelos provedores sempre existirão e seriam preferíveis em detrimento da inserção intencional de brechas de segurança em serviços de Internet.⁵²

Em contrapartida, uma nova abordagem de avaliação de risco é necessária, para além da esfera da criptografia⁵³ em serviços de mensageria instantânea. Não somente a naturalização sobre o uso de técnicas de hacking colocam novos riscos estruturais, sobretudo se considerarmos que não só comunicações encriptadas são alvo de acesso, mas uma infinidade de dados pessoais - de dados pessoais sensíveis a metadados - produzidos em dezenas de serviços, por cada usuário, e armazenados em dispositivos pessoais, mas também o acesso direto por parte de entidades governamentais aos dados e comunicações, mediante a exclusão de controladores dos dados, rompe uma mediação de confiança entre usuários e provedores.

O rompimento da cadeia de confiança entre usuário e provedor causado pelo acesso direto tem o condão, em primeiro lugar, de esvaziar o conteúdo de contratos privados, como políticas de privacidade que norteiam o procedimento de acesso a dados por entidades governamentais - sobre as quais usuários se ancoram, inclusive, na escolha de serviços⁵⁴ e cujos termos são objeto de pesquisa e escrutínio social.⁵⁵ Se entendemos, como propõe Ari Ezra Waldman,⁵⁶ a privacidade como propriedade de controle da informação inerente das interações sociais e, portanto, central para o estabelecimento da confiança nas relações rotineiras, é necessário reconhecer os potenciais de insegurança e instabilidade do uso e abuso da exploração de vulnerabilidades pode trazer para as sociedades e economias crescentemente digitalizadas.

Em segundo lugar, causa retrocessos quanto a políticas públicas que vêm sendo paulatinamente consolidadas mundialmente e que avançam no estabelecimento de regimes de privacidade, sigilo das comunicações e na proteção de dados pessoais - regimes que envolvem, fundamentalmente, a responsabilidade dos atores privados, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, no Brasil, bem como às leis de proteção de dados pessoais regionais e domésticas no âmbito internacional. O acesso direto, mediante afastamento dos provedores de aplicação, inaugura um novo caminho de devi- do processo legal sem regulação específica, ignorando, por exemplo, as diretrizes de legalidade do MCI.

Colateralmente, a exploração de vulnerabilidades em serviços tecnológicos envolve uma “postura ofensiva” dos atores que fornecem tais ferramentas às entidades governamentais. Como resultado, empresas cujos sistemas de segurança foram comprometidos por ataques moveram ações judiciais contra fornecedores de serviços de hacking: em 2019, o então Facebook entrou com ação judicial contra a NSO Group, sob a alegação de que esta teria invadido o servidor do WhatsApp para infectar com seu spyware 1.400 usuários;⁵⁷ em 2021, a Apple também entrou com ação judicial contra a mesma empresa por esta ter

51 PFEFFERKORN, Riana. Democracy, narratives dispute, and security conflicts in encryption policies. [Entrevista concedida a] André Ramiro. Instituto de Pesquisa em Direito e Tecnologia do Recife, 2020. Disponível em https://ip.rec.br/wp-content/uploads/2020/10/Democracy-narrative-disputes-and-security-conflicts-in-encryption-policies-Interview-with-Riana-Pfefferkorn-IPrec_.pdf. Acesso em 28 de maio de 2022.

52 BELLOVIN, Steven et al. Op. cit.

53 HERPING, Syen. Government Hacking: Computer Security vs. Investigative Powers. Stiftung Neue Verantwortung, 2017. Disponível em https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking_problem_analysis_0.pdf. Acesso em 20 de julho de 2022.

54 FORBES INSIDER. App de mensagens Signal vê crescimento meteórico em instalações. 2021. Disponível em <https://forbes.com.br/forbes-tech/2021/01/app-de-mensagens-signal-ve-crescimento-meteorico-em-instalacoes-apos-anuncio-do-whatsapp/>. Acesso em 20 de julho de 2022.

55 Instituto de Defesa do Consumidor (IDEC). Caso WhatsApp: proteção de dados dos usuários permanece ameaçada. 202. Disponível em <https://idec.org.br/noticia/caso-whatsapp-protecao-de-dados-dos-usuarios-permanece-ameacada>. Acesso em 20 de julho de 2022.

56 WALDMAN, Ari Ezra. Privacy as trust: Information privacy for an information age. Cambridge University Press, 2018.

57 BUSINESS & HUMAN RIGHTS RESOURCE CENTER. NSO Group lawsuit (re hacking WhatsApp users). Disponível em <https://www.business-humanrights.org/en/latest-news/ns0-group-lawsuit-re-hacking-whatsapp-users/>. Acesso em 14 de julho de 2022.



explorado continuamente vulnerabilidades em seus produtos. Em ambos os casos, as autoras das ações denunciam que os alvos dos ataques incluem ativistas, dissidentes políticos e jornalistas.⁵⁸

Sendo assim, antes mesmo de oferecerem um potencial de vigilância supostamente reduzido, essas técnicas redesenham os riscos estruturais à segurança e aos direitos fundamentais dos usuários ao excluir provedores de serviços da mediação quanto ao acesso a dados e comunicações privadas. Usuários, portanto, são postos em uma relação de ainda maior hipossuficiência dada a disparidade de meios de recursos de segurança face a aparatos ofensivos de intrusão de agentes governamentais.

2.4. Nutrindo o Mercado de Vulnerabilidades

Diante do objetivo de acessar um sistema ou dispositivo protegidos, entidades estatais normalmente operam sua própria busca por vulnerabilidades - custando em termos de pesquisa e desenvolvimento de ferramentas⁵⁹ - ou contratam de agentes econômicos privados soluções prontas para uso. Para esse último caso, mais próximo de países em desenvolvimento,⁶⁰ a genealogia econômica do mercado de ferramentas de hacking denuncia uma estrutura que pode alimentar a exposição de brechas de segurança a partir de sua capitalização, resultando em um desincentivo a reportar a fabricantes eventuais e necessárias atualizações e gerando competições comerciais no mercado de vulnerabilidades.

Essa genealogia, de antemão, propõe um conjunto de decisões políticas e econômicas que percorrem desde a descoberta de uma vulnerabilidade até uma possível aplicação para o desenvolvimento de ferramentas de hacking. Descoberta uma brecha de segurança, um indivíduo poderia (i) usar para uma finalidade pessoal, como feito por cibercriminosos para fabricar ferramentas que automatizam ataques e, assim, extorquir outros usuários; (ii) divulgar para o público, provocando uma corrida entre o fabricante, que deverá atualizar seu sistema, e potenciais atacantes; (iii) reportar para o fabricante diretamente, através de seu programa de bug bounty,⁶¹ o qual poderá atualizar seu sistema com o privilégio de ser o único conhecedor do problema; (iv) ou reportar para outros programas de bug bounty, normalmente intermediários que irão negociar a informação com outros mercados e governos.

Na imagem abaixo, propomos, a partir da revisão de literatura, entrevistas e da análise de fatos e eventos, uma visualização de fluxos possíveis a partir de uma eventual descoberta de vulnerabilidade e suas variadas destinações e consequências.

58 PEARLROTH, Nicole. Apple sues Israeli spyware maker, seeking to block its access to iPhones. New York Times, 2021. Disponível em <https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html>. Acesso em 22 de julho de 2022.

59 Também é comum que haja “bancos de vulnerabilidades” conhecidas, como a National Vulnerabilities Database (NVD), mantida pelo National Institute of Standards and Technology (NIST) dos Estados Unidos. Ver NATIONAL VULNERABILITIES DATABASE, National Institute of Standards and Technology (NIST), 2022. Disponível em <https://www.nist.gov/programs-projects/national-vulnerability-database-nvd>. Acesso em 11 de junho de 2022; ou do China National Vulnerabilities Database of Information Security, do governo chinês, já acusada de ser mantida com privilégios para interesses da inteligência chinesa, que poderia explorar as vulnerabilidades antes de serem publicadas. Ver CHINA NATIONAL VULNERABILITIES DATABASE OF INFORMATION SECURITY. National Computer Network Emergency Technology Coordination Center, 2022; e O’NEILL, Patrick. China’s national vulnerability database is merely a tool for its intelligence agencies. Cyberscoop, 2019. Disponíveis, respectivamente, em <http://www.cnvd.org.cn/> e <https://www.cyberscoop.com/china-national-vulnerability-database-mss-recorded-future/>. Acesso em 11 de junho de 2022. Como resultado, a partir de uma suspeição coletiva sobre a integridade das informações disponíveis sobre os bancos de dados administrados por entidades governamentais, foi criado o Open Source Vulnerability Database, mantido entre 2002 e 2016. Ver OPEN SOURCE VULNERABILITY DATABASE. Wikipedia, 2022. Disponível em https://en.wikipedia.org/wiki/Open_Source_Vulnerability_Database. Acesso em 11 de junho de 2022.

60 Segundo pesquisador especialista em inteligência e ameaças de cibersegurança, entrevistado para essa pesquisa, esse seria o caso de entidades governamentais do Brasil, que preferem “ferramentas prontas para uso” de fabricantes privados.

61 Programas de recompensa para reportar vulnerabilidades ainda não descobertas em troca de uma compensação monetária.



Descoberta/ciência sobre uma vulnerabilidade

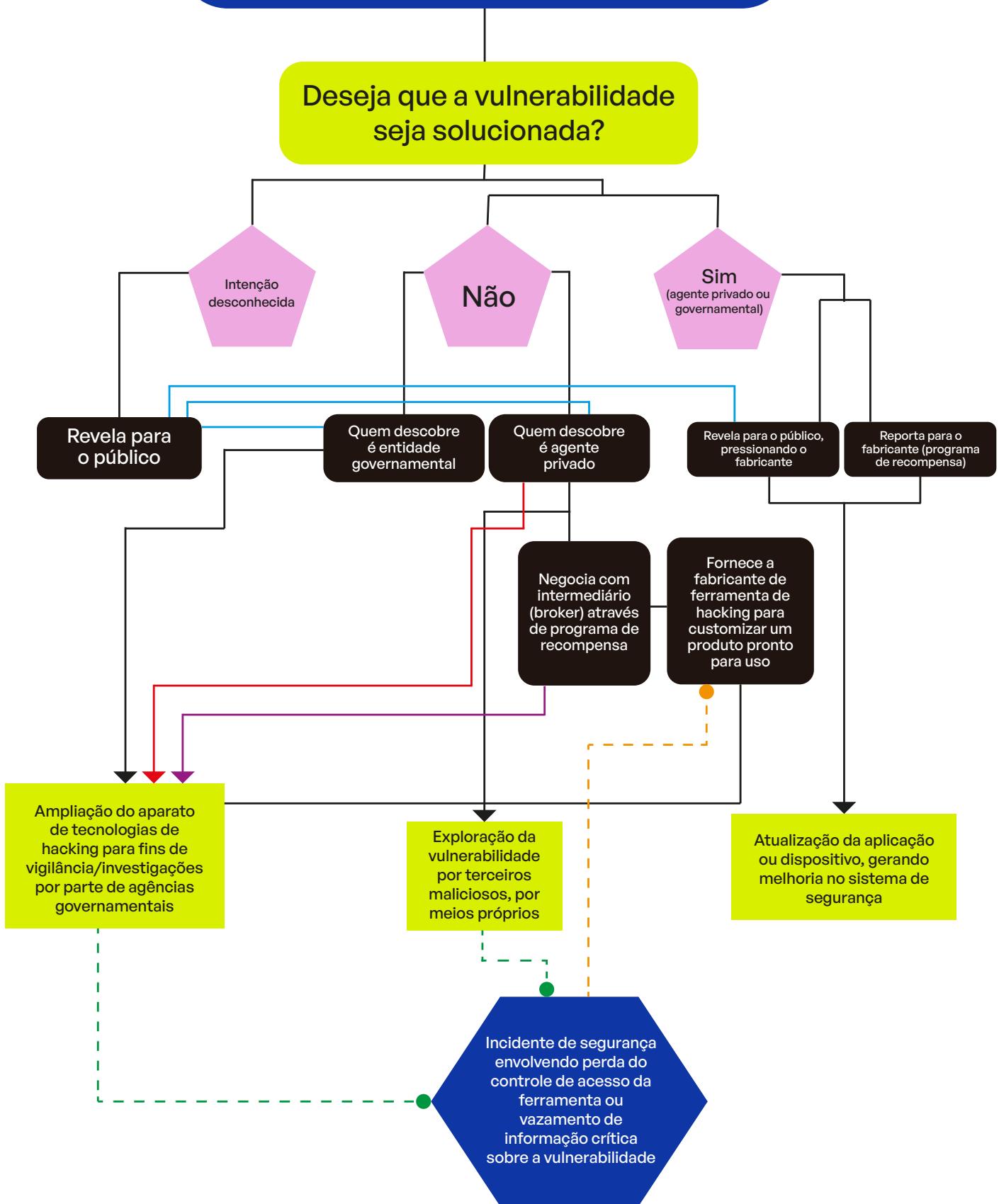


Gráfico 1: Esquema da descoberta, exploração e/ou publicização de vulnerabilidades.



A competição entre bug bounties, portanto, são relativamente comuns. Enquanto um fabricante como o Google paga, no máximo, U\$1.000.000 por informações que levem a uma vulnerabilidade zero-day⁶² no Android, competidores como a Zerodium poderiam pagar até U\$2.500.000.⁶³ Enquanto a Apple poderia pagar uma recompensa de U\$1.000.000 por uma vulnerabilidade em seu iOS, a Zerodium pagaria U\$2.000.000.⁶⁴ Ou seja, a partir de um modelo de negócio baseado na intermediação de inseguranças exploráveis por terceiros - como fabricantes de ferramentas de hacking, como Cellebrite, NSO Group, ou mesmo agências governamentais - intermediários como a Zerodium funcionam como brokers de informações que levem a uma vulnerabilidades.

O jornalista da Forbes e autor Andy Greenberg, ainda em 2012, ilustrou a dinâmica econômica sobre a não divulgação de uma vulnerabilidade diretamente ao fabricante. Em uma conferência de segurança, o Google promoveu uma competição para que pesquisadores encontrassem brechas de segurança em seu navegador Chrome. Quem encontrasse uma falha, poderia ser premiado com uma recompensa de U\$60.000 sob a condição de que instruísse o Google sobre os detalhes técnicos. Uma empresa chamada Vupen não somente encontrou uma falha, mas se negou a contar ao Google. Seu CEO disse que não revelariam a vulnerabilidade nem por um milhão de dólares: “nós não queremos fornecer nenhum conhecimento que os ajude a solucionar essa ou qualquer outra falha. Nós queremos mantê-las para nossos clientes”.⁶⁵ A Vupen, em 2015, irá renovar sua marca para se chamar Zerodium.⁶⁶

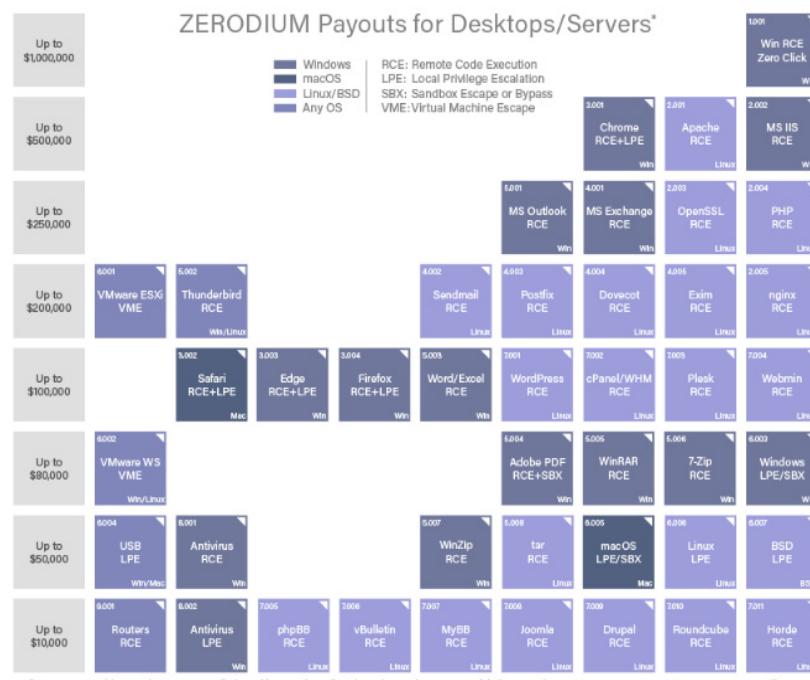


Tabela 1: Recompensas do programa de bug bounty da Zerodium.

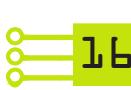
62 Vulnerabilidade crítica desconhecida pelo público ou pelo fabricante. Esse último teria, então, “zero dias” para corrigi-la antes de uma exploração.

63 Ver ZERODIUM. Zerodium Exploit Acquisition Program. 2022. Disponível em <https://zerodium.com/program.html>. Acesso em 20 de julho de 2022; SEALS, Tara. Google Offers \$1.5M Bug Bounty for Android 13 Beta. Darkreading, 2022. Disponível em <https://www.darkreading.com/vulnerabilities-threats/google-issues-1-5m-android-13-beta-bug-bounty>. Acesso em 20 de julho de 2022.

64 JEB, Su. Why Zerodium Will Pay \$2.5 Million For Anyone Who Can Hack Android But Only \$2 Million For An iPhone. Forbes, 2019. Disponível em <https://www.forbes.com/sites/jeanbaptiste/2019/09/04/why-zerodium-will-pay-2-5-million-for-anyone-who-can-hack-android-but-only-2-million-for-an-iphone/?sh=50c9b779716b>. Acesso em 12 de junho de 2022.

65 GREENBER, Andy. Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees). Forbes, 2012. Disponível em <https://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/?sh=4c49e8271f74>. Acesso em 12 de junho de 2021.

66 PEALROTH, Nicole. The Untold History of America’s Zero-Day Market. Wired, 2021. Disponível em <https://www.wired.com/story/untold-history-americas-zero-day-market/>. Acesso em 20 de julho de 2022.



Não seria difícil deduzir que uma das destinações do mercado de vulnerabilidades facilitado por esses brokers são grupos conhecidos por fabricar ferramentas de vigilância e espionagem e fornecê-las a regimes políticos opressores. Nesse sentido, é sintomático o caso da Netragard, empresa que também operava via programas de big bounty enquanto modelo de negócio: em 2015, a firma italiana Hacking Team foi alvo de um grande vazamento de dados, revelando que a empresa vendia ferramentas de vigilância a países com longo histórico de violação aos direitos humanos, como Sudão, Arábia Saudita, Cazaquistão e muitos outros, os quais tinham entre seus alvos jornalistas e dissidentes políticos.⁶⁷ Entre as documentações do vazamento, constava que a Netragard vendeu vulnerabilidades à Hacking Team por cerca de U\$100.000.⁶⁸ Devido a repercussão negativa, a Netragard encerrou seu programa de aquisição de vulnerabilidades.⁶⁹

Ryan Gallagher, então repórter do The Intercept, publicou a lista dos “top 5” clientes da Hacking Team, tendo a Polícia Federal brasileira no topo do ranking, seguida de agências governamentais do Cazaquistão e Etiópia.⁷⁰ Em outras palavras, a mercantilização internacional de vulnerabilidades alimenta diretamente o arsenal de agências de investigação brasileiras, tendo como pano de fundo o mesmo uso desses recursos contra a sociedade civil por atores internacionais. As forças da lei brasileiras se aproveitam diretamente do fomento mercadológico à insegurança do ecossistema conectado e podem estar comprando de fornecedores que alimentam, inclusive, facções de cibercrimes internacionais.

O cenário gera, portanto, uma leitura que sugere a commoditização⁷¹ das vulnerabilidades, disponíveis para compra pelo setor público ou privado, em franca expansão internacional. Consequentemente, o acúmulo desses recursos por Estados é visto como uma qualidade de defesa nacional ou segurança pública a partir dessa racionalidade. Ainda em 2013, Howard Schmidt, ex-coordenador de Cibersegurança da Casa Branca, comentava que governos estariam começando a pensar que “para tornar um país mais seguro, seria preciso encontrar vulnerabilidades sobre outros países”. Mas completa, “o problema é que todos nós nos tornamos fundamentalmente mais inseguros”⁷²

Portanto, a genealogia econômica das ferramentas exploração de vulnerabilidades, como as fornecidas pela Cellebrite, Hacking Team e de tantas outras com comprovadas relações comerciais com agências investigativas brasileiras, como demonstrado nos capítulos a seguir, sugerem um percurso de decisões políticas e éticas que capacitam técnicas estruturas forenses às custas da manutenção de brechas de segurança que são aproveitadas por uma diversidade de atores, privados e governamentais, legitimados e maliciosos. Então, apesar de forças investigativas operarem, em grande medida, em uma zona cinzenta de legalidade sobre a compra e uso desses recursos, coloca-se um dilema ético sobre a prevalência ou não do interesse público na exploração e fomento ativo de inseguranças em redes e dispositivos conectados.

67 ZETTER, Kim. Hacking Team leak shows how secretive zero-day exploits sales work. Wired, 2015. Disponível em <https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/>. Acesso em 22 de julho de 2022.

68 WEISSMAN, Cale Guthrie. One company thinks Hacking Team’s massive breach may bring about some good. Business Insider, 2015. Disponível em <https://www.businessinsider.com/hacking-team-vendor-netragard-apologizes-2015-7> Acesso em 22 de julho de 2022.

69 FISHER, Dennis. Netragard Shutters Controversial Exploit Acquisition Program. Threatpost. Disponível em: <https://threatpost.com/netragard-shutters-controversial-exploit-acquisition-program/113846/> Acesso em 22 de julho de 2022.

70 GALLAGHER, Ryan. Hacking Team’s “top five sales” for 2015 - w/ politically repressive regimes at #2 & #3 on the list. Disponível em https://twitter.com/rj_gallagher/status/618551248694943744/photo/1. Acesso em 22 de julho de 2022.

71 PEARLROTH, Nicole. Op. cit. 2021.

72 PEARLROTH, Nicole; SANGER, David E. Nations Buying as Hackers Sell Flaws in Computer Code. The New York Times, 2013. Disponível em <https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html>. Acesso em 30 de junho de 2022.



2.5. Vazamento de ferramentas, abusos e desvios de finalidade

Falar na possibilidade de um possível modelo de controle sobre o uso de ferramentas de hacking pelas entidades estatais é, também, estabelecer regras e protocolos de acesso a elas. Mesmo assim, sucessivos vazamentos de informações, perda de controle sobre tecnologias de alto potencial de danos à privacidade e à proteção de dados, bem como o desvio de finalidade compõem um histórico que sugere ser desafiador cumprir regras estritas de controle sobre o acesso. Um risco aparentemente inerente, portanto, é colocado.

Em 2017, por exemplo, o WikiLeaks iniciou uma série de denúncias que vieram a ficar conhecidas como “Vault 7”, revelando que a Central Intelligence Agency (CIA) havia perdido controle de grande parte de seu arsenal de ferramentas de hacking, incluindo diversos malwares como Trojans, programas de exploração de vulnerabilidades zero-days, programas de controle remoto sobre sistemas privados e outras tecnologias de vigilância. Os programas se aproveitavam de vulnerabilidades encontradas em aparelhos mundialmente utilizados por centenas de milhões de pessoas, incluindo iPhone, Android, Windows e mesmo televisões da Samsung.⁷³ Mais recentemente, um ex-funcionário da CIA foi condenado por ter vazado as informações.⁷⁴ As denúncias feitas por Edward Snowden em 2013, baseadas no vazamento de informações da National Security Agency (NSA), consideradas confidenciais pelos Estados Unidos, também revelam a fragilidade sobre a segurança de informações críticas. Ou seja, os episódios demonstram não somente o poder do arsenal forense de agências governamentais como a CIA e a NSA, mas também como informações sensíveis, classificadas como sigilosas, fogem ao controle do Estado.⁷⁵

Mas não somente informações são vazadas, mas o próprio acesso a ferramentas de hacking, as quais são apropriadas por organizações criminosas. Também em 2017, o ransomware WannaCry afetou mais de 200.000 computadores distribuídos em 150 países, gerando prejuízos estimados em bilhões de dólares. Posteriormente foi revelado que o WannaCry foi construído em cima do EternalBlue, código de exploração de vulnerabilidade no Windows desenvolvido pela NSA e vazado pelo grupo Shadow Brokers.⁷⁶ O código da NSA foi, novamente, utilizado para criar o NotPetya, outro ransomware de amplas proporções que infectou computadores de diversos países na Europa, sobretudo de sites governamentais, bancários, de companhias de provimento de energia de jornais na Ucrânia.⁷⁷ Pesquisas em cibersegurança seguem vinculando o vazamento da NSA a outros ciberataques.⁷⁸

Se associados os episódios a um cenário onde políticas públicas para o avanço de uma agenda de cibersegurança ainda são insuficientes, como no Brasil,⁷⁹ resvalando sobre a falta de letramento em segurança por parte majoritária da população, os impactos resultantes de um vazamento de ferramenta de hacking assumem ainda maiores proporções. Importante lembrar dos mega-vazamentos de dados e

73 Vault 7: CIA Hacking Tools Revealed. Disponível em: <https://wikileaks.org/ciav7p1/> Acesso em 22 de julho de 2022.

74 LAWLER, Richard. Ex-CIA engineer convicted for sending classified hacking tools and info to WikiLeaks. The Verge, 2022. Disponível em: <https://www.theverge.com/2022/7/13/23208635/cia-wikileaks-vault-7-joshua-schulte-conviction> Acesso em 22 de julho de 2022.

75 Esse é o caso, igualmente, das denúncias feitas por Edward Snowden em 2013, baseadas no vazamento de informações consideradas confidenciais pelos Estados Unidos.

76 GOODIN, Dan. NSA-leaking Shadow Brokers just dumped its most damaging release yet. Ars Technica, 2017. Disponível em : <https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/> Acesso em 22 de julho de 2022.

77 POLITYUK, Pavel; PRENTICE, Alessandra Ukrainian banks, electricity firm hit by fresh cyber attack. Reuters, 2017. Disponível em: <https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ> Acesso em 22 de julho de 2022.

78 GREENBERG, Andy. The Strange Journey of an NSA Zero-Day—Into Multiple Enemies’ Hands. Wired, 2019. Disponível em: <https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/>. Acesso em 22 de julho de 2022.

79 HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. Instituto Igarapé, 2021. Disponível em https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em 22 de julho de 2022.



infecções por malwares recentemente notados no Brasil: no caso do setor público, chaves do pix foram recentemente vazadas dos sistemas do Banco Central;⁸⁰ dados de mais de 200 milhões de brasileiros cadastrados no Sistema Único de Saúde ficaram expostos no site do Ministério da Saúde;⁸¹ além do ataque via ransomware que tomou controle das máquinas de mais 1.200 servidores do Superior Tribunal de Justiça. E no que foi considerado o maior vazamento de dados da história do país, dados pessoais vinculados a 223 milhões de CPFs eram vendidos em fóruns da deep web, tendo como fonte uma variedade de bancos de dados distintos, dados que colocam o Brasil como 12º entre os países que mais registraram vazamento de dados.⁸²

Casos de abuso de poder de vigilância para finalidades políticas no Brasil também compõem o histórico de arbitrariedades governamentais que devem ser levadas em consideração quando da criação de modelos de governança sobre uso e acesso a ferramentas de hacking por autoridades. Basta citar, por exemplo, a condenação do Brasil pela Corte Interamericana de Direitos Humanos, em 2009, no que ficou conhecido como Caso Escher, quando trabalhadores ligados ao MST do Paraná tiveram suas comunicações grampeadas pela Polícia Civil do Estado com base em ordens judiciais sem embasamento e comprovação de necessidade;⁸³ no mesmo ano, o relatório final da Comissão Parlamentar das Escutas Telefônicas Clandestina, a “CPI do Grampo”, instaurada na Câmara dos Deputados, resultou na conclusão de que o Ministro Gilmar Mendes, do STF, teria sido alvo de escuta ilegal, bem como no afastamento do então Diretor-Geral da Agência Brasileira de Inteligência (ABIn), Paulo Lacerda.⁸⁴

Fica patente como a conjuntura da cibersegurança no Brasil, compreendendo sobretudo a segurança dos sistemas sob responsabilidade do setor governamental, expõe um contexto que não imprime segurança sobre o controle de acesso a ferramentas de alto potencial de invasividade, como as de hacking. Portanto, situações como o vazamento interno de informações, ataques maliciosos de terceiros e a possibilidade de abuso sobre o uso de recursos de vigilância compõem um campo de possibilidades que devem ser levados em consideração no desenho regulatório sobre permissões e restrições do hacking governamental.

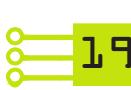
80 BANCO CENTRAL DO BRASIL. Banco Central comunica ocorrência em instituição. Banco Central do Brasil, s.d. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/BC_comunica_ocorrencia_Pix-2.pdf. Acesso em 22 de julho de 2022.

81 CAMBRICOLI, Fabiana. Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. Estadão, 2020. Disponível em: <https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340>. Acesso em 22 de julho de 2022.

82 STHALER, Gabriela. Ranking de vazamento de dados: Brasil é o 12º colocado. PrivacyTech, 2022. Disponível em: <https://privacytech.com.br/vazamentos/ranking-de-vazamento-de-dados-brasil-e-o-12-colocado,413580.jhtml>. Acesso em 22 de julho de 2022.

83 OLIVEIRA, Rafael. Caso Escher e outros versus Brasil. Reu Brasil, 2021. Disponível em: <https://reubrasil.jor.br/arley-jose-escher-e-outros/>. Acesso em 22 de julho de 2022.

84 CORREIO BRAZILIENSE. Entenda a CPI dos Grampos. Correio Braziliense, 2008. Disponível em: https://www.correio-braziliense.com.br/app/noticia/politica/2008/11/26/interna_politica,51893/entenda-a-cpi-dos-grampos.shtml. Acesso em 22 de julho de 2022.



3. INSEGURANÇA DISTRIBUÍDA: negociando a exploração de vulnerabilidades enquanto cultura investigativa no Brasil

3.1. O circuito internacional: importação e negociações entre Brasil e países exportadores de tecnologias de vigilância

Até que venha a efetivamente fazer parte do ferramental forense de uma agência de investigação, o comércio internacional de tecnologias de hacking pode passar por um circuito geopolítico complexo, que vão desde a descoberta contínua de vulnerabilidades em sistemas e dispositivos mundialmente usados, a intermediação de sua venda a fabricantes de softwares forenses, a negociação desses produtos com potenciais clientes e registros de patente, até à demanda interna de forças de investigação, dispensas de licitação para a contratação, variadas representações comerciais e, na melhor das hipóteses, regras internas sobre importação, acesso e uso a essas ferramentas. No caso do Brasil, boa parte desses elementos estão presentes e compõem um cenário para que a capilaridade de ferramentas de hacking seja consideravelmente ampla.

As negociações “diplomáticas” com fabricantes ficam mais claras, sobretudo no contexto de governos cuja agenda punitivista é mais marcante. Além das negociações envolvendo entre o Ministério da Justiça e Ainda esse ano, comitiva governamental envolvendo Eduardo Bolsonaro e representantes do Ministério da Defesa e a Secretaria de Assuntos Estratégicos da Presidência se reuniu em Abu Dhabi, com o Grupo Edge,⁸⁵ por trás da tecnologia DarkMatter⁸⁶ - já acusada pela Electronic Frontier Foundation ter sido meio para espionar e resultar na tortura de Loujain al-Hathloul, cidadã dos Emirados Árabes, em 2018.⁸⁷ E em 2021, foi revelado que Carlos Bolsonaro teria aproveitado visita diplomática à Israel, em 2019, para tentar negociar a aquisição do programa Sherlock,⁸⁸ desenvolvida pela Candiru, empresa já denunciada pelo Citizen Lab como “vendedora mercenária de spywares” e meio para a perseguição de jornalistas, políticos e defensores de direitos humanos sobretudo em uma diversidade de países do oriente médio, mas também de países como Espanha e Reino Unido.⁸⁹ Em 2021, a Candiru entrou para a lista do Bureau de Indústria e Segurança, do Departamento de Comércio dos Estados Unidos, por “participar de atividades contrárias à segurança nacional”⁹⁰

85 UOL. Eduardo Bolsonaro esteve em reunião com empresa árabe de espionagem. UOL, 2022. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2022/06/01/eduardo-bolsonaro-estava-em-reuniao-com-empresa-arabe-de-espionagem.htm>. Acesso em 22 de julho de 2022.

86 DAROS, Gabriel. DarkMatter: o que é, como funciona e qual o risco do app de espionagem? UOL, 2022. Disponível em <https://www.uol.com.br/tilt/noticias/redacao/2022/01/18/darkmatter-quais-riscos-oferecem-o-programa-espiao-que-o-governo-quer.htm> Acesso em: 29 de julho de 2022

87 ELECTRONIC FRONTIER FOUNDATION. Alhathloul v DarkMatter. Eletronic Frontier Foundation, 20221. Disponível em: <https://www.eff.org/document/alhathloul-v-darkmatter> Acesso em: 29 de julho de 2021

88 VALENÇA, Lucas. Além do Pegasus, Carlos Bolsonaro queria sistema para monitorar o Planalto. UOL, 2021. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2021/08/03/alem-do-pegasus-carlos-bolsonaro-previa-sistema-para-monitorar-planalto.htm> 29 de julho de 2022

89 MARCZAK, Bill et. al. Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus. CitIzen Lab, 2021. Disponível em: <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/> Acesso em: 29 de julho de 2022

90 DEPARTAMENTO DE COMÉRCIO DOS ESTADOS UNIDOS. 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 24 de julho de 2022.

Ainda que as negociações mencionadas tenham composto o histórico político recente e representem um termômetro significativo da inclinação governamental em adquirir as ferramentas, não encontramos contratos firmados com as mencionadas empresas. Por outro lado, outro conjunto amplo de fornecedores figuram nos achados do levantamento deste estudo. Cada um deles provê uma ou mais soluções, para finalidades que vão desde a extração de dados de todas as aplicações existentes em um dispositivo, inteligência artificial com reconhecimento facial de imagens armazenadas e quebra de criptografia até interceptação de comunicações e mensagens em tempo real e um raio de alcance amplo.

Durante o processo de coleta dos dados, coletamos 228 documentos contratuais. Entretanto, 19 deles referiam-se a negociações realizadas entre 2013 e 2014, ou seja fora do período estabelecido como recorte de análise (entre 2015 e 2021), ainda que mereçam atenção. Desta forma, as tabelas, gráficos e suas respectivas análises aqui presentes foram realizadas a partir do levantamento de 209 contratos (182 totalizando os estaduais e 27 federais) coletados, dentro do período destacado, nos Portais de Transparências federal e estaduais, incluindo o do Distrito Federal. Ademais, foram acionados por meio da Lei de Acesso à Informação, em âmbito estadual, as 27 Secretarias responsáveis por atividades de segurança pública, assim como os respectivos Ministérios Públicos estaduais. No campo federal, pelo mesmo mecanismo, foram solicitadas informações ao Ministério Público Federal e à Polícia Federal através do Ministério da Justiça e Segurança Pública, ao Ministério da Defesa, Comando do Exército (CEX), Comando da Marinha (CMAR) e ao Gabinete de Segurança Institucional. No caso das Secretarias estaduais, 5 delas não responderam aos pedidos. Já para os Ministérios Públicos Estaduais, 5 pedidos foram inviabilizados ou seguem tramitando e sem resposta conclusiva.⁹¹ No âmbito federal, todas as instituições responderam aos pedidos. Os problemas na obtenção de respostas também incluem plataformas de difícil acesso ou mesmo completamente inacessíveis, como no caso de Alagoas, que permaneceu de meados de março até o fim de julho de 2022 fora do ar.

No que concerne ao levantamento realizado nos Portais de Transparências, diversas dificuldades foram encontradas ao longo do processo. Entre elas, a mais significativa foi a falta da padronização dos mecanismos de busca entre os Portais acessados. Consequentemente, a cada Portal dos Estados acessados, fazia-se necessário reaprender os mecanismos do Portal e dos caminhos que levavam às empresas. Para encontrar um denominador comum, foram utilizados os mecanismos de buscas que levavam diretamente aos fornecedores, entre eles o próprio cadastro de fornecedores oferecidos pelos Portais ou notas de empenho destinadas aos credores que tínhamos interesse. Em especial aos dados coletados por meio de nota de empenho, fez-se distinguir, por exemplo, se dadas notas de empenho se referiam a um único contrato. Com isso, foi preciso coletar todas as informações de empenho sobre o mesmo contrato ou processo licitatório para que chegássemos ao valor total da aquisição dos produtos, e considerar todos esses empenhos como um único valor a fim de não inflacionar o quantitativo final de contratos.

Um outro ponto de dificuldade encontrado foi o fato de que alguns contratos coletados possuíam, nos dados cadastrados no Portal de Transparência, valores inferiores ao que realmente custavam ao se acessar o instrumento contratual em si. Assim, foi necessário acessar todos os contratos disponibilizados, quando possível, para conferir se o valor informado no Portal condizia com o montante negociado pelo produto adquirido.

Como resultado, surgiam dificuldades adicionais decorrentes do processo de coleta, quer dizer, nem sempre as informações disponibilizadas estavam completas. Em diversos casos, não tivemos acesso aos contratos assinados entre as partes em negociação, somente às informações cadastrais dos contratos disponibilizadas nos Portais de Transparência. Em outros casos, não era informado o quantitativo de ferramentas ou serviços adquiridos, nem qual a tecnologia foi adquirida. Para esses casos, conforme será observado nos gráficos de distribuição das ferramentas por região do país e em âmbito federal, optamos por transcrever conforme estava presente nos Portais. Diversos termos foram relevantes nas descrições para decidir se tais achados se incluíam no objeto de estudo, como os termos “extração”, “decodificação”,

91 Até a data de publicação deste estudo.

“perícia em telefones”, “análise forense em celulares”, “exame digital em celulares”, “quebra de senha”, “interceptação” e similares. Para a contabilização desses casos que não definiam quantidades de serviços adquiridos, entendemos que ao menos um serviço havia sido adquirido.

Chama atenção, também, a amplitude de terminologias para a mesma finalidade das ferramentas, que vão desde “dados em nuvem” e “dados de redes sociais” até “artefatos de Internet” para significar o acesso a dados pessoais de forma ampla. Ou mesmo uma variedade de terminologias para se referir à natureza da ferramenta em si, como “solução de inteligência tática”, “software de perícia forense”, “ciber inteligência”, “software para laboratório de forense digital” ou mesmo “solução para coleta, processamento e análise de dados e informações a partir de plataformas eletrônicas portáteis”. Além de expor uma leitura bastante variável sobre ferramentas de hacking e suas funções a depender da entidade contratante, essa amplitude de denominações dificulta a fiscalização pública. Como destacado na introdução deste estudo, não seria possível realizar um levantamento suficientemente amplo apenas a partir do nome de uma funcionalidade (“extração de dados”, por exemplo). Por isso, a busca nominal pelas empresas foi necessária.

Descrevemos a seguir, respectivamente, as empresas fabricantes, revendedores no Brasil (caso se aplique), produtos contratados e respectivas habilidades que oferecem às entidades governamentais contratantes. Nos capítulos seguintes, apresentamos a capilaridade dessas ferramentas na estrutura investigativa do Brasil.

Tabela 2: Perfil das ferramentas encontradas

Revendedor/Contratado direto: TechBiz Forense Digital	
Fabricante: Cellebrite DI Ltd.	
Produto	Funções
UFED ⁹² 4PC ou Touch 2 (portátil)	<ul style="list-style-type: none">Desbloqueio de dispositivos protegidos por padrão, senha ou código PIN, bem como extração de dados de celulares como HTC, Motorola, Samsung da família Galaxy S, SII e SIII;Bypass de criptografia em dispositivos Android e iOS;Extração lógica e física de celulares, drones, cartões SIM e SD, dispositivos de GPS e outros, incluindo extração de todo o sistema de arquivos (full file system extraction) ou de arquivos selecionados de acordo, por exemplo, com a aplicação (redes sociais, aplicações de mensageria, navegadores, entre outros);Recuperação de arquivos deletados;Extração de dados de dispositivos baseados em chipsets Qualcomm, independente do fabricante (função para UFED 4PC).

UFED ⁹³ Cloud	<ul style="list-style-type: none"> Extração e análise de conteúdos baseados em nuvem disponíveis em mais de 50 aplicações e fontes em nuvem; Acesso a dados não mais armazenados em dispositivos físicos ao recuperar backups em nuvem;⁹⁴ Ganho de informações sobre as intenções de um indivíduo, seus interesses e relacionamentos ao analisar postagens, curtidas e conexões. Ver atividades e localizações de um usuário a partir do Facebook, Google e iCloud através de vários dispositivos; Visualização de correlações e conexões sobre um indivíduo a partir de diferentes fontes de dados.
Cellebrite Physical Analyzer ⁹⁵	<ul style="list-style-type: none"> Visualização, categorização e sistematização de backups feitos via extração de dados a partir do UFED,⁹⁶ incluindo dados criptografados; Recuperação de arquivos e dados deletados; Emulação de aplicações para visualização, em formato original, dos dados extraídos.
Cellebrite Premium ⁹⁷	<p>Recursos para sistemas iOS:</p> <ul style="list-style-type: none"> Desbloqueio de dispositivos Apple nas versões mais atuais do iOS; Minimização de tentativas de desbloqueio no uso de técnicas de força-bruta para revelar senhas; Extração full-file system de dispositivos iOS, incluindo bypass de criptografia de backups do iTunes; Acesso a senhas armazenadas e tokens do Keychain (sistema de gerenciamento de senhas no macOS); Recuperação de dados de outras aplicações como WhatsApp, Facebook e Telegram; Acesso a emails e arquivos anexados; Acesso a dados de geolocalização provenientes de torres de celular e Wi-Fi; Extração parcial de dados mesmo enquanto o dispositivo está bloqueado. <p>Recursos para sistemas Android:</p> <ul style="list-style-type: none"> Burlar ou determinar senhas em todos os principais dispositivos Samsung; Acesso a dados de aplicações protegidas com senha adicional via KNOX; Secure Folder (recurso do Galaxy para encriptação de dados); Extração de dados não alocados para maximização da recuperação de itens deletados; Recuperação de dados de outras aplicações como WhatsApp, Facebook e Telegram; Acesso a emails e arquivos anexados; Acesso a dados de geolocalização provenientes de torres de celular e Wi-Fi.

93 Ver https://cellebrite.com/wp-content/uploads/2020/05/ProductOverview_Cellebrite_UFEDCloud_web.pdf

94 Ver lista completa de fontes de dados suportadas pela ferramenta (última atualização em 2017): https://cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf. Acesso em 20 de julho de 2022.

95 Ver <https://techbiz.com.br/produto/cellebrite-physical-analyzer/> e https://cellebrite.com/wp-content/uploads/2020/07/ProductOverview_Cellebrite_Physical_Analyzer.pdf

96 Ver lista completa de fontes de dados suportadas pela ferramenta (última atualização em 2017): https://cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf. Acesso em 20 de julho de 2022.

97 https://cellebrite.com/wp-content/uploads/2020/07/ProductOverview_CellebritePremium.pdf



Cellebrite Pathfinder ⁹⁸	<ul style="list-style-type: none"> • Recursos baseados em algoritmos de machine learning e reconhecimento de padrões, correlacionando arquivos de mídia, análise de contatos e interações com terceiros para definir quem, o quê, onde, quando e porquê; • Detecção, reconhecimento e categorização de imagens, incluindo objetos e faces.
Cellebrite Advanced Services ⁹⁹	<ul style="list-style-type: none"> • Baseado em consultoria com especialistas da Cellebrite; • Desbloqueio de tela por padrão, código PIN ou senha nos dispositivos mais recentes com iOS e Android; • Extração física e decriptação de dados de dispositivos móveis, inclusive com extração full-file system dos dispositivos com iOS e Android, com envio posterior à contratante de unidade USB com as informações extraídas; • Recuperação e exame de dados em dispositivos esmagados, quebrados, queimados ou danificados por água.
Cellebrite CHINEX	<ul style="list-style-type: none"> • Extração física de dados existentes, escondidos e deletados de celulares de fabricação chinesa; • Extração de senhas de usuário; • Reconhecimento automático de pin-outs; • Habilidade de superar e decodificar códigos de bloqueio de dispositivos.
Cellebrite Commander ¹⁰⁰	<ul style="list-style-type: none"> • Supervisão sobre o uso de outras ferramentas de extração e análise de dados; • Distribuição e instalação remota de atualizações de software e modificações de configuração; • Coleta automática de estatísticas de uso de outras ferramentas; • Backup automático de metadados de todas as extrações de dados; • Guarda de logs de atividades de uso com painel de análise.
Fabricante: OpenText	
Encase Forensic ¹⁰¹	<ul style="list-style-type: none"> • Acesso a dados encriptados com Bitlocker (Windows 10), Data Protection 8.17 (Dell) e PGP v10.3 (Symantec); • Acesso a dados encriptados com APFS (Apple File System);¹⁰² • Bypass da segurança para o Apple T2.¹⁰³

98 Ver https://cellebrite.com/wp-content/uploads/2020/08/ProductOverview_Cellebrite_Pathfinder.pdf

99 Ver <https://cellebrite.com/pt/servicos-avancados/>

100 Ver https://cellebrite.com/wp-content/uploads/2020/05/ProductOverview_Commander_LTR_web.pdf

101 OPENTEXT. OpenText Encase Forensic. 2022. Disponível em https://security.opentext.com/docs/default-source/documents/library/product-brief/encase-forensic-product-overview_f2989faa-5cd6-42e2-b23e-dc031dd5f471.pdf. Acesso em 22 de julho de 2022.

102 Sistema de arquivos proprietário da Apple, com criptografia forte. Aplicado a todas as plataformas da Apple, como iPhone, iPad, iPod Touch, Mac, Apple TV e Apple Watch. Ver <https://support.apple.com/de-de/guide/seca6147599e/web>

103 O Apple T2 Security Chips fornece armazenamento criptografado, funções para inicialização segura e proteção de dados do Touch ID, entre outras funções. Ver <https://support.apple.com/de-de/HT208862>



Fabricante: OpenText

Magnet AXIOM¹⁰⁴

- Suporte para computador, celular, nuvem e carros;
- Reconhecimento de imagens, incluindo faces e objetos;
- Suporte à análise de dados extraídos de dispositivos de outras ferramentas;
- Bypass de senhas para recuperar imagens de sistemas Android bloqueados, como Samsung, Motorola, LG, MTK, e Qualcomm, com capacidades avançadas de extração;
- Sua fabricante, a Magnet Forensics, tem parceria com Passware, provendo a examinadores a habilidade de resgatar dados de drives encriptados com TrueCrypt e BitLocker;
- Recuperação de dados e comunicações de aplicativos com armazenamento em nuvem, como WhatsApp, Facebook, Instagram, Google, Twitter e outros;
- Filtragem, marcação e visualização de conversas para mensagens individuais e chats completos.

Fabricante: Exterro / AccessData

Forensic Toolkit (FTK)¹⁰⁵

- Unificação de banco de dados para armazenamento de provas; Indexação, filtragem e ferramentas de pesquisa de resultados de dados armazenados;
- Reconhecimento e detecção de imagens, incluindo faces e objetos;
- Localização, manuseio e filtragem de dados, móveis, de rede, com segmentação entre dados e comunicações;
- Busca de histórico de navegação de todos os navegadores e segmentação de por metadados categoria (conteúdo adulto, conversas, dark web, notícias etc);
- Decriptação de arquivos, quebra de senhas; recuperação de senhas de mais de 100 aplicações; Decriptação de discos de computador encriptados com a última versão do McAfee Drive Encryption;
- Coleta, processamento e análise de conjuntos de dados contendo arquivos do sistema Apple que estejam encriptados, comprimidos ou deletados;
- Faz a decriptação de FileVault 2 do sistema de arquivos APFS (Apple File System).

104 MAGNET FORENSICS. Magnet AXIOM. 2022. Disponível em http://go.magnetforensics.com/Why_Upgrade_ENG. Acesso em 22 de julho de 2022. Ver, também, MAGNET FORENSICS. Getting Started with Magnet AXIOM Process - Computers. 2018. Disponível em https://www.youtube.com/watch?v=UhD5jXg6KFo&list=PLrDSw3yTk3XiGdhjD6r-d6lggHVbwNa&ab_channel=MagnetForensics. Acesso em 22 de julho de 2022. Também foram realizadas aquisições da ferramenta Internet Evidence Finder (IEF), do mesmo desenvolvedor, por órgãos brasileiros. O produto foi descontinuado pela Magnet Forensics e substituído pelo Magnet AXIOM, por possuir menos funcionalidades que sua sucessora.

105 EXTERRO. FTK Forensic Toolkit. 2022. Disponível em <https://www.exterro.com/forensic-toolkit>. Acesso em 22 de julho de 2022; EXTERRO. Zero In On Evidence Faster—recognized around the world as the standard in computer forensics software. Disponível em https://go.exterro.com/l/43312/2021-07-28/f5r9hf/43312/1627485686szZaKkD2/FTK_Brochure.pdf. Acesso em 22 de julho de 2022.



Fabricante: Micro Systemation AB (MSAB)

Produto	Funções
XRY Logical ¹⁰⁶	<ul style="list-style-type: none"> Extração e cópia de dados de dispositivos digitais, incluindo cartões de memória SIM e SD; Acesso e análise de dados em aplicações com criptografia forte, como WhatsApp, WhatsApp Business e Telegram e Signal. Compatível com dispositivos Android.
XRY Physical	<ul style="list-style-type: none"> Extração física de dados de dispositivos móveis; Bypass e/ou recuperação de senhas; Possibilidade de acessar dados de celulares bloqueados; Reconstrução de arquivos deletados; Clonagem de cartões SIM.
XAMN Horizon	<ul style="list-style-type: none"> Adiciona recursos de visualização ao XAMN Spotlight, como análise a partir de geolocalização, de conversas em aplicações de mensageria e conexões entre diferentes usuários e dispositivos distintos.
XAMN Spotlight	<ul style="list-style-type: none"> Análise, filtragem, visualização e sistematização de dados extraídos de dispositivos móveis, drones, tecnologias vestíveis, de GPS, veículos, cartões SIM, cartões de memória e outras fontes; Reconhecimento de conteúdos em imagens
XRY Pinpoint ¹⁰⁷	<ul style="list-style-type: none"> Recurso adicional ao XRY Logical e Physical; Suporte para extração e decodificação de dados de dispositivos “non-standard” (“typically manufactured in Eastern Asia”); Identificação automática de “pin-outs”; Suporte para chipsets MediaTek, SpreadTrum, Coolsand e Infineon.
XRY Cloud ¹⁰⁸	<ul style="list-style-type: none"> Extração de dados de dispositivos digitais; Extração de dados de aplicações com armazenamento em nuvem, como Facebook, Google, iCloud, Twitter e Snapchat. Inclui modalidade de extração automática, a partir de tokens de acesso a aplicações previamente extraídos com aparelho em mãos, e de extração manual, sem necessidade do aparelho estar presente, a partir de login e senha previamente acessados por outros meios.
MSAB Office ¹⁰⁹	<ul style="list-style-type: none"> Extração lógica e física de dados de dispositivos móveis, incluindo dados deletados; Leitura e clonagem de cartão SIM; Extração de dados de dispositivos GPS.

106 MSAB. XRY Logical. 2022. Disponível em https://www.msab.com/wp-content/uploads/2022/06/XRY_Logical_EN-2.pdf, Acesso em 22 de julho de 2022; MSAB. What is XRY Photon. 2022. Disponível em <https://www.msab.com/product/xry-extract/xry-photon/>. Acesso em 22 de julho de 2022.

107 MSAB. XRY PinPoint. 2021. Disponível em https://www.msab.com/wp-content/uploads/2021/10/XRY_PinPoint_US.pdf. Acesso em 22 de julho de 2022.

108 MSAB. XRZ Cloud. 2022. Disponível em https://www.msab.com/wp-content/uploads/2022/06/XRY_Cloud_EN.pdf. Acesso em 22 de julho de 2022.

109 MSAB, MSAB Office. 2022. Disponível em https://www.msab.com/wp-content/uploads/2022/05/MSAB_Office_EN.pdf. Acesso em 22 de julho de 2022.

Fabricante: Exterro / AccessData	
Produto	Funções
Forensic Toolkit (FTK) ¹¹⁰	<ul style="list-style-type: none"> • Unificação de banco de dados para armazenamento de provas; • Indexação, filtragem e ferramentas de pesquisa de resultados de dados armazenados; • Reconhecimento e detecção de imagens, incluindo faces e objetos; • Localização, manuseio e filtragem de dados, móveis, de rede, com segmentação entre dados e comunicações; • Busca de histórico de navegação de todos os navegadores e segmentação de por metadados categoria (conteúdo adulto, conversas, dark web, notícias etc); • Decriptação de arquivos, quebra de senhas; recuperação de senhas de mais de 100 aplicações; • Decriptação de discos de computador encriptados com a última versão do McAfee Drive Encryption; • Coleta, processamento e análise de conjuntos de dados contendo arquivos do sistema Apple que estejam encriptados, comprimidos ou deletados; • Faz a decriptação de FileVault 2 do sistema de arquivos APFS (Apple File System).
Revendedor: Cognyte / Suntech	Fabricante: Verint Systems / Cognyte / Suntech

¹¹⁰ EXTERRO. FTK Forensic Toolkit. 2022. Disponível em <https://www.exterro.com/forensic-toolkit>. Acesso em 22 de julho de 2022; EXTERRO. Zero In On Evidence Faster—recognized around the world as the standard in computer forensics software. Disponível em https://go.exterro.com/l/43312/2021-07-28/f5r9hf/43312/1627485686szZaKkD2/FTK_Brochure.pdf. Acesso em 22 de julho de 2022.

¹¹¹ VERINT. Tactical Off-Air Intelligence Solutions. 2013. Disponível em <https://www.documentcloud.org/documents/885760-1278-verint-product-list-engage-gi2-engage-pi2>. Acesso em 22 de julho de 2022.

¹¹² VERINT. Op. cit.

3.2. Ferramentas de hacking no Brasil, em números

Porcentagem de contratos por fornecedor, em âmbito estadual

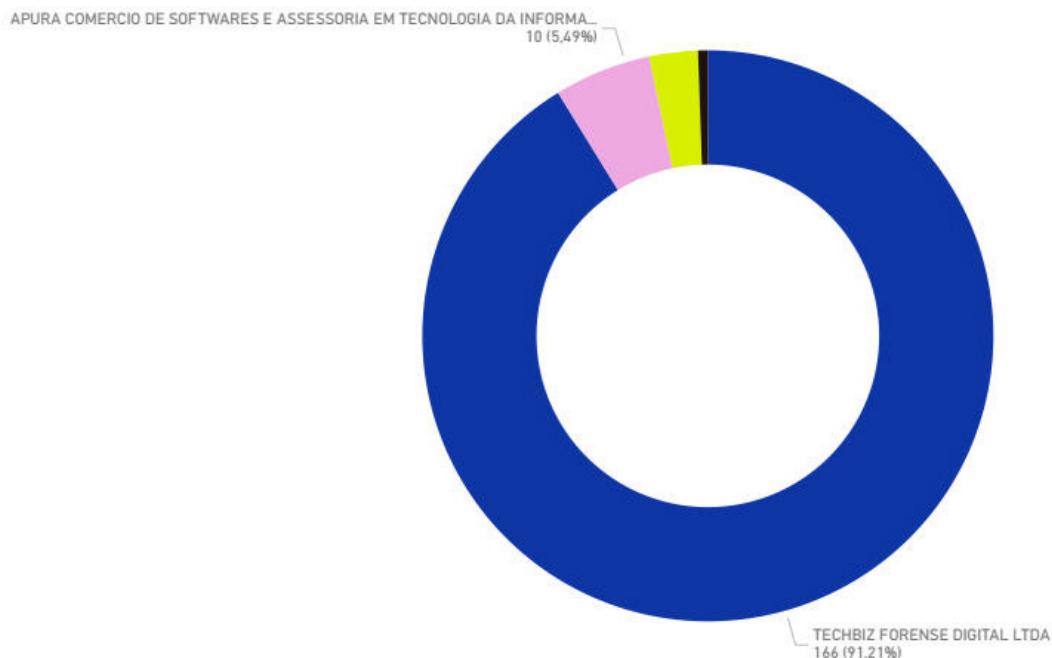


Gráfico 2: Porcentagem de contratos estaduais, por fornecedor.

Porcentagem por empresa contratada, em âmbito federal

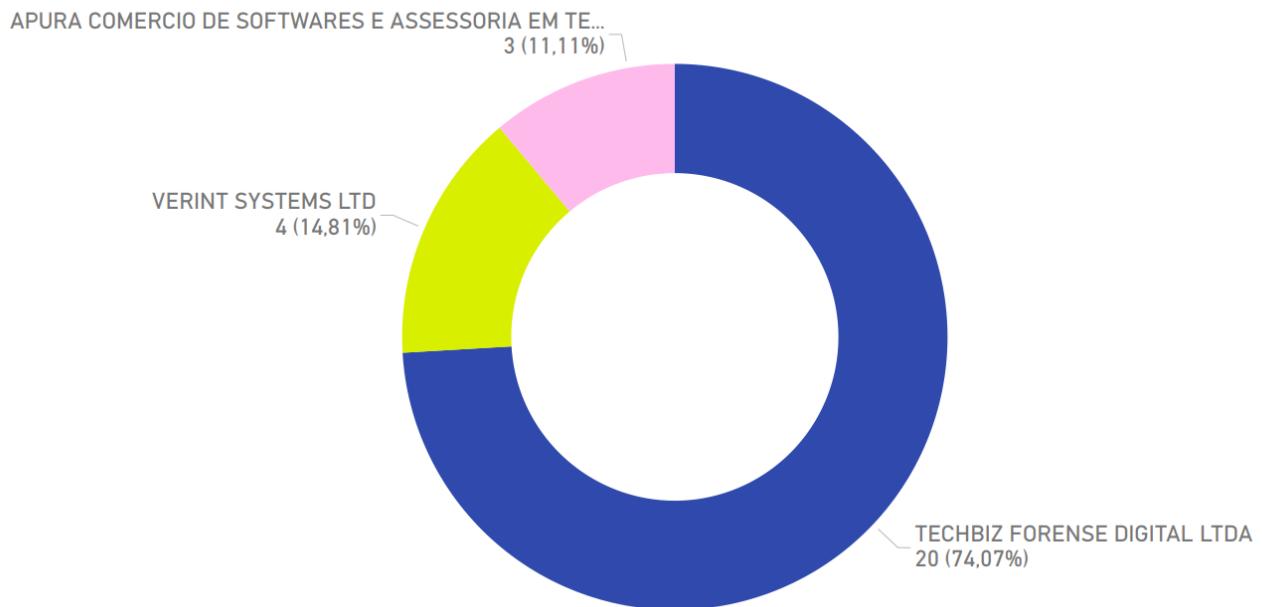


Gráfico 3: Porcentagem de contratos federais, por fornecedor.

Porcentagem de contratos por região

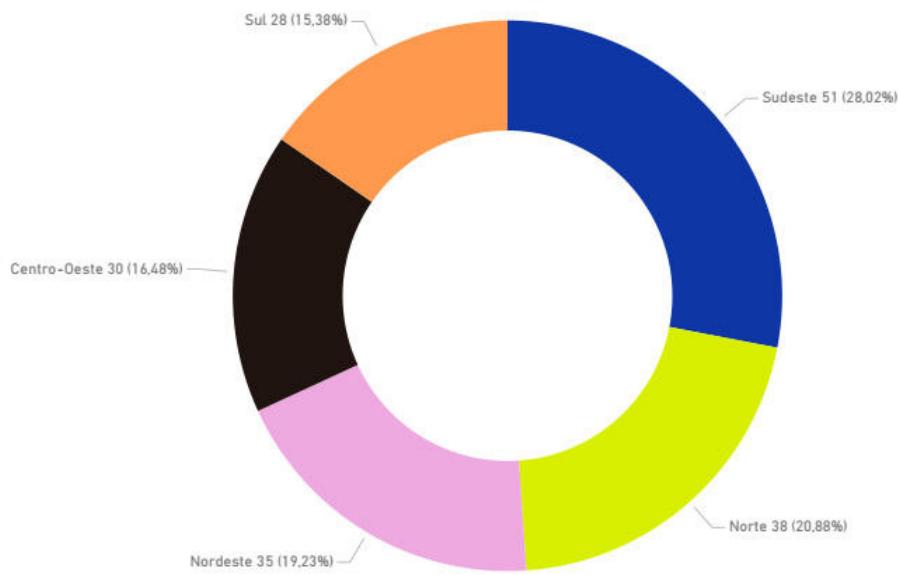


Gráfico 4: Porcentagem de contratos, por região.

Gastos estaduais e federais, entre 2015 e 2021

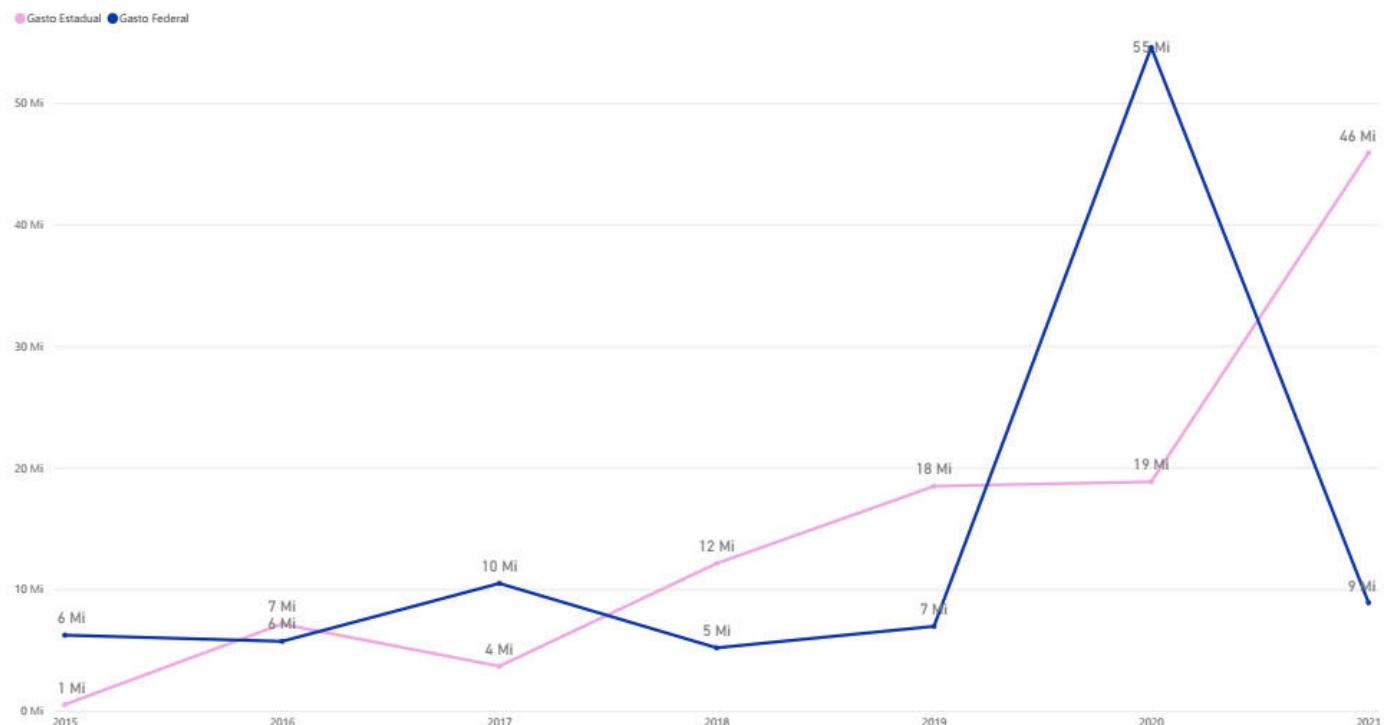


Gráfico 5: Gastos estaduais e federais, por ano
(em número nominais, sem correção de inflação)

3.3. Distribuição de contratos no Brasil

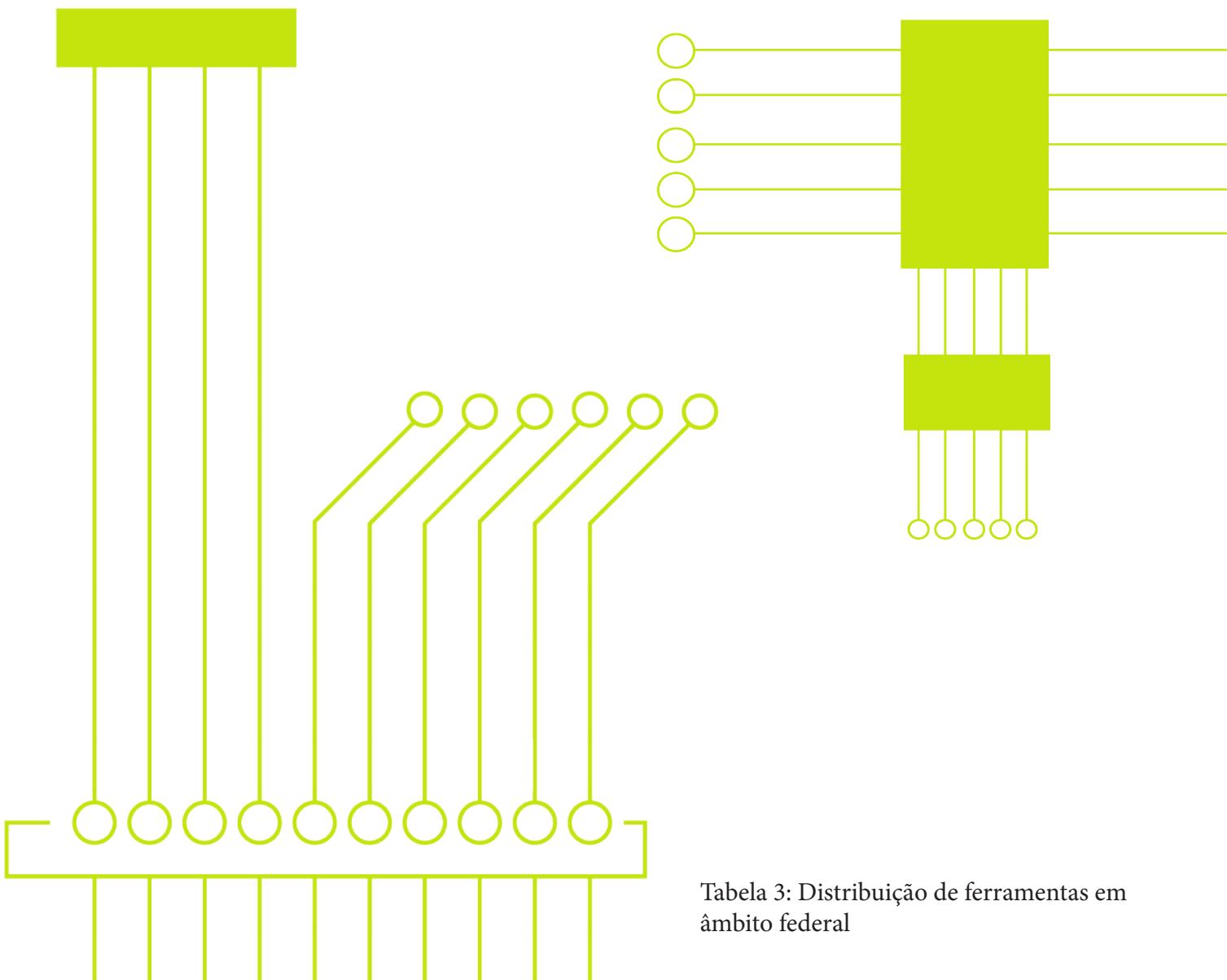


Tabela 3: Distribuição de ferramentas em âmbito federal

Responsável pela compra	Fabricante (Revendedor)	Ferramenta
Ministério da Defesa / Comando do Exército / Comissão do Exército Brasileiro em Washington	Verint Systems (Verint Systems)	<ul style="list-style-type: none">• GI2• PI2
Ministério da Defesa / Comando do Exército / Comando do Militar Leste	Exterro/AccessData (Apura Comércio de Softwares e Assessoria em Tecnologia da Informação)	<ul style="list-style-type: none">• Forensic Toolkit

Ministério da Defesa / Comando da Marinha / Diretoria de Comunicação e Tecnologia da Informação da Marinha	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED 4PC
	OpenText (Techbiz Forense Digital)	<ul style="list-style-type: none"> EnCase Forensic
	Exterro/AccessData (Techbiz Forense Digital)	<ul style="list-style-type: none"> Forensic Toolkit
Ministério da Defesa / Comando da Marinha / Comissão Naval Brasileira na Europa	Verint Systems (Verint Systems)	<ul style="list-style-type: none"> GI2
Ministério da Defesa / Comando do Exército / BASE ADMINISTRATIVA DO CCOMGE	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> “UFED”
Ministério da Economia / Fundo Constitucional do Distrito Federal / FCDF-SSP-Polícia Civil do DF	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED Premium
Ministério da Justiça e Segurança Pública / Departamento de Polícia Federal / Superintendência Regional no Estado de SP	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED 4PC UFED Touch 2 UFED Cloud Analyzer UFED Desktop Analytics Cellebrite Commander
Ministério da Justiça e Segurança Pública / Departamento de Polícia Federal / Superintendência Regional no Estado do AM	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> Cellebrite Advanced Services
Ministério da Justiça e Segurança Pública / Departamento de Polícia Federal / Superintendência Regional Polícia Rodoviária de Goias	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED Touch UFED Cloud UFED Pathfinder



Ministério da Justiça e Segurança Pública / Departamento de Polícia Federal / Diretoria Técnico-Científica - DITEC/DPF	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED 4PC Ultimate
Ministério da Justiça e Segurança Pública / Unidades com Vínculo Direto / Coordenação-Geral de Logística e Contratos/MJ	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “UFED”
Ministério da Justiça e Segurança Pública / Conselho Administrativo de Defesa Econômica (CADE)	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Touch • “UFED”
	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de Software de Análise Forense”
Ministério da Justiça e Segurança Pública / Fundo Nacional de Segurança Pública	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “UFED”
	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Créditos Individuais e Perpétuos para Desbloqueio e Extração de Dispositivos Computacionais”
Ministério da Justiça e Segurança Pública / Unidades com Vínculo Direto / Secretaria Nacional de Segurança Pública	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Ferramenta tecnológica para Extração, processamento e Análise de Dados e Informações Obtidas por meio de Plataformas Eletrônicas Portáteis”



Estado	Responsável pela compra	Fabricante (Revendedor)	Ferramenta
Acre	Secretaria de Estado de Justiça e Segurança Pública - SEJUSP	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Cellebrite” • UFED Touch
	Fundo Estadual de Segurança - FUNDSEG / Fundo Especial do Ministério Público do Estado do Acre	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Pathfinder • UFED Touch
Amapá	SEJUSP	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Solução Tecnológica de Extração de Dados em Dispositivos Móveis”
	FUNESP	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de Solução de Extração de Dados em Dispositivos Móveis”
	MP-AP	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Cloud • UFED Touch • UFED Analyzer
Amazonas	Polícia Civil	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Sistema Extrator De Dados”
	Secretaria de Estado de Segurança Pública	Suntech (Verint Systems)	<ul style="list-style-type: none"> • GI2



Tabela 4: Distribuição de contratos na Região Norte

	Secretaria de Estado de Justiça e Segurança Pública - SEGUP	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de Solução, em Hardware Próprio, para Extração e Análise de Dados a partir de Plataformas Eletrônicas Portáteis”
Pará	Fundo de Investimento de Segurança Pública	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> Sistema para Extração, Decodificação e Análise Forense de Dados em Dispositivos Móveis, com Tela Touchscreen, Bateria Integrada e Mesa de Trabalho Incorporada, com Kit Completo e Pronto para Uso em Campo
Roraima	Secretaria de Estado da Segurança Pública (SESP)	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Equipamento para Perícia em Telefones Celulares (inclusive chineses) PDAS, GPS e Smartphones”
	Núcleo de Inteligência da Polícia Civil do Estado de Roraima (NI/DENARC/PCRR)	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED 4PC
	Ministério Público Estadual / Procuradoria Geral de Justiça de Roraima	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED Cloud



Tocantins	Núcleo Especializado de Computação Forense do Instituto de Criminalística	Magnet Forensics (Techbiz Forense Digital)	Magnet Axiom
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Cellebrite” • “UFED”
	Fundo de Segurança Pública do Estado do Tocantins	Magnet Forensics (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Magnet Axiom
	Procuradoria Geral da Justiça	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “UFED”
			<ul style="list-style-type: none"> • UFED Touch • UFED Touch 2



Tabela 5: Distribuição de contratos na Região Nordeste

Estado	Responsável pela compra	Fabricante (Revendedor)	Ferramenta
Alagoas	Perícia Oficial do Estado de Alagoas	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Ferramenta Forense Para Extração de Dados de Dispositivos Móveis”
	Ministério Público - AL	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição e implantação de solução tecnológica para extração e análise de dados de dispositivos móveis, incluindo hardwares, softwares e treinamento”
	Fundo Penitenciário do Estado de Alagoas	Verint Systems (Suntech S.A.)	<ul style="list-style-type: none"> GI2
Bahia	SSP	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Pag. Aquisição Conjunto De Soluções, Completa, P/ Análise Forense De Celulares, Dispositivos Portáteis De Gps...”
	Ministério Público - BA	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Cellebrite”
	SEAP	<ul style="list-style-type: none"> Cellebrite (Techbiz Forense Digital) Desconhecido (Apura Comercio de Softwares e Assessoria em Tecnologia da Informação) 	<ul style="list-style-type: none"> UFED 4PC UFED Pathfinder Desktop UFED Cloud “Solução Para Extração De Dados Em Equipamentos Móveis (Celulares, Smartphone, Tablets E Pdas); Equipamento De Análise Forense Acompanhado De Licença De Software”



Ceará	Secretaria da Segurança Pública e Defesa Social	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Solução perpétua integrada composta por hardware e software para extração, processamento e análise de dados a partir de plataformas eletrônicas portáteis, incluindo os serviços de suporte técnico e atualizações”
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED Cloud Analyzer Cellebrite Advanced Services UFED 4PC
Maranhão	Fundo Estadual de Segurança Pública e Defesa	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de equipamentos de extração/aquisição forense de dispositivos computacionais portáteis, softwares e suporte técnicos correspondentes”
		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Solução de Extração, Analises e Processamento de Dados em Plat,
	Secretaria de Estado da Segurança Pública	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> Monitoramento de Inteligência de dados, Coleta Analises e Processamento de Dados em Plataf.”
	Pólicia Civil	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> “UFED” “Cellebrite”



Paraíba	Ministério Público - PB	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de solução para extração, processamento e análise colaborativa de dados de plataformas eletrônicas portáteis.”
	Núcleo de Criminalística de João Pessoa e Núcleo de Criminalística de Campina Grande	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> Cellebrite Physical Analyser
	Polícia Militar	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Cellebrite”
	Secretaria de Estado da Segurança e da Defesa Social	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de Solução Tecnológica para Extração de Dados em Dispositivos Móveis”
Pernambuco	Ministério Público - PE	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Solução para coleta, processamento e análise de dados e informações a partir de plataformas eletrônicas portáteis. Solução básica de apoio na análise de dados e informações a partir de plataformas eletrônicas portáteis para cruzamento de vínculos. Solução de extração e processamento de dados a partir das nuvens. Solução avançada de análise para cruzamento de vínculos.”
	Secretaria de Defesa Social - PE	Magnet Forensics (Techbiz Forense Digital)	<ul style="list-style-type: none"> Magnet Axiom
Piauí	Fundo Estadual de Segurança Pública e Defesa Social - FUNSEP	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de Sistema para Extração e Análise Forense”
	Ministério Público - PI	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Cellebrite”
	Secretaria de Segurança Pública	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED 4PC



Rio Grande do Norte	Ministério Público - RN	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Fornecimento de solução para extração, processamento e análise de dados de aparelhos móveis a partir de plataformas eletrônica portátil” • “Aquisição de licença de uso de software, para fins de extração de dados de aparelhos móveis” • “Aquisição de solução forense para coleta e extração de dados armazenados em nuvem. Aquisição de equipamento forense para coleta e extração de dados de dispositivos móveis” • “Aquisição de sistema, atualização e renovação de licença, e renovação de garantia de equipamento para extração de dados de aparelhos móveis (telefones celular, tablets, etc.) para o Laboratório de Análise Forense Computacional do Ministério Público do Estado do Rio Grande do Norte.”
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED 4PC • UFED Touch2
Sergipe	Secretaria de Estado de Segurança Pública	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de Solução para Extração de Dados Forenses”
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “UFED”



Tabela 6: Distribuição de contratos na Região Sudeste

Estado	Responsável pela compra	Fabricante (Revendedor)	Ferramenta
Espírito Santo	Secretaria de Estado da Segurança Pública e Defesa Social	Desconhecido (Apura Comércio de Softwares e Assessoria em Tecnologia da Informação)	<ul style="list-style-type: none"> “Aquisição de Solução Tecnológica Destinada à Extração e Análise de Dados de Dispositivos Móveis”
		Micro Systemation AB (MSAB) (Apura Comércio de Softwares e Assessoria em Tecnologia da Informação)	<ul style="list-style-type: none"> XRY Office PinPoint XRY Cloud XMAN Spotlight XMAN Horizon
Minas Gerais	Ministério Público - MG	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Equipamentos e licenças de uso de software para realização de exame digital em celulares, mídias de armazenamento e nuvem.”
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Cellebrite”
	Polícia Militar	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED 4PC UFED Touch2 UFED Cloud UFED Analytics
		Magnet Forensics (Techbiz Forense Digital)	<ul style="list-style-type: none"> Magnet Axiom
		Exterro / AccessData (Techbiz Forense Digital)	<ul style="list-style-type: none"> Forensic Toolkit (FTK)
		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de equipamentos e licenças de uso de software para realização de exame digital em celulares, mídias de armazenamento e nuvem.”
	Secretaria de Estado de Fazenda	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED 4PC
	Secretaria de Estado de Justiça e Segurança	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED 4PC UFED Touch UFED Analytics Desktop UFED Cloud



	Corregedoria da Polícia Militar	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de Extratores de Celulares para uso Forense”
	Departamento Estadual de Investigações Criminais	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de equipamento de licença de uso de software para extração de dados e análise forense em dispositivos móveis.”
	Departamento de Operações Policiais Estratégicas	Verint Systems (Cognyte Brasil)	<ul style="list-style-type: none"> GI2
São Paulo	Departamento de Polícia Judiciária da Macro São Paulo	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de 01 Equipamento e Licença de Software para Extração de Dados e Análise Forense em Dispositivos Móveis, Extração de Dados na Nuvem e Análise de Vínculo entre Dispositivos”
	Departamento de Polícia Ministério Público - SP	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Solução para Extração, Análise e Indexação”
		Micro Systemation AB - MSAB (Apura Comércio de Softwares e Assessoria em Tecnologia da Informação)	<ul style="list-style-type: none"> XRY
		OpenText (Techbiz Forense Digital)	<ul style="list-style-type: none"> EnCase Forensic
São Paulo	Ministério Público - RJ	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de 04 Unidades de Solução de Extração e Análise de Dados de Dispositivos Móveis, com Vistas ao Aparelhamento do Laboratório de Perícias Forenses da CSI”
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED Touch UFED 4PC UFED Analytics
	Secretaria de Estado de Polícia Civil	Secretaria de Estado de Polícia Civil Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Contratação de solução de extração, processamento e análise de dados a partir de plataformas eletrônicas portáteis para unidades da Polícia Civil” “Contratação de Solução para Extração, Processamento e Análise de Dados a partir de Plataformas Eletrônicas Portáteis, Serviços de Computação em Nuvem (Cloud), Imagens de Vídeo e Artefatos de Internet”
		Magnet Forensics (Techbiz Forense Digital)	<ul style="list-style-type: none"> Magnet Axiom
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> Cellebrite (Techbiz Forense Digital)



Tabela 7: Distribuição de contratos na Região Centro-Oeste

Estado	Responsável pela compra	Fabricante (Revendedor)	Ferramenta
Distrito Federal	Ministério Público - DF	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Solução de Extração e Análise de Dispositivos Móveis e Processamento de Dados a partir de 02 Serviços de Computação em Nuvem (Cloud). Solução de Processamento e Análise de Dados de Plataformas 03 Eletrônicas Portáteis e Serviços De...”
	Seção de Perícias de Informática do Instituto de Criminalística PCDF	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED Touch
		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Aquisição de solução avançada para Quebra de Senha de Dispositivos Móveis (smartphones) para ser utilizada por peritos criminais” “Contratação de solução e tecnologia da informação que possibilite a extração forense de dados armazenados em nuvem com a utilização de credenciais de usuário obtidas em exames periciais”
Goiás	Ministério Público - GO	Magnet Forensic (Techbiz Forense Digital)	<ul style="list-style-type: none"> Internet Evidence Finder
		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> “Contratação de solução forense para extração de dados de dispositivos móveis e computacionais.”
	Superintendência da Polícia Técnico-Científica (SPTC)	Micro Systemation AB (MSAB) (Apura Comércio de Softwares e Assessoria em Tecnologia da Informação)	<ul style="list-style-type: none"> XRY Office PinPoint
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> UFED Ultimate



Goiás	Ministério Público - MT	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Cloud • UFED Premium • UFED Pathfinder • UFED Touch • UFED 4PC
		Desconhecido (Techbiz Forense Digital)	• “Sistema para extração e análise forense de equipamentos computacionais portáteis e de telefonia celular.”
		OpenText (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Encase Forensic
	Procuradoria Geral de Justiça	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Cloud • UFED Premium • UFED Touch • UFED 4PC
		Desconhecido (Techbiz Forense Digital)	• “Aquisição do sistema para extração e análise forense de equipamentos computacionais portáteis e de telefonia celular, de acordo com as especificações, quantidades e demais condições”
		OpenText (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Encase Forensic
	Secretaria de Estado de Fazenda	OpenText (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Encase Forensic
	Secretaria de Estado de Segurança Pública	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED • UFED 4PC
		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de 01 sistema de extração e análise forense de equipamentos computacionais portáteis e de telefonia celular, 01 equipamento de duplicação e bloqueio de escrita de mídias de armazenamento computacional e 01 software para perícia forense computacional em artefatos de internet. • Aquisição de equipamento pericial especializado em extração de dados de smartphones, celulares e dispositivos de armazenamento para a Diretoria Metropolitana de Criminalística da POLITEC, mediante Inexigibilidade”
		Magnet Forensic (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Magnet Axiom
		Micro Systemation AB - MSAB (Apura Comercio de Software e Assessoria em Tecnologia da Informação)	• “Aquisição de licenças da solução MSAB para extração e análise forense de dados de dispositivos móveis”



Mato Grosso do Sul	Fundo Estadual de Segurança Pública	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Cloud • UFED Premium • UFED Pathfinder • UFED Touch • UFED 4PC
	Ministério Público - MS	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Premium • UFED 4PC

Tabela 8: Distribuição de contratos na Região Sul

Estado	Responsável pela compra	Fabricante (Revendedor)	Ferramenta
Paraná	DEPEN - Departamento Penitenciário - SESP	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de leitor de dispositivos móveis com fornecedor exclusivo. Renovação de licenças de equipamentos de extração e análise de dados de celulares e outros dispositivos de armazenamento para atender as necessidades do Departamento Penitenciário - DEPEN”
	DPC-Departamento de Polícia Civil - SESP	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED 4PC • “UFED” • UFED Cloud • UFED Pathfinder • Cellebrite Advanced Services
		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de Soluções Tecnológicas (Hardwares, Softwares e Licenças de Uso) Compatíveis Entre Si, Para Quebra de Senhas, Extração, Análise, Exame Digital e Cruzamento de Dados e Informações de Dispositivos Móveis, Plataformas Portáteis e Nuvem.”
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “UFED” • UFED 4PC • UFED Touch
	IC-SESP-Instituto de Criminalística - SESP	Exterro / AccessData (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Forensic Toolkit
		Magnet Forensic (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Magnet Axiom • Internet Evidence Finder



	Colegiado Superior de Segurança Pública e Perícia Oficial	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Touch • UFED 4PC • UFED Analytics
Santa Catarina	Ministério Público - SC	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Renovação de Licenças de Softwares Forenses para Extração e Análise de Dados” • “Solução gerenciada para extração, processamento e análise de dados a partir de plataformas eletrônicas portáteis e serviços de computação em nuvem (cloud). Solução para extração e análise de dados a partir de serviços de computação em nuvem (Cloud); Solução central de gerenciamento e Serviços avançados de desbloqueio e extração de dados, em laboratório forense, a partir de dispositivos móveis bloqueados por senha.”
	Secretaria de Estado da Segurança Pública	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Cellebrite” • UFED Touch • UFED Cloud • UFED Pathfinder • Cellebrite Advanced Services
		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de Solução Tecnológica para Extração e Análise de Dados para Polícia Civil” • “Aquisição de solução tecnológica para coleta, processamento e apoio na análise de dados e informações a partir de plataformas eletrônicas portáteis, tais como smartphones, tablets, aparelhos de GPS, cartões de memória e cartões SIM, para atender as necessidades das unidades policiais da Delegacia Regional de Polícia de São Miguel do Oeste”
Rio Grande do Sul	Colegiado Superior de Segurança Pública e Perícia Oficial	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Touch • UFED 4PC Ultimate • UFED Analytics
	Ministério Público - RS	Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • UFED Touch • UFED 4PC
		OpenText (Techbiz Forense Digital)	<ul style="list-style-type: none"> • Encase Forensic
	SSP - Gabinetes e Órgãos Centrais	Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “ Aquisição de 05 Unidades da Ferramenta Forense P/ Extração, Processamento e Apoio na Análise de Dados e Informações. Aquisição de Software”



	SSP - Gabinetes e Órgãos Centrais	Desconhecido (Techbiz Forense Digital)	Ferramenta Forense P/ Extração, Processamento e Apoio na Análise de Dados e Informações. Aquisição de Software”
		Cellebrite (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Cellebrite” • UFED Premium • Commander • UFED Pathfinder • UFED Cloud • UFED 4PC
SSSP - Polícia Civil		Desconhecido (Techbiz Forense Digital)	<ul style="list-style-type: none"> • “Aquisição de 5 (cinco) Unidades da Ferramenta Forense Para Extração, Processamento e Apoio Na Análise de Dados e Informações a Partir de Plataformas Eletrônicas Portáteis, Visando Ao Fortalecimento da Polícia Civil do Rio Grande do Sul” • “Aquisição de softwares de manipulação de dados e informações, conforme especificações constantes no Anexo I e demais condições previstas no presente Contrato”. • “Aquisição de 2 (duas) unidades da Ferramenta Forense para análise de correlação e vínculos”



3.4. Panorama geral dos achados

No gráfico que trabalha com a distribuição de contratos no Brasil identificamos dados mais consistentes. Destaca-se no mapa como a região Sudeste desonta como líder na aquisição de ferramentas de hacking, número puxado pelas aquisições de ferramentas por parte de Minas Gerais (22) e Rio de Janeiro (19). Nas demais regiões, os estados federativos que se acentuaram na coleta de dados foram também Mato Grosso, com 19 contratos, Rio Grande do Sul, com 13, e Amapá com 12 contratos.¹¹³

Ferramentas como Cellebrite, destinada a extração de dados com os aparelhos em mãos, demonstram uma capilaridade significativa em órgãos de segurança pública. A inserção se dá, especialmente, em órgãos voltados para investigação, como Polícia Civil, Ministérios Públicos e setores de criminalística. Ainda assim, identificou-se que em estados como Paraíba e Minas Gerais esses tipos de soluções estão alocadas na Polícia Militar, órgão que não possui função de investigação. No caso de São Paulo, fomos também capazes de identificar que um aparelho voltado para extração de dados está no setor de Corregedoria da Polícia Militar, responsável por investigação, análise e solução de infrações ou crimes realizados por policiais militares, ou seja, a finalidade da ferramenta sugere que seria destinada para coletar provas dos dispositivos pessoais de policiais investigados.

No que concerne à capilaridade das ferramentas de acesso remoto da Verint, observamos que essas soluções são adquiridas em grande maioria pelo Ministério da Defesa. Em casos como a Intervenção Federal no Rio de Janeiro, em 2016, as ferramentas que foram adquiridas não foram reveladas. Para os casos que foram adquiridos pelos Governos Estaduais, não parece haver uma padronização. Localizadas no Amazonas, Pará, Mato Grosso, São Paulo e Alagoas, a solução foi adquirida pela Polícia Civil, com emprego de fundos penitenciários para efetuar a compra.

Vale salientar ainda que diversos portais contém informações incompletas acerca das ferramentas adquiridas, dificultando a mensuração do quantitativo de produtos e serviços adquiridos e disponíveis em cada estado. O déficit de informações é também qualitativo, visto que, muitas vezes, sequer há descrição no contrato sobre produto ou serviço adquirido. O mesmo vale para contratos com entes federais, ficando difícil saber o quê e quanto foi adquirido. Nesse sentido, como descrito, vários contratos encontrados nos Portais de Transparência foram objeto de Pedidos de Acesso à Informação e, em vários casos, ainda assim não foram disponibilizadas as informações acerca das compras feitas pela administração pública.

No que concerne ao investimento ao longo dos anos, sobressai o crescimento contínuo dos investimentos em tecnologias de extração de dados para fins de persecução penal e inteligência. No caso dos recursos estaduais, observa-se a evolução de 522 mil reais investidos, em 2015, para mais de 45 milhões de reais em 2021. A nível federal, se observa uma evolução de 5.720.225,07 reais em 2016, para 54.551.313,26 reais em 2020, com um decréscimo substantivo em 2021.¹¹⁴

Além disso, somos capazes de analisar o quantitativo de contratos da administração pública federal e estadual, respectivamente, e as empresas privadas contratadas. No caso federal, a Techbiz é a fornecedora de pouco mais de 70% dos contratos, enquanto que, no âmbito estadual, a mesma empresa detém um quantitativo dos contratos superiores, dominando o mercado de hacking. No caso federal,

113 Importante sinalizar que algumas discrepâncias no número de contratos encontrados podem se referir muito mais à dificuldade de se trabalhar com Portais de Transparência e Lei de Acesso à Informação do que uma ausência dessas ferramentas nos estados que possuem um baixo quantitativo.

114 O decréscimo para o ano de 2021 demanda análises adicionais. O investimento na área para esse ano é de cerca de R\$ 9.000.000,00, uma queda de quase R\$ 46.000.000,00. Uma hipótese levantada é do número ser resultado de deficiências e/ou atraso na inserção de dados na plataforma de transparência. Outra hipótese se relaciona com o sigilo crescente sobre informações relativas à contratação de ferramentas. Vale salientar que alguns dos principais contratos do ano de 2021 só foram fechados nos últimos dias do ano, como é o caso do contrato de aquisição das 30 licenças permanentes do Projeto Excel, do Ministério da Justiça e Segurança Pública.



observa-se contratos maiores, como é o caso dos contratos relacionados ao Projeto Excel, que será analisado mais à frente.

É interessante notar como essas ferramentas são apresentadas no campo midiático. Crimes de grande comoção nacional são um dos momentos nos quais aparelhos, como Cellebrite, ganham bastante destaque na imprensa. Não é raro que a imprensa realize apresentações sobre a funcionalidade e seus “feitos”, como observado em 2021 com o assassinato de Henry Borel.¹¹⁵ O otimismo frente ao uso de ferramentas de hacking é observado em esferas governamentais, nos quais promovem o Projeto Excel, por exemplo, como grande vitória frente ao crime organizado.¹¹⁶ Essa perspectiva é igualmente fortalecida pelas próprias empresas desenvolvedoras das ferramentas. Como forma de publicidade, a Cellebrite destaca a parceria com a Polícia Federal, na qual é assinalada o papel do ex-delegado Elvis Secco que equipou o Grupo Especial de Investigações Sensíveis (GISE) com ferramentas da empresa israelense, apreendendo grande aportes financeiros de lideranças do crime organizado.¹¹⁷ Outro espaço importante para essa construção narrativa são os próprios flyers das empresas, nos quais constantemente se reforçam noções de agilidade e eficiência no processo investigativo.¹¹⁸

3.4.1. Olhando de perto: o caso da Cellebrite e Techbiz Forense Digital

Chama atenção, especialmente, o protagonismo de um representante comercial específico que figura em grande parte dos achados, a Techbiz Forense Digital. Representante de fabricantes como Cellebrite, Opentext, Magnetic Forensics e Exterro/AccessData, faz a linha de frente na participação de contratações com a administração pública para o fornecimento de ferramentas de hacking e figura como uma grande fiadora e intermediária das tecnologias para fins de investigação atualmente vigentes no país, tendo como clientes desde os Ministérios Públicos e Secretarias de Segurança Estaduais ao próprio Ministério da Justiça. Segundo matéria do Intercept, a empresa possui mais de uma centena de contratos com a administração pública estadual e federal, somando mais de 100 milhões desde 2018.

Em artigo recente publicado por seu diretor comercial, Rafael Velasquez¹¹⁹ o uso massivo de smartphones, “ambientes colaborativos” e comunicações via Internet’ são grandes oportunidades para as investigações e o conjunto de evidências envolvem computadores pessoais e servidores (e-mail, arquivos apagados, decriptação de arquivos e histórico de Internet), dispositivos móveis (WhatsApp, drones, Telegram, e-mail, Viber, WeChat etc), redes e sistema CFTV (tráfego de rede, câmeras de vigilância e reconhecimento facial), nuvem (Office 365, Dropbox, Google Suite, Sharepoint, OneDrive etc) e Internet das Coisas. Logo, as habilidades de hacking oferecidas pela Techbiz são ilustrativas do “estado da arte” investigativo na atualidade: sendo a empresa a maior fornecedora do mercado nacionalmente, denun-

115 G1. **O QUE é o software usado pela polícia do Rio para investigar celulares no caso Henry Borel.** G1, 2021. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/2021/04/08/o-que-e-o-software-usado-pela-policia-do-rio-para-investigar-celulares-no-caso-henry-borel.ghtml>. Acesso em 27 de julho de 2022.

116 BRAGA, Juliana. **Projeto tecnológico tirou R\$ 1 bi do crime organizado, diz Ministério da Justiça.** Folha de São Paulo, 2022. Disponível em <https://www1.folha.uol.com.br/columnas/painel/2022/02/programa-do-ministerio-da-justica-ajuda-a-recuperar-r-1-bi-do-crime-organizado.shtml>. Acesso em 27 de julho de 2022.

117 JAFFE, Adam. **Milhões em bens apreendidos à medida que a Polícia Federal do Brasil se dedica a desmascarar chefes do tráfico de drogas.** Cellebrite, 2021, Disponível em: <https://cellebrite.com/pt/milhoes-em-bens-apreendidos-a-medida-que-a-policia-federal-do-brasil-se-dedica-a-desmascarar-chefes-do-trafico-de-drogas/>. Acesso em 22 de julho de 2022

118 MAGNET FORENSICS. **Magnet AXIOM: Recover and analyze your evidence in one case.** 2022. Disponível em https://cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf https://go.magnetforensics.com/AXIOM_Product_Brief. Acesso em 22 de julho de 2022; CELLEBRITE. **Cellebrite UFED: Product Overview.** 2020. Disponível em https://cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf. Acesso em 26 de maio de 2022.

119 VELASQUEZ, Rafael. **Desafios da investigação criminal tecnológica.** Techbiz Forense Digital, 2022. Disponível em <https://techbiz.com.br/wp-content/uploads/2022/06/Artigo-Desafios-da-investigacao-criminal-tecnologica.pdf>. Acesso em 22 de julho de 2022



cia que qualquer dispositivo, aplicação, protocolo de segurança, incluindo bloqueio de tela ou serviço por código PIN, senha pessoal, biometria, criptografia de disco ou de tráfego de dados, de uso pessoal ou coletivo, é passível de acesso. É igualmente deduzível que um único acesso a um dispositivo pessoal provê a possibilidade um nível inédito de dados pessoais e comunicações, possibilitando traçar perfis de cidadãos a partir do cruzamento inúmeros “data points” provenientes de dados de naturezas consideravelmente distintas (localização, rastreamento de interações, buscas de pesquisa, conteúdo de comunicações, likes, fotos e vídeos, dados cadastrais, biometria e tantos outros).

Principal fabricante de soluções de extração de dados com atuação no Brasil através da Techbiz, a Cellebrite tem sede em Israel e especializou-se na produção de uma ferramenta intitulada Universal Memory Exchange (UME), capaz de extrair e transferir dados entre dois aparelhos, assim como fazer backup, restaurar e sincronizar dados.¹²⁰ Os UME começaram a ser vendidos para agências de investigação em 2006 para extração de dados e geração de pistas investigativas. Como o material coletado não tinha parâmetros necessários para ser considerado prova em sede de investigação, a empresa foi levada a criar um ramo de soluções forense. Em 2007, a Cellebrite lança o primeiro UFED, aparelho principal no catálogo oferecido às forças de segurança.¹²¹

Alguns pontos merecem destaque no que diz respeito à proteção de dados pessoais dos usuários cujos dados são extraídos mediante essas soluções. O primeiro deles se refere ao acesso a dados de investigações por parte das empresas fabricantes: ainda que a Techbiz afirme que, por exemplo, “a empresa [Cellebrite] não tem acesso a quaisquer informações sobre as operações policiais”,¹²² o próprio descriptivo de serviços como o “Cellebrite Advanced Services” descreve: “Descarregue casos de rotina e alivie os acúmulos ao permitir que os nossos especialistas extraiam e decodifiquem os dados para você. Envie dispositivos compatíveis pelo UFED e receba uma unidade USB com os dados.”¹²³ Ou seja, invariavelmente, dados de investigações têm que passar pelas mãos da Cellebrite, a qual coleta, trata e compartilha (e descarta?) dados pessoais de um suposto investigado e dos usuários que estejam em sua rede de conexões. Ainda sobre o descaso com protocolos de segurança dos dados extraídos, vem sendo reportado no campo internacional que ferramentas da Cellebrite são vendidas em mercados clandestinos ainda com bancos de informações sensíveis sobre investigações realizadas.¹²⁴

Adicionalmente, é sintomática a narrativa da Cellebrite no incentivo ao desvio do devido processo legal intermediado pela requisição de dados aos provedores de aplicação: “afaste a dependência de provedores de serviços para rapidamente coletar dados de usuários ao utilizar tokens extraídos de dispositivos digitais ou credenciais de usuários.”¹²⁵ Como descrito no tópico 2.3.2, o corte do intermediário na busca pelo acesso a dados em investigações abre margem para o rompimento de uma relação de confiança mínima entre usuário e provedor, retrocedem quanto a procedimentos historicamente estabelecidos para uma governança de dados segura e colocam em risco sistemas de segurança que podem comprometer a coletividade de usuários. Isso não impede, contudo, que os dados recebidos via mandados aos provedores também sejam tratados conjuntamente com os dados extraídos, segundo a própria

120 ZETTER, Kim. **When the FBI has a phone it can't crack, it calls these Israeli hackers.** The Intercept, 2016. Disponível em [https://theintercept.com/2016/07/12/cellebrite-hackers-fbi/](#)

121 NURICK, Ori. **The Solution That Changed Modern Digital Investigations Forever.** Cellebrite Blog, 2021. Disponível em [https://www.cellebrite.com/the-solution-that-changed-modern-digital-investigations-forever/](#)

122 AMENO, Fernando. **Op. cit.**

123 Ver CELLEBRITE. **Extração e desbloqueio avançados: Cellebrite Advanced Services.** 2020. Disponível em [https://www.cellebrite.com/advanced-data-extraction-and-unlocking/](#)

124 BREWSTER, Thomas. **The Feds' Favorite iPhone Hacking Tool Is Selling On eBay For \$100—And It's Leaking Data.** Forbes, 2019. Disponível em [https://www.forbes.com/sites/thomasbrewster/2019/02/27/the-feds-favorite-iphone-hacking-tool-is-selling-on-ebay-for-100-and-its-leaking-data/#:~:text=The%20Feds%27%20favorite%20iPhone%20hacking,of%20the%20UFED%20Cloud%20to%20the%20UFED%20Tool%20itself.](#)

125 Ver Cellebrite. **Cellebrite UFED CLOUD: Product Overview.** 2020. Disponível em [https://cellebrite.com/wp-content/uploads/2020/06/UFED_CLOUD_Product_Overview.pdf](#)



Cellebrite.¹²⁶

A interpretação sobre o regime de proteção de dados pessoais da própria Cellebrite induz o agente investigativo ao acúmulo de dados. A empresa considera, por exemplo, dados provenientes de redes sociais como Facebook, Instagram e Twitter como “dados públicos”, passíveis de “captura”, além de ter uma solução, inclusive, para “evidências que não seriam admissíveis em tribunal”,¹²⁷ concluindo que o UFED Cloud seria a ferramenta apropriada. Outra ferramenta, a UFED Pathfinder, utiliza algoritmos de machine learning para a identificação de objetos e pessoas, levando a conclusão que treina o próprio recurso a partir de dados pessoais sensíveis de titulares de dados constantes nos dispositivos analisados, em violação às bases legais para o tratamento de dados pessoais da LGPD.

A capilaridade das ferramentas na administração pública chega a apontar a existência de ferramentas de extração de dados em órgãos que, tipicamente, não conduzem investigações criminais mediante técnicas forenses com tecnologia de ponta. É o caso da existência de contrato para aquisição de um UFED Touch pelo Conselho Administrativo de Defesa Econômica (CADE), órgão tipicamente responsável por, entre outras atribuições, conduzir processos administrativos e promoção de políticas em matéria concorrencial.¹²⁸ O relatório de gestão da entidade para o ano de 2021 reafirma a aquisição da ferramenta para a “persecução de infrações à ordem econômica”, no valor de mais de meio milhão de reais.¹²⁹

3.4.2. Olhando de perto: o caso da Verint Systems (Cognite/Suntech)

A multiplicação de representações jurídicas de fornecedores de ferramentas de hacking é uma transversal no circuito comercial dessas ferramentas no Brasil - e um dos resultados diretos é o desafio em traçar a trilha dos CNPJs que acompanham essas tecnologias. O caso da Verint exemplifica: foram encontrados contratos da “Verint” a partir da sua subsidiária nacional, Suntech, em negociações com o Fundo Penitenciário do Estado de Alagoas e com a Polícia Civil do Pará; contrato da Cognite, ramificação da Verint para produtos relacionados à “defesa e cibersegurança”, com o Departamento de Operações Policiais Estratégicas do Estado de São Paulo; e da Verint propriamente dita com, por exemplo, a Polícia Civil do Distrito Federal. A Suntech, recentemente, ainda teve seu nome atualizado para Cognite Brasil.

A Verint - incluindo suas representações locais em outros países - tem sido alvo de denúncias internacionais por fornecer tecnologias de interceptação de comunicações “em campo” para países com regime autoritário. Relatório da Anistia Internacional¹³⁰ documentou que a Israel Verint Systems Ltd, subsidiária da Verint Systems Inc., forneceu equipamentos de interceptação de comunicações ao governo do Sudão do Sul, o qual vem sistematicamente utilizando o conteúdo de comunicações interceptadas, assim como dados coletados de redes sociais, para prender arbitrariamente e constranger jornalistas e defensores de direitos humanos. O mesmo cenário de monitoramento sobre comunicações tem sido

126 LORENTZ, Paul. **Warrant Returns: What They Are, Challenges Involved, and How to Leverage Their Data**. Cellebrite Blog, 2022. Disponível em: <https://cellebrite.com/en/warrant-returns-what-they-are-challenges-involved-and-how-to-leverage-their-data/>. Acesso em 28 de julho de 2022.

127 Cellebrite. **Cellebrite UFED CLOUD: Product Overview**. Disponível em: <https://cellebrite.com/pt/cellebrite-ufed-cloud-pt/>. Acesso em 28 de julho de 2022

128 BRASIL. GOVERNO FEDERAL. **Conselho Administrativo de Defesa Econômica (CADE)**. Disponível em <https://www.gov.br/pt-br/orgaos/conselho-administrativo-de-defesa-economica>. Acesso em 22 de juho de 2022.

129 PEREIRA et al. **Relatório Integrado de Gestão do Conselho Administrativo de Defesa Econômica (Cade) - Exercício 2021**. 2022. Disponível em https://cdn.cade.gov.br/Portal/acesso-a-informacao/Transpar%C3%A3ncia%20e%20Presta%C3%A7%C3%A3o%20de%20Contas/Relat%C3%B3rio%20Integrado%20de%20Gest%C3%A3o%202021_2.pdf. Acesso em 22 de julho de 2022.

130 ANISTIA INTERNACIONAL. **“These walls have ears”: The chilling effect of surveillance in South Sudan**. 2021. Disponível em <https://www.amnesty.org/en/documents/afr65/3577/2021/en/>. Acesso em 22 de julho de 2022.



reportado sobre as relações da Verint com países com longo histórico de repressão a dissidentes, como o Cazaquistão e o Usbequistão, segundo a Privacy International.¹³¹

Segundo o Portal de Transparência, a Verint está entre as 10 maiores empresas favorecidas com a intervenção militar no Rio de Janeiro (mais de R\$1.700.000).¹³² Reportagem do Brasil de Fato, no entanto, aponta para a Verint como a maior favorecida, com mais de 40 milhões arrecadados pela empresa no “fornecimento de soluções de segurança de dados e espionagem”.¹³³ Em relatório do Exército de 2015, já eram citadas contratações com a Verint para aquisição de Medidas de Apoio à Guerra Eletrônica (MAGE).¹³⁴

Mais recentemente, foi revelado¹³⁵ que a ferramenta GI2 da empresa, cujo contrato é encontrado sob alçada da Polícia Civil do Pará, firmado sem licitação e custando R\$ 5 milhões, foi utilizada no esquema do ora governador do Pará, Helder Barbalho, para espionar investigadores de esquema de corrupção na compra de respiradores, durante a Covid-19, pelo Governo do Estado. Segundo o Ministro Francisco Falcão, relator do caso do Superior Tribunal de Justiça, “confirmou-se que o dispositivo é capaz de extrair dados de aparelhos telefônicos, interceptar diálogos criptografados e fazer gravações ambientais, tudo sem autorização judicial, podendo os dados ser apagados facilmente, não deixando rastro sobre sua utilização”. Em outra investigação da Polícia Federal, a Operação Chabu,¹³⁶ um dos sócios da Sutech, José Augusto Alves, foi preso por ser suspeito de ser o articulador central, junto com dois delegados e um policial rodoviário federal, de um esquema de vazamento de informações sigilosas de investigações criminais a políticos investigados em troca de benefícios, incluindo a venda de produtos da Suntech.

A posição da Verint e das empresas a ela vinculadas, associadas ao contexto político em que se colocam, ajudam a evidenciar a margem de abusos que se amplia a partir da aproximação da indústria de ferramentas de hacking com os órgãos de segurança pública e vigilância no Brasil.

3.5. Muito a esconder: a cultura do sigilo sobre as ferramentas de hacking

Como descrito, duas estratégias de coleta de informações foram acionadas: uma através dos Portais da Transparência e outra através dos Serviços de Informação ao Cidadão (SIC) dos Estados, da União e dos Ministérios Públicos Estaduais e Federal, com base na Lei de Acesso à Informação Nesse último caso, observamos uma tendência à declaração de sigilo para grande parte das informações sobre a contratação, para as condições processuais, de armazenamento e de uso dessas ferramentas.

131 PRIVACY INTERNATIONAL. **Private interests: monitoring Central Asia.** 2014. Disponível em https://privacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf. Acesso em 22 de julho de 2022.

132 GOVERNO FEDERAL. PORTAL DE TRANSPARÊNCIA. **AÇÕES DECORRENTES DA INTERVENÇÃO FEDERAL NO ESTADO DO RIO DE JANEIRO NA ÁREA DE SEGURANÇA PÚBLICA (DECRETO N. 9.288, DE 16 DE FEVEREIRO DE 2018).** Disponível em <https://www.portaltransparencia.gov.br/programas-e-acoes/acao/00QS-acoes-decorrentes-da-intervencao-federal-no-estado-do-rio-de-janeiro-na-area-de-seguranca-publica-decreto-n-9-288-2018>. Acesso em 22 de julho de 2022.

133 DEISTER, Jaqueline. **Intervenção militar: 10 meses depois, medida segue sem solução para a segurança no RJ.** Brasil de Fato RJ, 2018. Disponível em <https://www.brasildefatorj.com.br/2018/12/06/intervencao-militar-10-meses-depois-medida-segue-sem-solucao-para-a-seguranca-no-rio>. Acesso em 22 de julho de 2022.

134 <http://www.cciex.eb.mil.br/images/pca/2014/160085pca2014.pdf>

135 DANTAS, Claudio. **EXCLUSIVO: A empresa que vendeu a ‘maleta hacker’ para o esquema de Helder Barbalho.** O Antagonista, 2020. Disponível em <https://oantagonista.uol.com.br/brasil/exclusivo-a-empresa-que-vendeu-a-maleta-hacker-para-o-esquema-de-helder-barbalho/>. Acesso em 22 de julho de 2022.

136 G1. **Operação Chabu: Prefeito de Florianópolis e mais seis são denunciados por organização criminosa.** 2020. Disponível em <https://g1.globo.com/sc/santa-catarina/noticia/2020/02/07/prefeito-de-florianopolis-e-mais-seis-pessoas-sao-denunciadas-por-organizacao-criminosa.ghtml>. Acesso em 22 de julho de 2022.



3.5.1. Recursos empregados para negar acesso às informações

As leis comumente usadas para negar acesso a informações solicitadas via SIC são a Lei nº 9.883/1999, que institui o Sistema Brasileiro de Inteligência (Sisbin) e a Agência Brasileira de Inteligência, estipulando que, em seu Art. 3º, parágrafo único, “as atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos (...);”¹³⁷ a Lei nº 12.850/2013 (Lei das Organizações Criminosas), Art. 3º, § 1º, sobre a necessidade de proteção pelo Estado de sua capacidade investigatória através da manutenção e guarda de sigilo sobre suas metodologias, recursos técnicos e atividades especializadas;¹³⁸ a própria Lei nº 12.527/2011 (Lei de Acesso à Informação), a qual admite exceções à transparência com base no Art. 23, inciso VIII, apontando a exceção visando à preservação de “atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações”;¹³⁹ e, finalmente, a Política Nacional de Inteligência, instituída pelo Decreto 8.793/2016, regulamentando a Lei 9883/99, reafirmando que as “atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado.”¹⁴⁰

Nas tabelas abaixo, apresentamos objetivamente informações acerca das respostas dadas pelos órgãos públicos em relação às questões sobre parâmetros de segurança, condições processuais e regras de cadeia de custódia referentes ao uso de tecnologias de hacking.

137 GOVERNO FEDERAL. LEI N° 9.883, DE 7 DE DEZEMBRO DE 1999 (Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9883.htm. Acesso em 22 de julho de 2022.

138 GOVERNO FEDERAL. LEI N° 12.850, DE 2 DE AGOSTO DE 2013 (bre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em 22 de julho de 2022.

139 GOVERNO FEDERAL. LEI N° 12.527, DE 18 DE NOVEMBRO DE 2011 (Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências). Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 22 de julho de 2022.

140 GOVERNO FEDERAL. DECRETO N° 8.793, DE 29 DE JUNHO DE 2016 (Fixa a Política Nacional de Inteligência). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm. Acesso em 22 de julho de 2022.



Tabela 9: Resultados das perguntas a Órgãos Federais

Ente	Parâmetros de segurança	Condições processuais	Regras de cadeia de custódia	Resumo
MJSP	A informação se refere “às padronizações técnicas internacionais recomendadas pela ISO/IEC 27042:2015 - Técnicas de segurança - diretrizes para a análise e interpretação de evidências digitais e ABNT NBR ISO/IEC 27037 - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.” Negado acesso ao “instrumento jurídico e os parâmetros de segurança” com base na Política Nacional de Inteligência, item 2.4; Lei nº 12.527/2011 (LAI), arts. 22 e 23, VIII; Lei 2.850/2013 (Lei das Org. Criminosas), art. 3, § 1, e 23º.	“Quanto à indagação relacionada ao instrumento jurídico que baseie as condições processuais para o uso de ferramentas de desbloqueio e extração de dados, tais informações podem ser acessadas no link http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm [Código de Processo Penal] e legislação penal correlata, uma vez que a implementação do Projeto pelos Estados aderentes se dá por meio do exercício regular das suas atividades de polícia judiciária.”	As informações constam “nos artigos 158 a 181 do Código de Processo Penal Brasileiro, uma vez que o uso das ferramentas de desbloqueio e extração mencionadas nos questionamentos se dá mediante exercício regular das suas atividades de polícia judiciária.” O fornecimento dos “instrumento jurídico e os parâmetros de segurança” com base na Política Nacional de Inteligência, item 2.4; Lei nº 12.527/2011 (LAI), arts. 22 e 23, VIII; Lei 2.850/2013 (Lei das Org. Criminosas), art. 3, § 1, e art. 23º.	O pedido foi parcialmente atendido. A resposta, que negava parte das informações solicitadas, segue o mesmo padrão das respostas de vários Estados, sendo praticamente idênticas.
GSI	Não existe instrumento administrativo “por não haver celebrado nenhum contrato nesse sentido”.			Pedido respondido.
PF	A questão não foi respondida. Adicionalmente, o Pedido de Acesso à Informação foi encaminhado para vários órgãos da Polícia Federal, cujas respostas, algumas vezes, não informavam a qual item se referia, e nenhuma endereçou os parâmetros de segurança.	A Diretoria de Inteligência informou que “as ferramentas são as previstas no Código de Processo Penal, a Lei do Crime organizado (LEI Nº 12.850, DE 2 DE AGOSTO DE 2013) e a Lei de interceptação telefônica (LEI Nº 9.296, DE 24 DE JULHO DE 1996)”	A Corregedoria-Geral da Polícia Federal negou acesso às informações sobre cadeia de custódia com base na ausência de previsão sobre isso na Instrução Normativa nº153-DG/PF/2020, “que instituiu a Política de Transparência Ativa e Dados Abertos da Polícia Federal, estabeleceu as atribuições de cada Diretoria da PF”.	Dentre as justificativas sem direcionamento expresso para itens específicos das perguntas, a Diretoria de Tecnologia da Informação e Inovações justificou a negativa de acesso à informação com fundamento na Lei Nº 12.527, artigo 23, inciso VII.
MD	A resposta informa que “esta Pasta não possui registro de contratação e uso de tecnologias de desbloqueio, extração de dados e acesso remoto”.			Pedido respondido, porém sem resultado. Foi apontada a autonomia administrativa das forças militares.
MPF	As questões sobre parâmetros de segurança da informação, condições processuais de uso das ferramentas e regras de cadeia de custódia não foram abordadas diretamente na resposta enviada pelo MPF.			Pedido respondido, porém sem resultado.



Tabela 10: Resultados das perguntas a Secretarias de Segurança Pública Estaduais

	Parâmetros de segurança	Condições processuais	Regras de cadeia de custódia	Resumo
AC	O pedido foi encaminhado para Polícia Civil do Acre e está tramitando desde 02/02/2022, e permaneceu sem resposta até 19/08/2022.			Pedido não respondido.
AL	O pedido foi encaminhado para o Instituto de Tecnologia em Informática e Informação (ITEC), o qual não tem relação com o objeto do Pedido de Acesso à Informação (PAI). O site do SIC de Alagoas está com os certificados revogados, dificultando o acesso e o acompanhamento do PAI.			O ITEC, não tem relação com atividades de persecução penal e segurança pública, não pode responder. Pedido respondido, porém sem resultado.
AP	Não houve resposta sobre parâmetros de segurança, condições processuais e regras de cadeia de custódia.			Pedido respondido, porém sem resultado.
AM	O pedido de informação foi parcialmente atendido, mas foi negado acesso a instrumentos administrativos referentes a parâmetros de segurança, condições processuais ou regras de cadeia e custódia, pois seriam “informação com natureza de atividade especializada de inteligência” e sigilosas com base nos seguintes dispositivos: Política Nacional de Inteligência, Item 2.4; Lei n 12.527/2011 (LAI), artigos 22 e 23, VIII; e Lei 12.850/2013 (Lei das Org. Criminosas), artigos 3º, § 1º, e 23.		Pedido negado parcialmente.	
BA	O pedido foi encaminhado para a Superintendência de Gestão Tecnologia Organizacional, da Secretaria de Segurança Pública, porém não foi respondido.			Pedido não respondido.
CE	O pedido foi negado, considerando as informações sigilosas com base na Portaria CGAI nº 01/2016 da Controladoria e Ouvidoria-Geral do Estado, a qual classifica as informações relacionadas à Pasta da Segurança Pública e sua operacionalidade como sigilosas, e na Lei Estadual nº 15.175/2012, que regulamenta a LAI no Ceará e dispõe sobre os deveres do Estado em proteger o sigilo de determinadas informações.			Pedido negado em sua totalidade.
DF	A resposta informa que o “Instrumento Jurídico encontra-se em fase de elaboração”	A resposta informa que as “condições processuais para o uso de ferramentas investigativas estão previstas na legislação processual e especial em vigor e são consideradas, em cada caso concreto, pelo Delegado de Polícia que formula o pedido, pelo membro do Ministério Público que opina em cada investigação e pelo juiz competente para conceder ou não a representação da autoridade policial.”	A resposta informa que o “Instrumento Jurídico encontra-se em fase de elaboração”	Pedido respondido. Enfatizamos que não havia, no momento da resposta ao pedido de informação, instrumento jurídico orientador de ferramentas que já estão em uso pelas forças de aplicação da lei do Distrito Federal.
ES	O pedido foi negado, “independentemente de classificação, com base na natureza sigilosa das informações”, com base nos seguintes dispositivos: CF 88 art 5º inciso XXXIII; Lei 12.850/12 art. 3º, § 1º; Lei 12.527/2011 (LAI), Art. 22; Lei no 9883/99 (Sistema Brasileiro de Inteligência), Artigo 2º, § 1º; Política Nacional de Inteligência, 2.4.			Pedido negado em sua totalidade.
GO	O pedido foi negado, considerando a informação solicitada como sigilosa, no nível reservado, com base na Portaria n.o 031/2020 - PCGO, Anexo II; na Lei n 12.527/11 (LAI), artigo 23, incisos III, VII e VIII, e na Lei estadual nº 18.025/13, Art. 34, inciso I. Os Termos de Classificação da Informação (TCI) foram assinados em 07/12/2021 e 23/02/2022.			Pedido negado em sua totalidade. Um dos TCI foi assinado após nossos pedidos de informação.



MA	<p>"Destacamos que seguimos as próprias orientações dos equipamentos adquiridos, bem como o treinamento específico ministrado de forma híbrida, com modalidade on line e presencial, composto de 03 módulos, cada um com 32 horas sobre o UFED, Axiom, CFTV Input Ace e CFTV DRV Examiner. Ademais, quaisquer outros parâmetros de segurança deverão ser solicitados para empresa contratada, haja vista que são sigilosos, e os desenvolvedores de ferramentas para a perícia digital não expõem suas tecnologias para preservarem o produto bem como toda a sociedade, que ficariam exposta e refém dos criminosos, caso a técnica e a segurança envolvida venha parar em mãos erradas."</p>	<p>"O Instrumento Jurídico que garante a legalidade processual das provas extraídas é a própria decisão Judicial autorizando e determinando o exame para extração de dados dos aparelhos."</p>	<p>"As regras da Cadeia de Custódia das informações, são definida pelo próprio Código de Processo Penal no Capítulo II que trata DO EXAME DE CORPO DE DELITO, DA CADEIA DE CUSTÓDIA E DAS PERÍCIAS EM GERAL, vigente no mundo jurídico de forma detalhada desde 2019, Incluídos pela Lei no 13.964."</p>	<p>Pedido respondido.</p>
MG	<p>Informação solicitada como sigilosa, com base na Lei 12.527/2012 (LAI), art. 23, inciso VIII.</p>			
MT	<p>O pedido foi negado, sem embasamento legal expresso, justificando apenas que "por questões de segurança e proteção do sigilo de dados de terceiros, fica reservada sua difusão".</p>			
MS	<p>As informações solicitadas foram consideradas de acesso restrito, com base na Portaria do MJSP n.o 880/2019, artigo 16.</p>			
PA	<p>O pedido foi encaminhado para o Gabinete do Delegado Geral do Pará, em 25/03/2022, e permaneceu sem resposta até a data de publicação deste estudo.</p>			
PB	<p>O Núcleo de Criminalística de João Pessoa informou que "Desde o ano de 2015 o Instituto de Polícia Científica da Paraíba - IPC somente realiza perícias em dispositivos tecnológicos pessoais mediante autorização pertinente - pessoal ou judicial, conforme orientação administrativa constante em ofício circular e memorando em anexo."</p>	<p>O Núcleo de Criminalística de João Pessoa informou que "desde o ano de 2015 a tomada de decisão para o procedimento deste Instituto em somente realizar perícias em dispositivos tecnológicos pessoais mediante autorização pertinente - pessoal ou judicial, segue as bases legais e jurisprudenciais constantes do Despacho CA/PGE 14/2015".</p>	<p>O Núcleo de Criminalística de João Pessoa informou que "O Instituto de Polícia Científica da Paraíba, em todos os seus cinco Núcleos, adota desde 08 de outubro de 2020 um procedimento operacional padrão referente à custódia de vestígios no âmbito do IPC conforme o documento "Procedimento Operacional Padrão nº001/DG/IPC - Recebimento, Armazenamento e Entrega de Vestígios na Central de Custódia de Vestígios - CCV" (p. 15)</p>	<p>O ped foi negado pela Gerência de Planejamento foi encaminhado para dois entes ermento da Secretaria de Estado da Segurança e da Defesa Social, a qual considerou a informação como sigilosa, segundo a Lei nº 12.527/2011 (LAI), artigo 3, inciso I, e artigo 23, inciso VIII, mas o pedido foi respondido pelo Núcleo de Criminalística de João Pessoa, do Instituto de Polícia Científica da Paraíba. Pedido respondido</p>



PR	<p>Na resposta em relação aos parâmetros de segurança e condições processuais, o respondente afirmou que “não foi possível compreender a demanda solicitada”.</p>	<p>A Ouvidoria da Polícia Científica do Paraná informou que “os equipamentos eletrônicos apreendidos, bem como os dados deles extraídos, são considerados vestígios de crimes, e, assim como quaisquer outros vestígios, seguem o que preconiza o Código de Processo Penal (Lei no 3689/1941) acerca da Cadeia de Custódia, conforme consta do CAPÍTULO II - Do Exame de Corpo de Delito, da Cadeia de Custódia e das Perícias em Geral, da referida Lei”</p>	<p>Pedido respondido.</p>	
PE	<p>A questão não foi respondida, com recusa de fornecimento dos “instrumento jurídico e os parâmetros de segurança” segundo a Política Nacional de Inteligência, item 2.4; a Lei nº 12.527/2011 (LAI), arts. 22 e 23, VIII; a Lei 12.850/2013 (Lei da Org. Criminosa), art. 3, §1, e art 23º.</p>	<p>“Quanto à indagação relacionada ao instrumento jurídico que baseie as condições processuais para uso de ferramentas de desbloqueio e extração de dados, tais informações estão fundamentadas na Constituição Federal, no Código de Processo Penal Brasileiro e legislação correlata”</p>	<p>A questão não foi respondida, com recusa de fornecimento dos “instrumento jurídico e os parâmetros de segurança” segundo a Política Nacional de Inteligência, item 2.4; a Lei nº 12.527/2011, arts. 22 e 23, VIII; a Lei 12.850/2013 (Lei da Org. Criminosa), art. 3, §1; e art. 23º.</p>	<p>Pedido parcialmente negado. A resposta, que negava parte das informações solicitadas, seguiu o padrão das respostas de outros Estados e do MJSP, sendo praticamente idênticas.</p>
PI	<p>Na primeira resposta, foi comunicado um problema no acesso ao sistema do SIC, atrasando a resposta. Em seguida, o pedido foi concluído com a resposta: “informo que entre em contato com o setor competente” por meio do telefone ou e-mail, mas os meios disponibilizados para contato não funcionaram.</p>		<p>Não foi possível o contato com setor responsável pela resposta. Pedido não respondido.</p>	
RJ	<p>A questão foi respondida com o encaminhamento do Procedimento Operacional (POP) do Ministério da Justiça e Segurança Pública.</p>	<p>O pedido foi negado com base legal no Decreto Estadual nº 46475/2018 art. 26 e art. 29, §3º, classificando a informação como sigilosa, no nível reservado.</p>	<p>A questão foi respondida com o encaminhamento do Procedimento Operacional (POP) do Ministério da Justiça e Segurança Pública.</p>	<p>Pedido parcialmente negado. Questão sobre as condições processuais de uso foi negada com base em um Termo de Classificação da Informação, assinado posteriormente ao pedido.</p>



RN	<p>A questão foi parcialmente respondida, com recusa de fornecimento dos “instrumento jurídico e os parâmetros de segurança” com base na Política Nacional de Inteligência, item 2.4; na Lei nº 12.527/2011, arts. 22 e 23, VIII; na Lei 2.850/2013, art. 3, § 1º; e na Lei nº 12.850/12, art. 23º. A informação é: “Quanto à indagação relacionada ao instrumento jurídico e aos parâmetros de segurança de uso de ferramentas de desbloqueio e extração de dados, tais informações se referem às padronizações técnicas internacionais recomendadas pela ISO/IEC 27042:2015 - Técnicas de segurança - diretrizes para a análise e interpretação de evidências digitais - e ABNT NBR ISO/IEC 27037- Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.”</p>	<p>Foi respondido que sobre o “instrumento jurídico que define as condições processuais para o uso de ferramentas de desbloqueio e extração de dados, tais informações estão fundamentadas na Constituição Federal, no Código de Processo Penal Brasileiro e legislação especial correlata”</p>	<p>A questão foi parcialmente respondida, com recusa de fornecimento dos “instrumento jurídico e os parâmetros de segurança” com base na Política Nacional de Inteligência, item 2.4; na Lei nº 12.527/2011 (LAI), arts. 22 e 23, VIII; na Lei 2.850/2013 (Lei das Org. Criminosas), art. 3, § 1º; e art. 23º. Quanto ao instrumento jurídico que estabelece as normas que regulamentam as regras para a cadeia de custódias e dados obtidos mediante desbloqueio e extração de dados, tais informações podem ser acessada por meio do link http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm, mais especificamente nos artigos 158 a 181 do Código de Processo Penal Brasileiro;“</p>	<p>Pedido parcialmente negado. A resposta, que negava parte das informações solicitadas, seguiu o padrão das respostas de outros Estados e do MJSP, sendo praticamente idênticas.</p>
RS	<p>A Polícia Civil do Rio Grande do Sul informou que “segue o previsto no Código de Processo Penal e o disposto no site da fabricante”. O Instituto Geral de Perícia do Rio Grande do Sul informou que “são seguidos os preceitos do Código de Processo Penal.”</p>	<p>A Polícia Civil do Rio Grande do Sul indicou que aplica as leis “a) Constituição Federal, artigo 5, inciso XII, e artigo 144, § 4º; b) Código de Processo Penal, artigo 4, artigo 6, inciso III, artigo 155, parágrafo único, artigo 240, §1º e §2º; c) Lei nº 9.296/1996, artigo 1, parágrafo único; d) Lei nº 12.965/2014, artigo 7, incisos I e II, e artigo 10, §2º. O Instituto Geral de Perícia do Rio Grande do Sul informou que “Em âmbito jurídico, são seguidos os preceitos do Código de Processo Penal”.</p>	<p>A Polícia Civil do Rio Grande do Sul indicou que segue a regra geral dos objetos apreendidos no curso de uma investigação, bem como do sigilo, que é inerente a todas as investigações”, isso é, o Código de Processo Penal, artigos 6, 240 e 245, e a Lei nº 13.964/2019, Capítulo II: Do Exame de Corpo de Delito, da Cadeia de Custódia e das Perícias em Geral. O Instituto Geral de Perícia do Rio Grande do Sul informou que segue o disposto na Lei nº 13.964, de 24 de dezembro de 2019 (Capítulo II: Do Exame de Corpo de Delito, da Cadeia de Custódia e das Perícias em Geral), Manual de Cadeia de Custódia”.</p>	<p>Pedido respondido.</p>



RO	A questão foi parcialmente respondida, com recusa de fornecimento dos “instrumento jurídico e os parâmetros de segurança” com base na Política Nacional de Inteligência, item 2.4; Lei nº 12.527/2011 (LAI), arts. 22 e 23, VIII; Lei 2.850/2013 (Lei das Org. Criminosas), art. 3, § 1; e art. 23º. Foi informado, porém, que quanto ao “instrumento jurídico e aos parâmetros de segurança ao uso de ferramentas de desbloqueio, extração de dados tais informações se referem as padronizações técnicas internacionais recomendadas pela ISO/IEC 27042:2015 - Técnicas de segurança - diretrizes para a análise e interpretação de evidências digitais e ABNT NBR ISO/IEC 27037”.	Foi informado que “Quanto à indagação relacionada ao instrumento jurídico que baseie as condições processuais para o uso de ferramentas de desbloqueio e extração de dados tais informações estão fundamentadas na Constituição Federal, no Código de Processo Penal Brasileiro e legislação correlata”.	A questão foi parcialmente respondida, com recusa de fornecimento dos “instrumento jurídico e os parâmetros de segurança” com base na Política Nacional de Inteligência, item 2.4; Lei nº 12.527/2011 (LAI), arts. 22 e 23, VIII; Lei 2.850/2013 (Lei das Org. Criminosas), art. 3, § 1; e art. 23º. Foi informado, porém, que “quanto ao instrumento jurídico que estabelece as normas regulamentadoras quanto a cadeia de custódia e dados obtidos mediante desbloqueio e extração de dados” emprega o disposto “nos artigos 158 a 181 do Código de Processo Penal Brasileiro.”	Pedido parcialmente negado. A resposta, que negava parte das informações solicitadas, seguiu o padrão das respostas de outros Estados e do MJSP, sendo praticamente idênticas.
RR	O Núcleo de Inteligência da Polícia Civil do Estado de Roraima afirmou não ter condição de atender aos dados solicitados por não ter participado do Termo de Adesão ao Projeto Excel, apesar de ser o Órgão aquele responsável por operar ferramenta da Cellebrite, segundo a resposta recebida.			Pedido respondido, porém sem resultado.
SC	Foi informado que “Inexiste, por parte do Excelentíssimo Senhor Delegado-Geral, no âmbito do seu poder regulamentar, expedição de ‘instrumento jurídico e/ou administrativo’ quanto à ‘parâmetros de segurança’ (item 4) ou ‘condições processuais’ (item 5) ou ‘regras para a cadeia de custódia’ (item 6) no que se refere ao uso de ferramentas de desbloqueio, extração de dados e/ou acesso remoto a dispositivos tecnológicos pessoais. Oportuno destacar que tais temas, smj, já são disciplinados, à suficiência, pela legislação processual.”			Pedido respondido, porém sem resultado.
SP	O pedido foi negado e as informações foram classificadas como sigilosas, no nível reservado, com fundamento na Lei nº 12.527/11 (LAI), artigo 23, incisos III, VII e VIII; e no Decreto nº 58.052/12, Artigo 30, incisos III, VII e VIII, pois seriam informações “cuja divulgação pode comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.” As informações classificadas envolvem “Contratação e o uso de tecnologias de desbloqueio, extração de dados e acesso remoto de dispositivos tecnológicos”.			O pedido foi negado em sua totalidade via Termo de Classificação da Informação, assinado posteriormente ao pedido.
SE	Foi informado que “os parâmetros estão definidos nas leis penais (Código de Processo Penal) e processuais penais extravagantes (que o solicitante deve pesquisar na internet), senão vejamos: No âmbito infraconstitucional, por exemplo, as normas do artigo 3º, II, III; 7º, I, II, III, VII; 10 e 11 da Lei 12.965/2014 estabelecem diversas proteções à privacidade, aos dados pessoais, à vida privada, ao fluxo de comunicações e às comunicações privadas dos usuários da internet. A norma do artigo 7º, III, da referida lei é elucidativa ao prever a inviolabilidade e sigilo das comunicações privadas armazenadas (dados armazenados), “salvo por ordem judicial” ou, conforme entendimento doutrinário, o acesso poderá existir se ocorrer a autorização da pessoa. Mas, mesmo antes do Marco Civil da Internet, visando a dar corpo à garantia constitucional, o legislador infraconstitucional afirmou essa proteção no artigo 3º, inciso V, da Lei nº 9.472/1997 (Lei de Interceptações). Na mesma linha, há a Resolução 73/1998 da Anatel. Disposições similares estão presentes nos regulamentos dos serviços de telecomunicação.”			Pedido respondido.



TO

Foi informado que “A Computação Forense propõe métodos científicos para identificar, coletar, preservar, analisar e documentar evidências digitais em dispositivos eletrônicos. O método proposto para realizar uma análise pericial em um smartphone está baseado nas melhores práticas utilizadas atualmente pela Polícia Federal do Brasil, pelo NIST (JANSON e AYRES, 2007), pelo Departamento de Justiça dos Estados Unidos (ASHCROFT, 2001), pela polícia Inglesa (Association of Chief Police Officers, 2008) e Instituto Forense da Holanda (Netherlands Forensic Institute, 2007). De outro lado, a Lei nº13.964, de 24 de Dezembro de 2019, que aperfeiçoa a legislação penal e processual penal, alterando dispositivos do Decreto Lei nº 3.689/1941 que dispõe sobre o Código de Processo Penal, criando a figura do Juiz de Garantias, assim estabelece: Art. 3º-B. O juiz das garantias é responsável pelo controle da legalidade da investigação criminal e pela salvaguarda dos direitos individuais cuja franquia tenha sido reservada à autorização prévia do Poder Judiciário, competindo-lhe especialmente: XI - decidir sobre os requerimentos de: a) interceptação telefônica, do fluxo de comunicações em sistemas de informática e telemática ou de outras formas de comunicação.”

Pedido respondido.

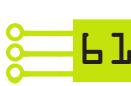


Tabela 11: Resultados das perguntas aos Ministérios Públicos Estaduais

	Parâmetros de segurança	Condições processuais	Regras de cadeia de custódia	Comentários
AC	Foi informado que o MPAC não detém a informação, que conteria “expedientes técnicos dos próprios desenvolvedores e fornecedores das ferramentas a que se refere, além de normas editadas pela Associação Brasileira de Normas Técnicas e inseridas em leis processuais”, negando com fundamento na Resolução Conselho Nacional do Ministério Público (CNMP) 89/2012.			Pedido respondido, porém sem resultado.
AL	A questão não foi respondida.	“Impende ressaltar que as quebras ou transferência de dados telemáticos, fiscais e/ou bancários efetivadas pelo Ministério Público do Estado de Alagoas é feita mediante autorização judicial” e cabendo “a cada órgão atuar mediante colaboração de todo arcabouço imbuído do mister investigativo sua efetivação”	A questão não foi respondida.	Pedido respondido, mas sem resultado e seguia tramitando no sistema do MPE-AL até 19/08/2022.
AP	Foi informado que o “MP-AP não possui instrumento jurídico e/ou administrativo com objeto relacionado a oferecer parâmetros de segurança ao uso de ferramentas de desbloqueio, extração de dados e/ou de acesso remoto a dispositivos tecnológicos pessoais, ou ainda, não possui instrumento jurídico que baseie as condições processuais para o uso dessas ferramentas.”, que “as unidades de investigação norteiam seus procedimentos por regras operacionais definidas e para melhor entendimento, foi apresentada a NOTA TÉCNICA 0001 - ASSEINTI, elaborada pela ASSEINTI de norteamento interno da equipe, que trata do recebimento à devolução de evidências digitais, visando dar segurança e eficiência ao processamento das provas em ambientes forenses dos vestígios computacionais de posse do MP-AP” e que “os procedimentos e metodologias utilizados para operacionalização dessas ferramentas englobam um conjunto de boas práticas definidas pela ABNT NBR ISO 27.037:2013 (diretrizes para identificação, coleta, aquisição e preservação de evidência digital), bem como o Procedimento Operacional Padrão (POP), divulgado pelo Ministério da Justiça e pela Secretaria Nacional de Segurança Pública, Resoluções do Conselho Nacional do Ministério Público Brasileiro - CNMP e encontram-se em processo de atualização para atender mudanças organizacionais propostas pela LEI NO 2621 DE 29 DE DEZEMBRO DE 2021, que entrou em vigor agora em Janeiro e centraliza as atividades investigativas no Centro Integrado de Investigação e Inteligência.”		Pedido respondido.	
AM	“Quanto aos parâmetros de segurança na extração de dados de dispositivos, a legislação pertinente é o CPP”	“Quanto a instrumentos jurídicos relativos à atuação do GAEKO, o mesmo é a legislação correlata (Código de Processo Penal, Lei de Interceptação Telefônica, etc) de natureza pública, bem como Decisões Judiciais, de teor SIGILOSO. Não há dispositivo normativo institucional/administrativo sob a material, cuja competência de legislação, de caráter penal e processual penal, pertence a União (art. 22, I, CF/88);”	“No que tange às suas disposições relativas à cadeia de custódia, bem como normatividade decorrente da Lei Geral da Proteção de Dados, a despeito de inexistir norma específica para o âmbito penal. Ademais, e nestes termos, todo servidor público que tem contato com dados sensíveis é responsável pelo mesmo grau de acesso à informação.”	Pedido respondido



BA	O pedido foi negado com fundamento na Lei nº 12.527/2011, artigo 23, inciso VIII; e na Lei nº 12.850/2013 (LAI), artigo 3º, §1º e 2º, justificando que “sua divulgação pode comprometer as investigações em andamento e futuras do MPBA na repressão às organizações criminosas. Ademais, o fornecimento das informações requeridas implica em divulgar os métodos, procedimentos, técnicas e ferramentas de investigação utilizadas pelo Ministério P\xfablico no enfrentamento \xe0 criminalidade organizada, enfraquecendo as estrat\xe9gias investigat\xf3rias do MPBA e contrariando o interesse p\xfablico.”	Pedido negado em sua totalidade.
CE	Não foi possível acompanhar o processo do pedido de acesso à informação.	O acompanhamento foi prejudicado por erros do sistema e o resultado do pedido é desconhecido.
DF	A informação foi negada, justificando que a publicidade das informações comprometeriam as “atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações” e fundamentado na Lei 12527/2011, artigo 23, inciso VII; no Decreto nº7724/2012, artigo 25, inciso IX; e na Portaria Normativa PGJ nº 426/2016, artigo 3, inciso VIII. No entanto, a resposta aponta ainda “aquisição de tecnologias e inovações para modernizar seus meios investigativos e de ações de inteligência ministerial devem sempre se pautar pela estrita legalidade e adequação ao ordenamento jurídico brasileiro, respeitando os direitos e garantias fundamentais de todos os cidadãos, neste sentido inclusive ocorreu a recente edição da Portaria Normativa PGJ no 796, de 28 de janeiro de 2022, que dispõe sobre a aquisição e a utilização de ferramentas tecnológicas destinadas a realizar intrusão ou captura remota de dados.”	O pedido foi negado, porém a resposta aponta a existência da Portaria Normativa PGJ nº796/2022 que dispõe sobre a aquisição de utilização de ferramentas de intrusão ou captura remota de dados. Essa Portaria, no entanto, não foi encontrada.
ES	O pedido de acesso à informação foi negado com base na Resolução CNMP 89/2012 e na Lei 12527/2011 (LAI), artigo 16, incisos II e III, que definem que “Não serão atendidos pedidos de acesso à informação: II - desproporcionais ou desarrazoados; III - que exijam trabalhos adicionais de análise, interpretação ou consolidação de dados e informações, ou serviço de produção ou tratamento de dados que não seja de competência do órgão ou entidade; que pedidos não serão o pedido desproporcional” e que comprometeria a prestação do serviço de acesso à informação do MPES.	Pedido negado em sua totalidade.
GO	O pedido foi respondido com base na Resolução CNMP 89/2012, art. 16, inciso III, considerando que o dado solicitado “não se reveste da natureza de acesso à informação produzida e detida pelo Ministério P\xfablico do Estado de Goiás. Tratam-se de expedientes t\xedcnicos dos pr\xf3prios desenvolvedores e fornecedores das ferramentas a que se refere, al\xe9m de normas editadas pela Associação Brasileira de Normas T\xedcnicas e inseridas em leis processuais.”	Pedido negado em sua totalidade.
MA	Não foi possível acompanhar o processo do pedido de acesso à informação.	O acompanhamento foi prejudicado por questões do sistema e o resultado do pedido é desconhecido.
MG	O pedido foi negado com base na Lei nº 12.527/2011 (LAI), artigo 23, e na Resolução PGJ nº65/2013, considerando as informações solicitadas como sigilosas.	Pedido negado em sua totalidade.
MT	Negado, provisoriamente, com base na Resolução CNMP nº 89/2012.	Pedido negado em sua totalidade.
MS	As informações “s\u00e3o classificadas como sigilosas” com base na Lei nº 12.527/2011 (LAI), artigo 23, incisos VII e VIII; e na Portaria CNMP-Presi nº122/2021, artigo 13 e artigo 25, incisos VIII e IX.	Pedido negado em sua totalidade.
PA	O pedido est\u00e1 tramitando no Gabinete de Segurança Institucional do MPPA desde 03/02/2022. Um e-mail foi enviado ao \u00d3rg\u00e3o em agosto, por\u00e9m sem nenhum retorno.	Pedido n\u00e3o respondido.



PB	A resposta informa que os instrumentos jurídicos e/ou administrativos "não se reveste da natureza de acesso à informação produzida e detida pelo Ministério Pùblico, mas sim de acesso a expedientes técnicos dos próprios desenvolvedores e fornecedores das ferramentas a que se refere, além de normas editadas pela Associação Brasileira de Normas Técnicas e inseridas em leis processuais."	Pedido negado em sua totalidade.	
PR	As questões não foram respondidas pelos diversos departamentos (GRUPO DE ATUAÇÃO ESPECIAL DE COMBATE AO CRIME ORGANIZADO, DIVISÃO DE GESTÃO DE CONTRATOS DO DEPARTAMENTO DE AQUISIÇÕES E LOGÍSTICA, Centro de Apoio Técnico à Execução e a Comissão Permanente de Licitação) que responderam ao pedido de informação.	Pedido respondido, porém sem resultado.	
PE	O pedido está tramitando na Subprocuradoria Geral em Assuntos Institucionais do MPPE.	Pedido não respondido.	
PI	O pedido de informação ainda tramitava no Núcleo das Promotorias de Justiça de Defesa do Patrimônio Pùblico e da Probidade Administrativa até a data de publicação deste estudo.	Pedido não respondido.	
RJ	Não foi possível solicitar as informações, pois o cadastro no Sistema Eletrônico de Informação (SEI) do MPRJ não foi liberado.	O pedido foi inviabilizado.	
RN	O pedido não foi respondido, com a justificativa de que "não é possível o atendimento, pois a manifestação em tela é complexa, envolvendo inclusive outros órgãos. Ademais, nosso sistema atual não permite que acionemos todas as unidades".	Pedido negado em sua totalidade.	
RS	As questões ainda não foram respondidas.	Pedido não respondido.	
RO	O pedido foi inviabilizado por problema no sistema de informação ao cidadão (sic) do MPRO.	O pedido foi inviabilizado.	
RR	A informação solicitada foi negada com base na Resolução CNMP n.o 89/2012, artigo 16, inciso III, "visto que uma vez que não se tratam de instrumentos próprios deste Ministério Pùblico, mas de expedientes técnicos dos próprios desenvolvedores e fornecedores das ferramentas mencionadas."	"Informa-se que não há instrumentos jurídicos e/ou administrativos formalizados no âmbito deste Parquet quanto às condições processuais para uso ferramentas de desbloqueio, extração e acesso remoto de dados de dispositivos ou quanto às regras para cadeia de custódia, sendo seguidas as prescrições contidas no Código de Processo Penal Brasileiro, Lei n.o 9.296/1996 e Resolução do Conselho Nacional de Justiça nº 36, de 6 de abril de 2009, no que são cabíveis."	Pedido respondido
SC	A resposta informa que o MPSC "não realiza desbloqueio, extração de dados ou acesso remoto de dispositivos tecnológicos pessoais, de modo que fica prejudicado o fornecimento da informação solicitada."	Pedido não respondido.	
SP	O pedido foi respondido com base na Resolução CNMP 89/2012, art. 16, inciso III, considerando que o dado solicitado "não se reveste da natureza de acesso à informação produzida e detida pelo Ministério Pùblico do Estado de Goiás. Tratam-se de expedientes técnicos dos próprios desenvolvedores e fornecedores das ferramentas a que se refere, além de normas editadas pela Associação Brasileira de Normas Técnicas e inseridas em leis processuais."	O pedido foi respondido, mas sem resultado.	



SE	"Comunicamos que, além das normas legais contidas no Código de Processo Penal e Legislação Extravagante aplicável a espécie, foram editadas, no âmbito do Ministério Público do Estado de Sergipe, a Portaria nº876, de 24 de março de 2015 e a Portaria nº 2.082, de 04 de agosto de 2015, que, respectivamente, regulamentam os procedimentos relativos a contratação de bens, obras e serviços e os procedimentos relativos a contratação de Soluções de Tecnologia da Informação."	O pedido foi respondido.
TO	A solicitação de informação foi considerada desarrazoada e negada com base no Decreto Federal n. 7724/2012, art. 13, II; e na Lei Federal nº 12.527/2011 (LAI), art. 7º, §1º.	Pedido negado em sua totalidade.



Nem todos os pedidos que foram negados se basearam em legislações. À parte, algumas justificativas simplesmente alegaram sigilo em função do “interesse do Estado”. Logo, existe, por um lado, o interesse do Estado na opacidade das informações, e, por outro, há um poder crescente de devassa das informações e acúmulo injustificável de dados pessoais pelos agentes do mesmo Estado,¹⁴¹ que se nega a compartilhar informações essenciais para o controle externo de sua atividade, criando frustrações sociais quanto às diretrizes de “governo aberto” e, assim, uma crise de confiança dos cidadãos perante o governo.¹⁴²

O caráter manipulável da regra¹⁴³ permite que os atores governamentais a empreguem de maneira arbitrária e injustificada, alegando sigilo, muitas vezes, a todo o conjunto das informações requisitadas, como nos casos dos Estados de Goiás e São Paulo. Nesse último, o Termo de Classificação da Informação foi assinado justamente em resposta ao Pedido de Acesso à Informação feito no âmbito deste estudo para o SIC São Paulo. Especificamente, o pedido de informação foi protocolado no dia 02/02/2022 e o [Termo de Classificação da Informação \(TCI\) nº 04/2022](#), da Polícia Civil do Estado de São Paulo, foi assinado no dia 07/03/2022.

Diversos outros problemas foram enfrentados nos pedidos de acesso às plataformas dos SIC, prejudicando o acompanhamento dos pedidos. Em vários casos, as questões enfatizadas nas tabelas acima apenas não foram abordadas. Curiosamente, uma parte dos Órgãos que negaram toda ou quase toda a totalidade do pedido usaram textos de justificativa quase ou totalmente idênticos, enquanto outros produziram TCIs em resposta aos pedidos feitos.

Se no âmbito das entidades governamentais federais há uma tendência à opacidade para fiscalização externa, no caso das agências aplicação da lei, como as polícias, essa opacidade pode ser ainda maior devido à posição que assumem em relação à sociedade, uma relação coercitiva e de emprego da força sobre cidadãos, comunidades e territórios.¹⁴⁴ Os dados das respostas de pedidos de acesso à informação reforçam essa forte opacidade na segurança pública estadual, nacional e no setor de inteligência.

Esse cenário pode ser agravado com as retóricas e práticas de militarização da segurança pública, de um lado, e sua privatização, de outro. A militarização da segurança pública, processo antigo, mas atualizado, é realizada e alcançada pelo uso de dispositivos de “guerra ao crime” e “guerra às drogas”, como as ferramentas de hacking. Na lógica militar e na ética de guerra, o “inimigo” deve ser neutralizado. Isso envolve, portanto, um controle informacional mais restrito e políticas de inteligência e contrainteligência avançadas. Entendendo que guerra consiste, segundo a noção de Clausewitz,¹⁴⁵ em uma violência escalável, que a guerra seja um instrumento para um fim e que haja vontade política, a informação se encontra tornada opaca naquilo que o autor considera a “névoa de guerra”, que envolve justamente aumentar as assimetrias de poder, incluindo, do conhecimento e da informação.

Por outro lado, a privatização da segurança pública, já imbuída de uma lógica militarizada e inserida num mundo crescentemente digitalizado, envolve a formação e desenvolvimento de uma indústria privada de tecnologias da informação e comunicação que aprofundam os poderes e capacidades de controle da informação, ainda que ambigamente. Isso porque os entes privados, buscando proteção pela via dos segredos industriais e corporativos, assim como pelo domínio das tecnologias em questão, operam em uma assimetria de poder em relação aos Estados do Sul Global. Assim como o Brasil, estes países não detém, em escala, capacidade estatal equiparável aos complexos industriais tecnológicos que vendem as soluções de extração de dados e acesso remoto aqui investigadas, advindos de países do Norte Global, especialmente dos Estados Unidos e de Israel.¹⁴⁶ Por outro lado, a privatização da segurança pública, em suas diversas esferas, envolve geralmente a expansão das capacidades estatais.¹⁴⁷ É observável, argumentamos, um cenário de aprofundamento da assimetria de poder entre Estado e sociedade

141 SCHNEIER, Bruce. *Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company, 2015.

142 FENSTER, Mark. *The opacity of Transparency*. SSRN Electronic Journal 91(3), 2006. Disponível em https://www.researchgate.net/publication/228161258_The_Opacity_of_Transparency. Acesso em 22 de julho de 2022.

143 GARFINKEL, Harold. *Estudos de etnometodologia*. Editora Vozes Ltda., 2018.

144 MONJARDET, Dominique. *O que faz a polícia: sociologia da força pública*. In: *O que faz a polícia: sociologia da força pública*. 2002. p. 327-327.

145 CLAUSEWITZ, Carl. *On war*. Penguin UK, 2003.

146 THE CITIZEN BUREAU. *The Billion Dollar Spy: Inside Israel's Cyber War Industry*. The Citizen, 2021. Disponível em <https://www.thecitizen.in/index.php/en/NewsDetail/index/6/20683/The-Billion-Dollar-Spy:-Inside-Israels-Cyber-War-Industry-->. Acesso em 9 de setembro de 2022.

147 SPARKS, Richard; GACEK, James. Op. cit.



que fragiliza a democracia, por um lado, e entre Estados e corporações que enfraquece a soberania nacional, por outro lado.

3.5.2. Olhando de perto: o Projeto Excel

O mais substancial retorno aos pedidos de acesso à informação foi sobre a operacionalização do Projeto Excel, iniciativa do Ministério da Justiça e Segurança Pública. O projeto é coordenado pela Diretoria de Inteligência da Secretaria de Operações Integradas (Seopi) e, segundo o Art. 2º do seu ato de instauração (Portaria nº 26/2020),¹⁴⁸ tem por objetivo

"a criação de uma base de dados constituída por dados extraídos por ferramenta própria e compartilhados com a Diretoria de Inteligência possibilitando a produção de conhecimento qualificado, oportuno e eficiente e que resulte em efetivas ações policiais em face das organizações criminosas." (grifo nosso)

O apoio da Seopi também passa por ações de capacitação relacionadas com a atividade de inteligência da segurança pública com os parceiros envolvidos.¹⁴⁹ Os softwares e hardwares disponibilizados no âmbito do Projeto Excel são adquiridos da empresa Techbiz Forense Digital LTDA.¹⁵⁰ Apenas em 2021, o contrato para atualização de 30 licenças perpétuas completas dos softwares custou R\$5.197.596,00 aos cofres públicos, ao custo unitário de R\$173.253,20, dinheiro advindo do Fundo Nacional de Segurança Pública (FNSP). A atualização dessas 30 licenças, como informa o Projeto Básico para a contratação, obtido através de Pedido de Acesso à Informação, datado de julho de 2021, faz parte das

"medidas de reestruturação estratégica da Diretoria de Inteligência em proveito da segurança pública, fortalecendo as atividades de inteligência desenvolvidas por órgãos federais, estaduais e municipais, fomentando a integração, o desenvolvimento de expertise em fontes abertas, análise cibernética e lavagem de capitais, subsidiando todas atividades desenvolvidas e o processo decisório com informações qualificadas e um processo colaborativo". (grifo nosso)

As 30 licenças perpétuas adquiridas em 2021 foram distribuídas para 25 estados, além de 5 licenças para os 5 Centros Integrados de Inteligência e Segurança Pública regionais.

Essas aquisições fazem parte do Plano Diretor de Tecnologia da Informação (PDTIC),¹⁵¹ com previsão no Plano Anual de Contratações de 2020 do Ministério da Justiça e Segurança Pública e partem dos "Objetivos Estratégicos" OE01, sobre fortalecimento do enfrentamento da criminalidade, e OE03, sobre aperfeiçoamento da coordenação estratégica e integração dos órgãos de segurança pública. Cada licença perpétua adquirida como parte da "solução para extração, processamento e análise de dados e informações a partir de dispositivos portáteis", compostas por três módulos: 01) UFED 4PC (funcionalidade principal de extração), 2) UFED Analytics Desktop (funcionalidade principal de análise) e 3) UFED Cloud Analyser (funcionalidade principal de análise em plataformas de nuvem). **Todas as ferramentas são fabricadas pela Cellebrite.**

Há várias questões não esclarecidas acerca da guarda e acesso aos dados coletados pelas ferramentas

148 BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Portaria nº 26, de 9 de julho de 2020: Aprova o Protocolo do Projeto Excel, que visa estabelecer os critérios para adesão e utilização de ferramenta de extração e análise de dados de dispositivos móveis. 2020. Disponível em https://dspace.mj.gov.br/bitstream/1/1867/2/PRT_SEOPI_2020_26.html. Acesso em 29 de julho de 2022.

149 AMENO, Fernando. Op. cit.

150 Portal da Transparéncia. Contrato nº 52/2021 - Secretaria de Gestão e Ensino em Segurança Pública (SEGEN), Ministério de Justiça e Segurança Pública. 2021. Disponível em: <https://www.portaltransparencia.gov.br/contratos/26216385?ordenarPor=descricao&direcao=asc>. Acesso em 29 de julho de 2022.

151 Ministério da Justiça e Segurança Pública. Plano Diretor de Tecnologia da Informação e Comunicação MJSP: PDTIC 2021-2023. 2021. Disponível em: [@download/file/PDTIC%202021-2023%20\(2%C2%AA%20Revis%C3%A3o%20-%202021\).pdf](https://www.gov.br/mj/pt-br/centrais-de-conteudo/publicacoes/categorias-de-publicacoes/pdtic/pdtic-2021-2023.pdf). Acesso em 26 de maio 2022.



disponibilizadas no Programa Excel.¹⁵² Nas perguntas feitas pelo The Intercept Brasil ao Ministério da Justiça e Segurança Pública, não foi respondido adequadamente o nível de acesso da Seopi aos dados coletados pelas ferramentas fornecidas aos Estados e aos Centros Integrados de Inteligência e Segurança Pública regionais, sob a justificativa de sigilo das atividades de inteligência. No entanto, consta no item 3.1.5 do Projeto Básico a seguinte informação: “cabe à Diretoria de Inteligência o intercâmbio de dados e conhecimentos do SISP junto ao Sistema Brasileiro de Inteligência - SISBIN, tanto no campo administrativo como operacional”, o que parece envolver a capacidade da referida Diretoria, componente da Seopi, de acessar e intermediar os dados coletados.

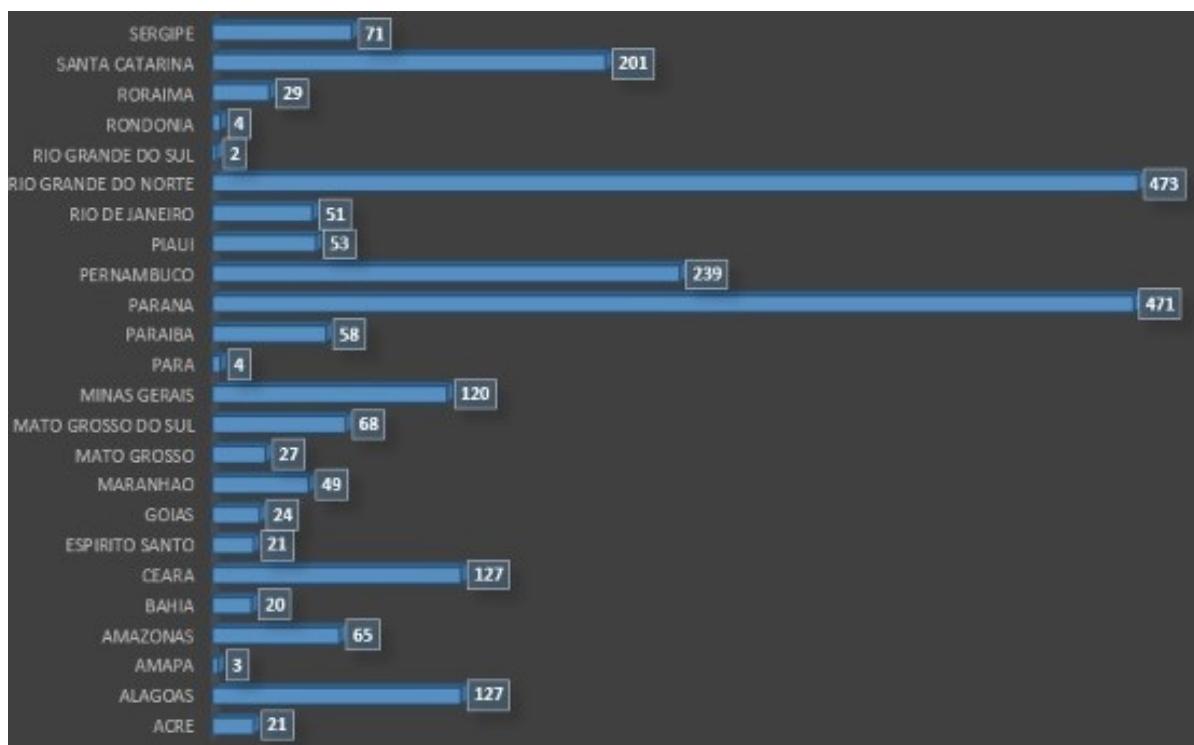
Tabela 12: “Dispositivos tecnológicos estaduais que foram autorizados por esta diretoria, após a validação documental (confirmação de ordem judicial) a realizar as tentativas de extração de dados.”

2018	2019	2020	2021
349	3274	2427	2691

Fonte: Resposta ao Pedido de Acesso à Informação.

O acesso irrestrito ao banco de dados do Projeto Excel é um dos pontos centrais de preocupação, visto que, até 2021, foram autorizadas a extração de dados de 8.741 dispositivos, como consta no quadro acima extraído da resposta ao pedido de informação feito pela equipe de pesquisa, compondo um robusto conjunto de informações e habilitando a Seopi como potencial centralizadora dos dados relativos a operações investigativas. Vale apontar que o montante de dispositivos autorizados à extração de dados foram advindos de 2.350 ordens judiciais, como pode ser observado na imagem abaixo.¹⁵³

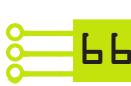
Gráfico 6: Número de ordens judiciais do Projeto Excel, por Estado



Fonte: Gazetaweb

152 AMENO, Fernando. Op. cit.

153 BARROS, Jobisson. Projeto do Ministério da Justiça e Segurança Pública auxilia Alagoas no combate ao crime organizado. Gazetaweb, 2022. Disponível em <https://www.gazetaweb.com/noticias/geral/projeto-do-ministerio-da-justica-e-seguranca-publica-auxilia-alagoas-no-combate-ao-crime-organizado/>. Acesso 9 de setembro de 2022.



O processo compartilhamento de dados extraídos de investigações criminais com ferramentas oferecidas pelo MJSP confere ao órgão uma função similar a de um *data broker*¹⁵⁴ - nesse caso governamental. Reforça ainda mais a inquietude o fato dos crimes investigados serem aqueles dos quais a população negra é mais vulnerável a condenações. Em vídeo do Ministério da Justiça e Segurança Pública, os crimes mais investigados, até 2021, foram de tráfico de drogas (1346 casos), homicídio (325) e roubo (131). Outros como tipificados como crimes de colarinho branco são minorias, tais como lavagem de dinheiro (21), estelionato (20) e peculato (15).¹⁵⁵

Ter compreensão disso é essencial para levantar questionamentos sobre a natureza do tipo de banco de dados que está sendo construído pelo Ministério da Justiça e Segurança Pública. Conforme dados demonstram, a “guerra às drogas” acelerou o encarceramento em massa, atingindo de maneira desproporcional a população pobre e negra brasileira, que em 2019 representava 66,7% das pessoas privadas de liberdade.¹⁵⁶ No Brasil, 78% das vítimas de homicídio por arma de fogo são pessoas negras, principalmente estando em maior vulnerabilidade se são homens e jovens.¹⁵⁷ Dessa forma, há um alto grau de probabilidade de que os dados com os quais o MJSD trabalha são marcados por um nível de seletividade socioeconômica exacerbado de enviesamento, fruto do racismo incrustado na estrutura social brasileira.

As preocupações se agravam com a notícia recente de que o Ministério da Economia, a Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República (Seme/PR) e a Polícia Federal (PF) assinaram um acordo de cooperação técnica para criação de um sistema de integração de análise criminal.¹⁵⁸ A medida ocorre em um vácuo regulatório, no qual o Anteprojeto da Lei Geral de Proteção de Dados para fins de segurança pública e investigações criminais (LGPD Penal) sequer teve sua tramitação iniciada.¹⁵⁹ Assim, além dos riscos envolvidos no que concerne os direitos humanos para o uso dessa ferramenta, qualquer política pública pautada nessas informações estaria comprometida, em especial aquelas que utilizam de *machine learning* como base de funcionamento, como policiamento preditivo, notoriamente conhecida por reforçar a vigilância sobre populações marginalizadas.^{0z}

154 Ver, por exemplo, GARTNER. Gartner Glossary: Data broker. 2022. Disponível em <https://www.gartner.com/en/information-technology/glossary/data-broker>. Acesso em 22 de julho de 2022; SHERMAN, Justin. Data brokers are a threat to democracy. Wired, 2021. Disponível em <https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/>. Acesso em 22 de julho de 2022.

155 O vídeo, inicialmente acessível no YouTube, foi removido. No entanto, pode ser acessado no link: https://drive.google.com/file/d/1t_sTDvWrfAms1PiMMiy5U7GTDncJkOWw/view.

156 LUIZ, Gil Mendes. Guerra às drogas, guerra aos negros. Ponte Jornalismo, 2021. Disponível em <https://ponte.org/guerra-as-drogas-guerra-aos-negros/>. Acesso em 28 de julho de 2022

157 PORTO, Douglas. Negros representam 78% das pessoas mortas por armas de fogo no Brasil. CNN Brasil, 2021. Disponível em <https://www.cnnbrasil.com.br/nacional/negros-representam-78-das-pessoas-mortas-por-armas-de-fogo-no-brasil/>. Acesso em 28 de julho de 2022.

158 MINISTÉRIO da Economia. Ministério da Economia firma parceria para desenvolver sistema integrado de análise criminal. Ministério da Economia, 2022. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/noticias/2022/agosto/ministerio-da-economia-firma-parceria-para-desenvolver-sistema-integrado-de-analise-criminal>. Acesso em: 01/09/2022.

159 GROSSMAN, Luis Osvaldo. Sem LGPD Penal, governo prepara cruzamento de dados criminais. Convergência Digital, 2022. Disponível em: <https://www.convergenciadigital.com.br/Governo/Legislacao/Sem-LGPD-Penal%2C-governo-prepara-cruzamento-de-dados-criminais-61315.html> Acesso em: 01/09/2022



4. CONJUNTOS REGULATÓRIOS

4.1. Um breve panorama internacional

Ainda em 2014, o Alto Comissariado da ONU para os Direitos Humanos afirmou que “os governos frequentemente justificam programas de vigilância de comunicações digitais com base na segurança nacional, incluindo os riscos representados pelo terrorismo”¹⁶⁰. Verificou-se, no entanto, que várias das disposições específicas instaladas para regular o uso de técnicas de hacking pelas forças da lei foram aprovadas sob os auspícios da legislação desenvolvida para o combate ao crime organizado e ao terrorismo. Ao longo da última década, desde a revelação de informações relacionadas a empresas fornecedoras de ferramentas de hacking, a questão tornou-se amplamente discutida a nível internacional:

União Europeia

Em matéria penal, a cooperação policial e judiciária na União Europeia é estabelecida no Tratado de Funcionamento da União Europeia (TFUE), podendo envolver a **aproximação das leis, a introdução de padrões mínimos ou técnicas comuns de investigação**. O tratado pode ser observado à luz de expedientes do hacking governamental.¹⁶¹

No primeiro caso, destaca-se a Diretiva 2014/41/UE que inclui disposições sobre a interceptação de comunicações. A Diretiva não menciona, no entanto, diretamente a possibilidade de agências de aplicação da lei usarem técnicas de hacking para atingir esse fim. Já em relação à introdução de padrões mínimos, não há legislação adotada sobre como e quando agências de investigação podem usar práticas de hacking em situações transfronteiriças, por exemplo. No entanto, já foi adotada legislação que inclui disposições sobre a interceptação de comunicações para prevenção e combate ao tráfico de seres humanos (Diretiva 2011/36/UE), permitindo a interceptação de comunicações e a vigilância eletrónica. Em matéria de técnicas comuns de investigação, há leituras de que a UE pode adotar o hacking como uma “técnica de investigação útil” à deteção “de formas graves de criminalidade organizada, como a detecção de grandes redes internacionais de pornografia infantil, bem como tráfico de drogas e/ou de seres humanos etc”¹⁶². Por outro lado, por fim, a Diretiva 2016/680/UE estabeleceu um regime geral de proteção de dados pessoais no âmbito de investigações criminais, consolidando diretrizes e princípios de legalidade, necessidade e proporcionalidade no uso de métodos que envolvam o processamento de dados pessoais,¹⁶³ aplicável, portanto, a casos que envolvam técnicas de hacking por agências investigativas.

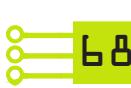
utilização de ferramentas de vigilância digital pelas autoridades dos Estados-Membros da UE para fins de segurança nacional, mesmo quando fora do âmbito do direito da União, está, no entanto, sujeita ao direito constitucional de cada país, bem como ao quadro jurídico relevante do Conselho da Europa, em especial o Convenção Europeia de Direitos Humanos.

160 OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. Human Rights, Terrorism and Counter-terrorism: Fact Sheet No. 32. 2008 Disponível em <https://www.ohchr.org/sites/default/files/Documents/Publications/Fact-sheet32EN.pdf>. Acesso em 30 de julho de 222.

161 EUROPEAN PARLIAMENT. Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices. 2017. Disponível em [https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU\(2017\)583137_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf)

162 Ibidem

163 <https://eur-lex.europa.eu/EN/legal-content/summary/protecting-personal-data-that-is-used-by-police-and-criminal-judicial-authorities-from-2018.html>



França

A França possui a Lei nº 2016-731, de 3 de junho de 2016, que alterou o seu Código de Processo Penal. Esta alteração introduziu a possibilidade de as agências policiais francesas acessarem remotamente os dados de computador, se condições específicas forem atendidas.¹⁶⁴

Alemanha

Embora não existam disposições específicas no Código de Processo Penal Alemão (Strafprozessordnung – StPO), a Lei da Polícia Criminal Federal permite explicitamente que a Polícia Criminal Federal intervenha com “os meios técnicos de sistemas de tecnologia da informação”, se determinadas condicionais forem atendidas.¹⁶⁴ Embora não existam disposições específicas, é possível que as forças da lei utilizem técnicas de hacking por meio do que denominam “competências anexas” a disposições consideradas de natureza semelhante (como a intercepção de telecomunicações, §100a StPO). Percebe-se que a ausência de disposições legislativas específicas não necessariamente proíbe ou impede o uso de técnicas de hacking por autoridades policiais na Europa.

Ainda em 2008, diante de uma decisão da Corte Constitucional Alemã entendeu que as práticas de hacking extrapolam a privacidade e devem ser utilizadas com restrições e bases legais rígidas, apenas contra crimes contra a vida, contra a humanidade e contra as “bases de existência do Estado”.¹⁶⁵ Concluiu, portanto, pela existência de um direito fundamental à garantia da confidencialidade e integridade de sistemas tecnológicos de informação. A decisão foi reafirmada em 2016.¹⁶⁶

Recentemente, o Escritório Federal de Polícia Criminal da Alemanha (BKA) confirmou à Comissão Parlamentar Europeia de Assuntos Internos que havia adquirido e implantado uma versão modificada do software Pegasus, após concluir que a versão padrão violaria a lei alemã. Em relatório não divulgado, o BKA afirma que a versão padrão não fez as distinções necessárias entre ‘vigilância de telecomunicações de origem’ e ‘pesquisa online’ e não registrou suficientemente suas atividades no telefone de destino. Em resposta a uma pergunta parlamentar, o Governo Federal indicou que o uso do Pegasus só é permitido em casos individuais e no respeito de condições legais estritas estabelecidas no StPO, a Lei de Restrições ao Sigilo do Correio, Correios e Telecomunicações e a Lei da Polícia Criminal Federal (BKAG).

Muitos levantam, no entanto, questões e preocupações como a “terceirização ilegal de poderes soberanos”, garantias insuficientes contra acesso e exclusão não autorizados, comissionamento ilegal de processamento de dados e exploração ilegal de vulnerabilidades de segurança. Recentemente, um projeto de resolução ao parlamento federal alemão foi apresentado contra a compra e uso de spyware por autoridades federais. A discussão sobre o Pegasus se integra ao debate em curso sobre a constitucionalidade da ‘vigilância de telecomunicações de origem’ e o uso de software forense de “acesso remoto” no país.¹⁶⁷

Itália

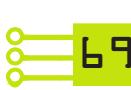
Recentemente, o Projeto de Lei “DDL Orlando” foi apresentado na Itália como uma oportunidade para

164 <https://www.gesetze-im-internet.de/stpo/BJNR006290950.html>

165 ALEMANHA. CORTE CONSTITUCIONAL ALEMÃ [Bundesverfassungsgericht]. Judgment of 27 February 2008 - 1 BvR 370/07. Disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1b_vr037007en.html. Acesso em 22 de julho de 2022.

166 ALEMANHA. CORTE CONSTITUCIONAL ALEMÃ [Bundesverfassungsgericht]. Judgment of 20 April 2016 - 1 BvR 966/09. Disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1b_vr096609en.html. Acesso em 22 de julho de 2022.

167 EUROPEAN PARLIAMENT. Europe’s PegasusGate: Countering spyware abuse. 2022. Disponível em [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU\(2022\)729397_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf). Acesso em 30 de setembro de 2022.



preencher a lacuna legislativa atual no uso de hackers para fins investigativos no país. Especialistas, entretanto, afirmam que a proposta está aquém dos requisitos do Direito Internacional sobre de direitos humanos¹⁶⁸.

Reino Unido

A governança específica de mecanismos de hacking governamental está prevista na Investigatory Powers Act, que entrou em vigor em novembro de 2016. A Lei permite que as autoridades obtenham dados de dispositivos interferindo no equipamento eletrônico associado. Esta disposição é comumente chamada de “interferência de equipamento” (*equipment interference*).

Em 2021, no entanto, o Supremo Tribunal do Reino Unido anulou uma decisão do *Investigatory Powers Tribunal (IPT)* e decidiu que a seção 5 da Intelligence Services Act (ISA) de 1994 não permite a emissão de mandados gerais (e, portanto, podem se aplicar a centenas, milhares ou até milhões de pessoas) para autorizar interferência de propriedade e certas formas de hacking, mesmo no contexto da segurança nacional. A decisão significa que as agências de inteligência não podem mais confiar em ‘mandados gerais’ para certas formas de interferência de propriedade, incluindo o *hacking*¹⁶⁹.

Austrália

Apesar de não adotar lei específica, a Austrália recentemente pôs o direito à privacidade e segurança de milhares de cidadãos e cidadãs em risco a partir da *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021*. Apesar de autoridades já se utilizarem de leis como o *Telecommunications (Interception and Access) Act* (2017) e o *Surveillance Devices Act* (2004) como bases legais para o hacking governamental nos últimos anos, a nova lei preocupa especialistas¹⁷⁰ já que confere base legal para que autoridades não apenas acessem dados de qualquer dispositivo, mas também que adicionem ou alterem conteúdos (*data disruption warrant*), controlem contas de serviços online (*account takeover warrant*), e interceptem todos os meios de comunicação eletrônica (*network activity warrant*). Tudo isso pode ser feito sem consentimento ou conhecimento.

Estados Unidos

A legislação estadunidense não detalha ou regula especificamente o uso de hacking pelas autoridades. Leis federais, como o *Electronic Communications Act (ECPA)* (1986) – uma expansão do ‘*Wiretap Act*’ (1968) – e o *Stored Communications Act (SCA)* tratam, respectivamente, da vigilância da aplicação da lei de tempo e comunicações armazenadas. De maneira geral - e não oficial - agências de investigação buscam autorização para o uso de hacking em mandados de busca e apreensão (Regra 41 do *Federal Rules of Criminal Procedure*).

A fim de endereçar o uso e a divulgação de vulnerabilidades encontradas, o governo americano, por meio de um grupo de trabalho liderado pelo Diretor de Inteligência Nacional do governo Obama, criou em 2010 o Vulnerabilities Equities Process (VEP). Tendo vindo à público apenas em 2016 como resultado de pedido de acesso à informação feito pela Electronic Frontier Foundation,¹⁷¹ o VEP estabelece o procedimento a partir do qual o governo conduz avaliações de risco sobre se explora ou divulga vulnerabilidades em redes, aplicações e dispositivos.

168 PRIVACY INTERNATIONAL. Privacy International's Analysis of the Italian Hacking Reform, under DDL Orlando. 2017. Disponível em https://privacyinternational.org/sites/default/files/2018-01/PI_hacking_DDL_Orlando.pdf. Acesso em 30 de setembro de 2022.

169 PRIVACY INTERNATIONAL. Victory at the High Court against the government’s use of ‘general warrants’. 2021. Disponível em <https://privacyinternational.org/press-release/4358/victory-high-court-against-governments-use-general-warrants>

170 ACCESS NOW. Surveillance state incoming with Australia’s “hacking” bill. 2021. Disponível em <https://www.accessnow.org/surveillance-state-incoming-with-australias-hacking-bill/>. Acesso em 20 de setembro de 2022.

171 CROCKER, Andrew. Time Will Tell if the New Vulnerabilities Equities Process Is a Step Forward for Transparency. Electronic Frontier Foundation, 2017. Disponível em <https://www.eff.org/deeplinks/2017/11/time-will-tell-if-new-vulnerabilities-equities-process-step-forward-transparency>. Acesso em 19 de julho de 2022.



A falta de transparência no VEP, no entanto, continua sendo a maior crítica ao processo. Até onde se sabe, os requisitos de transparência e relatórios públicos nunca foram cumpridos¹⁷². Para alguns especialistas¹⁷³, o equilíbrio pode ser encontrado por meio de uma composição multisectorial do comitê: por meio da inserção de um ou dois representantes eleitos e organizações representantes da sociedade civil, seria possível combater possíveis abusos por parte de agências de inteligência e militares em relação à retenção de informações. De acordo com Heather West, Senior Policy Manager da Mozilla, no passado, o VEP foi dominado pela comunidade de inteligência ou por vozes de aplicação da lei, forçando o uso operacional de uma exploração sem equilibrar as vozes das agências com a, por exemplo, a segurança do consumidor. Às vezes, os participantes do VEP usam o nível de classificação de uma exploração para excluir participantes de agências civis, as quais seriam motivadas principalmente pela manutenção do ecossistema e da segurança do usuário.¹⁷⁴

Nesse sentido, o Bureau de Indústria e Segurança (BIS) do Departamento de Comércio dos EUA proibiu efetivamente o comércio do país com a empresa (exceto com permissão excepcional), em razão do uso do *spyware* tendo como alvos funcionários do governo, jornalistas e outros. No entanto, essa parece ser apenas a ponta do iceberg da relação do governo americano com o mercado de spywares¹⁷⁵. Apesar da reação, é importante destacar que os Estados Unidos não apenas não tomaram medidas preventivas necessárias à limitação do uso de spywares no país como também apoiaram tacitamente essas vendas, aprovando, por exemplo, licenças de exportação¹⁷⁶.

Recentemente, WhatsApp e Facebook (agora Meta), assim como a Apple, entraram com ações contra o NSO Group. Microsoft, Google, Cisco, GitHub, LinkedIn e VMWare apresentaram conjuntamente argumentos e recomendações em favor da ação judicial conjunta WhatsApp-Facebook (*amicus brief*). Em resposta, o NSO Group requereu a intervenção da Suprema Corte dos EUA e convidou o Procurador-Geral do Departamento de Justiça dos EUA a apresentar as opiniões do país.¹⁷⁷

O Acordo de Wassenaar

Organizações internacionais e a sociedade civil organizada questionam os atuais regimes de controle de exportação de tecnologias de dupla utilização (*dual-use*) e pedem que essas empresas sejam devidamente regulamentadas.

A nível internacional, as exportações de dupla utilização são reguladas principalmente pelo Acordo de Wassenaar, um instrumento não vinculativo. Apesar da orientação de apoio sobre o Acordo de Wassenaar afirmar que as licenças de exportação não devem ser emitidas para uma empresa privada se seu produto puder “ser usado para a violação ou supressão de direitos humanos e liberdades fundamentais”¹⁷⁸, especialistas em direitos fundamentais argumentam que esse regime de controle de exportação não impede a exportação de ferramentas de hacking para os governos autoritários¹⁷⁹.

172 THOMPSON, A. W. Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter. 2021. Disponível em <https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter>. Acesso em 30 de setembro de 2022.

173 MOZILLA. The Vulnerabilities Equities Process What we know and what we'd like to see. 2017. Disponível em <https://blog.mozilla.org/press/files/2017/05/VEP-WhatWeKnow.pdf>. Acesso em 30 de setembro de 2022.

174 Atualmente, países como o Reino Unido e a Alemanha buscam seus próprios procedimentos de avaliação sobre exploração de vulnerabilidades. Ver HERPIG, Sven. Governmental Vulnerability Assessment and Management. Stiftung Neue verantwortung, 2018 Disponível em https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf. Acesso em 19 de julho de 2022.

175 FARROW, R. How Democracies Spy on their Citizens. The New Yorker, 2022. Disponível em <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>

176 FELDSTEIN, S. Governments Are Using Spyware on Citizens. Can They Be Stopped? Carnegie Endowment 2021. Disponível em <https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019>.

177 FEDERMAN, Josef. NSO turns to US Supreme Court for immunity in WhatsApp suit. Business and Human Rights Resource Center, 2022. Disponível em <https://www.business-humanrights.org/pt/%C3%BAltimas-not%C3%ADcias/nso-turns-to-us-supreme-court-for-immunity-in-whatsapp-suit/>. Acesso em 19 de julho de 2022.

178 WASSENAAR ARRANGEMENT SECRETARIAT. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. 2019 Disponível em: <https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf>. Acesso em 19 de julho de 2022.

179 RUOHONEN, Jukka; KIMIPPA, Kai. ‘Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity’. Journal of Information Technology & Politics, Vol. 16(2), 2019.



O fato de o Acordo de Wassenaar não ser juridicamente vinculativo, além das divergências de interpretação e aplicação da terminologia do regime a nível nacional, são os principais impulsionadores desse argumento. A nível internacional, 42 Estados comprometeram-se com o Acordo de Wassenaar. Sua eficácia em conter a proliferação de tecnologias de vigilância digital, no entanto, é reduzida por sua associação limitada e voluntária, sua lista específica de armas cibernéticas qualificadas como itens de uso duplo e sua implementação desigual por cada país.

Os produtos da NSO, por exemplo, se qualificam como exportações de uso duplo sob o regime de controle de exportação de defesa de Israel, que é administrado pela Agência de Controle de Exportação de Defesa (DECA). No entanto, como Israel não participa do Acordo de Wassenaar, o país incorpora itens da lista de controle de Wassenaar em sua Lei de Controle de Exportação de Defesa. Em tese, Israel instrumentalizou sua capacidade de aprovar ou negar acesso às armas cibernéticas do NSO para fins diplomáticos. Recentemente, foi relatado que Israel bloqueou a Ucrânia de comprar o Pegasus por temer retaliação da Rússia, onde as autoridades aplicam a lista de controle da UE (que se baseia na lista de controle de Wassenaar).

4.2. Quadro regulatório atual no Brasil: na omissão há permissão?

A utilização de vácuos regulatórios e zonas cinzentas da vigilância governamental instrumentalizada por atores privados é uma tendência internacional. No Brasil, o avanço do que muitos chamam de “tecnoautoritarismo”, chamou a atenção para a falta de regulação associada à matéria em diversas leis que tratam de assuntos correlatos e que muitas vezes são utilizados como justificativa para o hacking governamental,¹⁸⁰ comumente com a aplicação de bases legais a partir de analogias com instrumentos de vigilância e investigação distintos, como a interceptação telefônica, a infiltração ou mandados genéricos de busca e apreensão.

No entanto, os critérios de necessidade e proporcionalidade normalmente sopesados quando da autorização judicial para essas atividades, assim como a análise sobre suspensão de direitos que fundamentalmente ocorrem, são consideravelmente distintos e podem não dar conta das novas esferas de risco que as atividades de hacking colocam em questão. As métricas de análise de risco não somente aos direitos conexos a essas atividades, mas também à segurança da infraestrutura tecnológica precisam, portanto, ser repensadas a partir de atualizações necessárias à conjuntura legal nacional.

Lei de Interceptações (Lei 9.296/96)

Ainda em 2017, pôde-se verificar que diversas autoridades brasileiras já tentaram amparar a utilização de malware para vigilância na Lei de Interceptações. Entretanto, uma problemática é estabelecida a partir do momento em que a falta de clareza em relação ao momento de aplicação da legislação é identificada. A Lei 9.296/96 regulamenta o acesso a ligações ou comunicações eletrônicas pessoais a partir do momento em que se inicia a investigação, durando, desta forma, um período limitado de dias. Quando se fala em hacking governamental, seja por meio de acesso remoto ao dispositivo ou por meio de extração de dados com o dispositivo em mãos, autoridades podem, no entanto, vir a possuir o acesso a diversos tipos de dados armazenados em dispositivos (ou seja, não somente de comunicações em trânsito, objeto de busca da Lei de Interceptações), resultando na inadequação da Lei para essa finalidade.

Quer dizer, ao estender a aplicação da Lei para novos casos, como infecção por malware em celulares e computadores, princípios como o da legalidade e proporcionalidade são colocados em risco assim como direitos e garantias fundamentais uma vez que a ação não só quebra o sigilo das comunicações, mas introduz novos contornos acerca da proteção de dados e sigilo das comunicações envolvidas nesses sistemas.

180 LAUT. (2021) Retrospectiva Tecnoautoritarismo. Disponível em <https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf>



Estatuto da Criança e do Adolescente (Lei 8069/1990)

Em 2017, a lei 13.441/2017 alterou o Estatuto da Criança e do Adolescente (Lei 8069/1990) prevendo a *infiltração virtual* de agentes da polícia na Internet com o fim de investigar crimes contra a liberdade sexual de crianças ou adolescentes. Assim, o diploma hoje autoriza que, mediante pedido do Ministério Público ou de representação do delegado de polícia e dependendo de autorização judicial fundamentada, agentes policiais possam se infiltrar anonimamente na Internet.

O texto se preocupa em estabelecer a infiltração como último recurso, entretanto, não há definição no texto legal do que possa ser entendido como “infiltração”. Ainda que exista uma “distância comportamental” considerável entre o agente infiltrado dissimular sua identidade na rede e o agente acionar, manipular ou operar código malicioso com a finalidade de obter acesso não autorizado a dados e comunicações, há um risco da lei ser utilizada para justificar o uso de dispositivos como spywares por parte das autoridades. Mais uma vez, os testes de legalidade, necessidade e proporcionalidade mereceriam dedicada leitura tendo em vista os bens jurídicos em jogo.

Lei de Organizações Criminosas (Lei 9.713/98)

Estabelecida em 1998, a Lei das Organizações Criminosas define o tipo penal e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal a ser aplicado. Autoriza a infiltração de policiais como meio de obtenção de prova em investigações contra organizações criminosas e “em qualquer fase da persecução penal”. A Lei das Organizações Criminosas não traz, contudo, a modalidade de infiltração virtual em seu escopo. Além disso, assim como no caso da Lei de Interceptações, a quantidade de informações potencialmente coletadas em caso de intrusão em dispositivo, seja por via remota ou física, atinge novas dimensões que não permitem que a infiltração seja interpretada analogamente às técnicas de hacking.

Marco Civil da Internet (Lei 12.965/14) e o Decreto 8.771

Garantias constitucionais ao devido processo legal no campo da privacidade e proteção de dados também estão presentes no Marco Civil da Internet (MCI), uma vez que a Lei estabelece, por exemplo, a necessidade de ordem judicial para guarda e acesso a registros de conexão, aplicação, conteúdo de comunicações (Art. 7, II e III; Art. 10, §§1º e 2º; Art. 15, §1º). Ou seja, na aplicação do MCI, há fluxo processual a ser perseguido pela entidade investigativa quando o acesso a dados e comunicações seja feito via intermediário, provedor do serviço. No entanto, quando o acesso se dá de forma direta ao dispositivo, afastado o intermediário do procedimento, não há delineamento claro e específico no MCI, o que abre margem para a arbitrariedade, insegurança jurídica e abusos de vigilância.¹⁸¹

Na mesma linha, é válido lembrar que o Decreto 8.771/2016, que buscou regulamentar o MCI, menciona a defesa do uso de técnicas de encriptação como diretriz de padrão de segurança na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas por parte dos provedores de conexão e de aplicação, para que garantam a inviolabilidade dos respectivos dados e visando a proteção e segurança de informações dos usuários.

Conforme estabelecido de maneira clara no texto legal do MCI, a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. Dessa forma, o responsável pela guarda somente será obrigado a disponibilizar os registros mediante ordem judicial.

Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, o MCI estabelece a obrigatoriedade de observância à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Assim, o MCI

181 ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. *O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização de celulares no Brasil*. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. II. São Paulo. InternetLab, 2019.



veda a guarda de dados coletados sem consentimento prévio mas também de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei Geral de Proteção de Dados.

4.3. Perspectivas regulatórias

Constituição Federal

Enquanto corolário da proteção aos direitos fundamentais no país, a Constituição Federal estabelece os pontos de partida que, de antemão, devem servir de balizas para a instrumentalização de ferramentas que buscam, através da superação de mecanismos de segurança, acessar comunicações privadas e dados pessoais. A observação da salvaguarda a direitos fundamentais deve não somente ser algo que limite, em proporção e necessidade, o acesso a tais informações por parte de atividades investigativas e de vigilância, mas cuja efetivação é, também, algo a ser proativamente buscado através de políticas públicas e rotinas de transparência por entidades de fiscalização, como das instâncias de corregedoria e do Conselho Nacional de Justiça.

Além do direito à privacidade previsto no Art. 5º, inciso X, de observação central no sopesamento de direitos eventualmente suspensos com o uso de ferramentas de hacking, o acesso ao conteúdo de comunicações privadas também recebe proteção constitucional no inciso XII do mesmo artigo. Qualquer expediente de acesso à informações privadas *lato sensu*, incluindo comunicações, deve ser mediado por instrumentos processuais que assegurem a legalidade, a proporcionalidade e a comprovação de necessidade - por exemplo, de que nenhum outro expediente de coleta de provas surtiria efeito - do uso da tecnologia que invada o círculo da vida privada, incluindo a autorização por meio de mandado judicial que seja suficientemente fundamentado.

Mais recentemente, por meio da Emenda Constitucional nº 115/2022, um direito fundamental autônomo à proteção de dados pessoais foi incluído no rol do Art. 5º (inciso LXXIX). Sendo assim, os protocolos de segurança no tratamento de dados, bem como as diretrizes e princípios gerais do regime nacional de proteção de dados pessoais, devem ser institucionalizados a nível de procedimentos administrativos em matéria processual penal - envolvendo atividades “meio” das entidades da administração pública responsáveis, incluindo aqui parâmetros garantistas ao direito fundamental à proteção de dados pessoais nos pré-requisitos, por exemplo, de participação de agentes econômicos em processos de licitação (incluindo dispensa) e efetiva contratação das ferramentas em questão - bem como às atividades finalísticas do trabalho investigativo propriamente dito. O atendimento a princípios como, por exemplo, da finalidade, necessidade, qualidade dos dados, transparência, segurança, prevenção e prestação de contas dos agentes de tratamento envolvidos nas dinâmicas e rotinas de hacking são preceitos que devem ser sedimentados com base no direito constitucional à proteção de dados pessoais.

Ou seja, as leis infraconstitucionais e instrumentos administrativos que eventualmente venham a regular e estabelecer procedimentos para o uso de ferramentas de hacking devem partir da ponderação da proteção a direitos fundamentais consolidados na Constituição. Importa observar que a salvaguarda a esses direitos vão além da esfera individual, mas - sobretudo no que diz respeito à coleta de dados em massa, de variadas aplicações em dispositivos pessoais, como e-mails, redes sociais, aplicativos de mensagem instantânea, navegadores, entre outros - atingem esferas de coletividades envolvidas e implicadas nos dados objeto de apreensão. Ou seja, os testes de proporcionalidade e necessidade diante do uso de ferramentas de hacking devem dimensionar que outros - muitas vezes milhares - titulares de dados, não envolvidos em dada investigação criminal, terão seus direitos suspensos em função de rotinas investigativas e de vigilância dessa natureza.



Lei Geral de Proteção de Dados Penal

Com a Lei Geral de Proteção de Dados (LGPD), um novo regime regulatório avança em termos de princípios e salvaguardas que avançam na garantia da privacidade no Brasil. A Lei vem como instrumento fundamental para a harmonização da proteção dos direitos de cidadãos e cidadãs brasileiras e a garantia da segurança jurídica em relações que se interconectam com o tratamento de dados pessoais.

Entretanto, apesar da lei buscar regulamentar o uso dos dados pessoais utilizados pelo setor público e pelo setor privado, o artigo 4º da LGPD exclui do escopo de aplicação da lei o tratamento de dados realizados para “fins de segurança pública, defesa nacional, segurança de Estado e investigação e repressão de infrações penais”. Tal como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a matéria recebeu exceções para o campo da segurança pública, mas diferente da regulação europeia, que editou Diretiva específica para regular a esfera penal (Diretiva 2016/680), o Brasil ainda caminha lentamente em termos de perspectivas regulatórias.

De toda forma, o anteprojeto para uma Lei Geral de Proteção de Dados Penal foi apresentado à Câmara dos Deputados em 2020, construído por uma comissão de juristas presidida pelo Ministro do Superior Tribunal de Justiça (STJ) Nefi Cordeiro. O texto¹⁸² conta com sua fundamentação nos princípios constitucionais da autodeterminação informativa, reserva legal e presunção de inocência. Também vincula a lícitude do tratamento de dados pessoais a casos previstos em lei e estabelece formas de garantir o respeito a princípios como o da transparência e da necessidade durante o processo de coleta e tratamento de dados pessoais. O anteprojeto também busca estabelecer a necessidade de realização de relatórios de impacto, por exemplo, no caso da utilização de tecnologias de monitoramento e tratamento de dados de elevado risco - o que nos parece ser o caso de expedientes de hacking governamental. Finalmente, também é importante destacar a previsão estabelecida pelo anteprojeto de que medidas de segurança da informação, técnicas e administrativas sejam previstas.

Reforma do Código de Processo Penal

O Projeto de Lei Substitutivo n.º 8045/2010, do Senado Federal, também conhecido como o anteprojeto do novo Código de Processo Penal, tem chamado a atenção de especialistas da sociedade civil, que alertam para os riscos trazidos pela forma como o acesso e o uso de dados foram abordados pela atual redação do texto.

Ao dispor dos meios de obtenção da prova digital, o artigo 304 visa possibilitar, por exemplo, “a coleta por acesso forçado de sistema informático ou de redes de dados” e “o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial”. Os termos utilizados pelo texto podem ser considerados possíveis sinônimos de hacking facilitados por ferramentas aqui investigadas. Além disso, acredita-se que o texto poderá legitimar práticas de *“fishing expedition”*¹⁸³ a partir de uma interpretação da atual redação do art. 320, que permite que dados relacionados à infração penal obtidos por meio de “encontro fortuito” sejam remetidos como notícia crime ao órgão de investigação. A partir deste cenário, é possível que, sem conexão direta com o delito investigado, a “justa causa” necessária ao acesso a dados de forma forçada seja prejudicada.

Finalmente, pode-se dizer que ao permitir o acesso irrestrito a diversas modalidades de dados pessoais e metadados, o art. 307 é preocupante já que permite acesso não só a dispositivos específicos, mas se estende a *“redes de dados e sistemas informáticos”*. Assim, não parece existir uma observância ao princípio da presunção de inocência ou proporcionalidade. Qualquer usuário, independente de estar ou não sob investigação, estaria exposto e desprotegido, uma vez que não há sanção ou medida de controle a título de abuso de autoridade. Como afirma a Coalizão Direitos na Rede¹⁸⁴, a legitimação em lei destes meios de obtenção de prova pode significar um incentivo a práticas antidemocráticas.

182 Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em 20 de julho de 2022.

183 RAMIRO, André; AMARAL, Pedro. Muito além da vitória: perigos do “Fishing Expedition” digital no Caso Anom. Observatório da Criptografia, 2021. Disponível em <https://obcrypto.org.br/#/post/muito-alem-da-vitoria-perigos-do-fishing-expedition-digital-no-caso-anom>. Acesso em 20 de julho de 2022.

184 COALIZÃO DIREITOS NA REDE. Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. Disponível em <https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>. Acesso em 20 de julho de 2022.



Convenção de Budapeste

A Convenção de Budapeste tem como objetivo principal o estabelecimento de vias para cooperação internacional em matéria penal e a criação de procedimentos uniformes para o combate aos cibercrimes. O diploma, no entanto, vem sendo duramente criticado uma vez que lacunas legais ainda podem ser verificadas.

Como defendido por diversos especialistas, a garantia do devido processo legal é matéria central nesse debate como modo de combater práticas de vigilantismo e abusivas no campo da investigação criminal como é o caso de *fishig expeditions*¹⁸⁵. Para a European Data Protection Supervisor (EDPS), ainda há uma necessidade de preenchimento de lacunas legais referentes à obtenção de metadados, por exemplo. Para o EDPS, a convenção pode significar uma grande ameaça em relação à possibilidade de colisão entre o diploma e normas que protegem não só dados pessoais mas direitos fundamentais.

A norma aborda problemáticas relacionadas ao acesso transfronteiriço de dados em casos de informações publicamente acessíveis e quando o consentimento legal e voluntário da pessoa legalmente autorizada a divulgá-los está presente. Entretanto há um grande debate acerca de quem seria “legitimamente autorizado” em casos circunstanciais, como por exemplo, no caso de armazenamento de dados pessoais em data centers. Obrigações legais são necessárias para que o princípio da legalidade seja reforçado no âmbito de crimes cibernéticos em ambientes democráticos, o que inclusive auxilia no combate à morosidade devida à falta de instrumentos processuais em certos ordenamentos jurídicos internos ou regulamentações de cooperação internacional.

Entretanto, ameaças à liberdade de indivíduos são identificadas a partir do momento em que dados se encontram hospedados em jurisdições estrangeiras. Para Mireille Hildebrandt, “a Convenção do Cibercrime não impõe às partes contratantes uma obrigação de decretar um poder legal para a polícia invadir remotamente os sistemas de computação”, isto é, o hacking governamental¹⁸⁶.

4.4. Princípios norteadores

Reconhecendo que governos ao redor do mundo estão ativamente investindo em expedientes de *hacking* e, ao mesmo tempo, que implicações concretas aos direitos humanos e à cibersegurança já estão sendo observadas, salvaguardas podem ser traçadas para que princípios vinculantes amortecam os impactos de tais ferramentas, incluindo mecanismos de transparência, auditoria, prestação de contas, avaliações de risco e controles de acesso. Da mesma forma, um conjunto de princípios também teria o condão de regular acordos comerciais de entidades governamentais, empresas fabricantes e representações comerciais para fiscalizar e, assim, “filtrar” a entrada de tecnologias de *hacking* no país.

Com base no levantamento de diretrizes sugeridas por organizações acadêmicas, da sociedade civil e governamentais,¹⁸⁷ bem como observando os riscos que já caracterizam a conjuntura nacional, sugerimos um conjunto de princípios que reúnem questões de ordem legal e administrativa para auxiliar possíveis propostas regulatórias que digam respeito aos direitos materiais e processuais no âmbito de investigações e operações de segurança pública mediante uso de ferramentas de hacking.

185 Eilberg, D. et al. (2021) Os cuidados com a Convenção de Budapeste. Disponível em <https://www.jota.info/opiniao-e-analise/columnas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021>

186 Ibidem.

187 Tópico desenvolvido com base em PEREIRA et al. Decálogo de recomendações sobre direitos digitais e produção de provas. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) e Instituto de Referência em Internet e Sociedade (IRIS), 2021. Disponível em <https://obcrypto.org.br/wp-content/uploads/2021/08/Decalogo-de-recomendacoes-sobre-direitos-digitais-e-producao-de-provas-1.pdf>. Acesso em 22 de julho de 2022; HERPIG, Sven. A Framework for Government Hacking in Criminal Investigations. Stiftung Neue verantwortung, 2018. Disponível em https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf. Acesso em 22 de julho de 2022. STEPANOVITCH, Amie. Op. cit; e PRIVACY INTERNATIONAL. Government Hacking and Surveillance: 10 Necessary Safeguards. 2018. Disponível em <https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>. Acesso em 22 de julho de 2022.



1. Legalidade

Operações de entidades governamentais baseadas em ferramentas de hacking devem estar expressamente previstas em lei federal, sendo vedado seu uso a partir de interpretações por analogia de outros expedientes, como interceptação telefônica ou telemática, infiltração ou “escuta ambiente”. Os riscos que impõe o hacking extrapolam os direitos afetados por outros tipos de operações e também inauguram efeitos colaterais derivados de eventual perda de controle sobre essas ferramentas. Operações de hacking devem estar amparadas por mandado judicial específico para tal, que delimita parâmetros de proporcionalidade e avalie a necessidade da medida caso a caso. A legalidade prevista em lei deve ser acompanhada do estabelecimento de procedimentos rígidos que assegurem a observação da lei a nível administrativo - através de portarias, por exemplo - consolidando diretrizes de segurança no acesso e manuseio dessas tecnologias, mecanismos de supervisão e remédios para a contenção de abusos por parte de autoridades.

Importante notar que o devido processo legal envolvido no curso do requerimento- autorização-operacionalização sobre o uso de ferramentas de hacking deve contar com autorizações judiciais que sejam suficientemente informadas e previamente letradas sobre as capacidades técnicas, potenciais riscos e efeitos colaterais em relação a direitos e garantias fundamentais derivados desses expedientes. Processos de capacitação sistemática de magistrados de varas criminais e respectivos assessores devem, preferencialmente, antecipar a expedição de decisões judiciais que venham a autorizar o uso de ferramentas de hacking.

Uma ressalva deve ser pré-estabelecida quanto ao uso de operações de *hacking* remoto, ou seja, sem o aparelho em mãos: uma vez que permitem maiores níveis de vigilância sobre vários indivíduos de uma só vez, colocam maior dificuldade de fiscalização sobre o uso e carregam margens mais amplas de erro (como interferências de conexão que podem afetar a integridade dos dados ou mesmo a intrusão em um dispositivo diferente do pretendido), a previsão de legalidade sobre essas ferramentas deve merecer atenção redobrada, inclusive podendo ser objeto de banimento em território nacional.

2. Proporcionalidade

A previsão legal deve ser acompanhada de parâmetros de proporcionalidade, como forma de reduzir as margens para abusos e amortecer os impactos aos direitos fundamentalmente afetados. Uma vez que a quantidade de dados acessados por essas ferramentas não tem precedentes se comparados a formas mais tradicionais de vigilância, deve ser restringida e minimizada a quantidade de dados coletados de acordo com a categoria dos dados alvo de coleta (por exemplo: localização, comunicações por meio de aplicações de e-mail ou mensageria, histórico de navegação, entre outros), comprovada sua necessidade. Da mesma forma, dois parâmetros temporais devem ser observados: como o alcance no tempo sobre os dados armazenados é muito amplo (por exemplo, e-mails enviados de 2010 até 2022), um recorte temporal proporcional, autorizado em ordem judicial, também deve delimitar a coleta de informações; em segundo lugar, deve ser específico o tempo durante o qual a operação deverá ocorrer, sendo vedada a perpetuação da intrusão no dispositivo. Por fim, deve ser vedada a coleta de dados relativos a indivíduos que não sejam alvos de investigação caso não seja devidamente comprovada sua correlação com o desenvolvimento da operação, devendo seus dados serem imediatamente - e de forma segura - descartados.

3. Necessidade

Dado o alto grau de impacto aos direitos fundamentais que oferecem operações por hacking, a necessidade da coleta de dados deve ser devidamente comprovada, sendo esse o último recurso disponível. Autoridades investigativas, portanto, deverão justificar as razões pelas quais os dados não são acessíveis por outras formas, bem como apontar a categoria dos dados supostamente necessários e as razões pelas quais estariam indisponíveis por outros meios. Essas informações deverão estar suficientemente descritas no requerimento de mandado da autoridade investigativa, adicionalmente à especificação da ferramenta que será utilizada e as razões para sua necessidade. Deve ser estritamente vedada a coleta de comunicações entre jornalistas e suas fontes, bem como entre advogados e seus clientes.



4. Proteção de dados pessoais

O regime brasileiro de proteção de dados pessoais deve ser observado em todas as etapas de tratamento mediante ferramentas de hacking, desde a coleta até o descarte. Os princípios constantes no Art. 6º na Lei Geral de Proteção de Dados Pessoais devem ser explicitamente referenciados em eventual legislação que venha a regularmentar o tema. Da mesma forma, procedimentos norteadores aos controladores de dados devem estar previstos, como requisitos exigências mais restritas para o tratamento de dados pessoais sensíveis, de crianças de adolescentes, para a transferência internacional de dados, bem como a necessidade de publicação - previamente à adoção da ferramenta - de relatórios de impactos à proteção de dados pessoais. Incidentes de segurança relacionados ao uso de ferramentas de hacking também deverão ser comunicados com base no regime nacional de proteção de dados tendo em vista o melhor interesse público.

5. Segurança

A aquisição e uso de ferramentas de hacking devem ser acompanhados de avaliações de impacto não somente aos direitos fundamentais, mas também à cadeia de integridade e segurança potencialmente afetada. Isso inclui avaliações de impactos à coletividade, por exemplo, decorrentes da exploração de uma vulnerabilidade mantida em segredo do fabricante do dispositivo envolvido; de incidentes de segurança envolvendo a perda do controle sobre a ferramenta ou dos dados através dela obtidos, seja accidentalmente, por investidas de atores externos (chantagem sobre funcionário público ou intrusão maliciosa sobre a rede interna da administração pública, por exemplo) ou por ato intencional de atores internos, sejam funcionários públicos ou profissionais contratados/terceirizados. Procedimentos de segurança sobre o armazenamento de tais ferramentas e dos dados através delas obtidos devem ser estabelecidos *a priori* e mantidos atualizados, considerando o estado da arte em segurança da informação.

6. Transparência

Informações sobre a aquisição de uso de ferramentas de hacking têm sido mantidas sob sigilo pelas mais variadas instâncias administrativas no Brasil e em outros países. No entanto, dados os níveis inéditos de impacto aos direitos e ao ecossistema de segurança, o grau de transparência e produção de estatísticas são fundamentais para permitir a fiscalização de entidades públicas de fiscalização e da sociedade civil organizada, assim como aferir o protagonismo e escalabilidade sobre o uso dessas ferramentas.

São fundamentais protocolos de transparência ativa, como a publicação rotineira de documentos e dados sobre contratos, incluindo valores, capacidades técnicas, fabricantes, revendedores, relatórios de impacto a partir dos quais são baseadas as contratações, bem como estatísticas de uso que envolvam o número de dispositivos afetados, número de mandados judiciais emitidos autorizando o uso, bem com a percentagem de crimes efetivamente concluídos com o auxílio dessas ferramentas em detrimento do número global de casos em que foram usadas.

Fabricantes de dispositivos pessoais e provedores de aplicação e conexão não deverão ser compelidos judicialmente a criar vulnerabilidades em seus sistemas de segurança como forma de efetivar o acesso a dados armazenados por meio de ferramentas de hacking. Ainda que formas de "acesso forçado" possam ser circunstancialmente admitidas, não é dever de provedores e fabricantes facilitar a superação de seus sistemas de segurança, o que provocaria, além de tudo, um rompimento na cadeia de confiança com seus usuários.

Para estabelecer uma corrente de confiabilidade e transparência do Estado em relação aos indivíduos afetados, bem como prover informações suficientes para o exercício do direito de defesa, esses deverão ser notificados, dentro de prazo razoável a ser estabelecido por eventual moldura legal, de que foram alvos de expedientes envolvendo o acesso a dados pessoais mediante ferramentas de hacking. Um modelo de notificação *ex-post*, com informações comprehensivas sobre a busca - como número do processo criminal aplicável, referência à autorização judicial e bases legais - tem o condão de gerar dados para a fiscalização dessas atividades, bem como dilui o efeito de inibição de cidadãos pelo receio de terem sido alvo de operações investigativas via ferramentas e hacking. Adicionalmente, facilita que indivíduos acessem a justiça caso julguem que seus direitos foram violados e, assim, busquem os remédios judiciais cabíveis.



Finalmente, como forma de garantir a autenticidade e integridade das provas, a efetividade da persecução penal, bem como o direito à ampla defesa e ao contraditório, as ferramentas utilizadas para fins de acesso forçado devem ser auditáveis. Em razão do interesse público envolvido na fiscalização sobre essas ferramentas, bem como a acessibilidade necessária a, por exemplo, perícias da defensoria pública ou mesmo independentes, contratadas pela defesa de um acusado, o interesse privado percebido no segredo de negócio das empresas envolvidas não deve se sobressair em detrimento da transparência sobre o funcionamento e arquitetura das tecnologias contratadas.

7. Fiscalização

Em razão do grau de invasividade sem precedentes sobre dados não só dos titulares dos dispositivos explorados, mas daqueles com quem um suspeito tem relações próximas, como familiares, amigos e companheiros, técnicas de hacking operadas pelo Estado devem ser fiscalizadas de perto e por variadas instâncias de fiscalização. Isso envolve desde a Autoridade Nacional de Proteção de Dados, passando pelo Conselho Nacional de Justiça, enquanto órgão autônomo e responsável, também, pela fiscalização do sistema de justiça criminal, e pelas corregedorias de polícia e dos Ministérios Públicos, as quais, de forma mais granular, poderão estabelecer rotinas de acompanhamento mais próximas dos órgãos que operem ferramentas de hacking. Todas as instâncias fiscalizatórias poderão disponibilizar ouvidorias que agreguem a participação do cidadão em caso de suspeitas e denúncias envolvendo as ferramentas mencionadas. Da mesma forma, é crucial que os órgãos responsáveis, sobretudo o Conselho Nacional de Justiça e a Autoridade Nacional de Proteção de Dados, contem com instâncias consultivas de participação multissetorial no acompanhamento e consolidação de diretrizes procedimentais sobre rotinas investigativas envolvendo ferramentas de hacking.



5. CONCLUSÃO

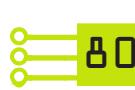
O *status quo* observado sobre a operacionalização de ferramentas de *hacking* por agências governamentais no Brasil permite concluir que técnicas de extração de dados já compõem o *modus operandi* de agências investigativas em todos o território brasileiro, incluindo Distrito Federal e entidades do Governo Federal. Agentes econômicos que incluem fabricantes e revendedores dessas ferramentas têm relações estreitas com a administração pública Federal e dos Estados, tornando-se parte componente de políticas voltadas à segurança pública. Por outro lado, a forma de contratação desses agentes privados, na grande maioria das vezes, é feita mediante dispensa de licitação e as informações sobre a contratação tem seu acesso dificultado, seja pela despadronização, inacessibilidade e insuficiência de dados nos Portais de Transparência, seja pelas declarações de sigilo das informações alegadas pelas entidades responsáveis pela contratação e uso dessas ferramentas quando acionadas com base na Lei de Acesso à Informação.

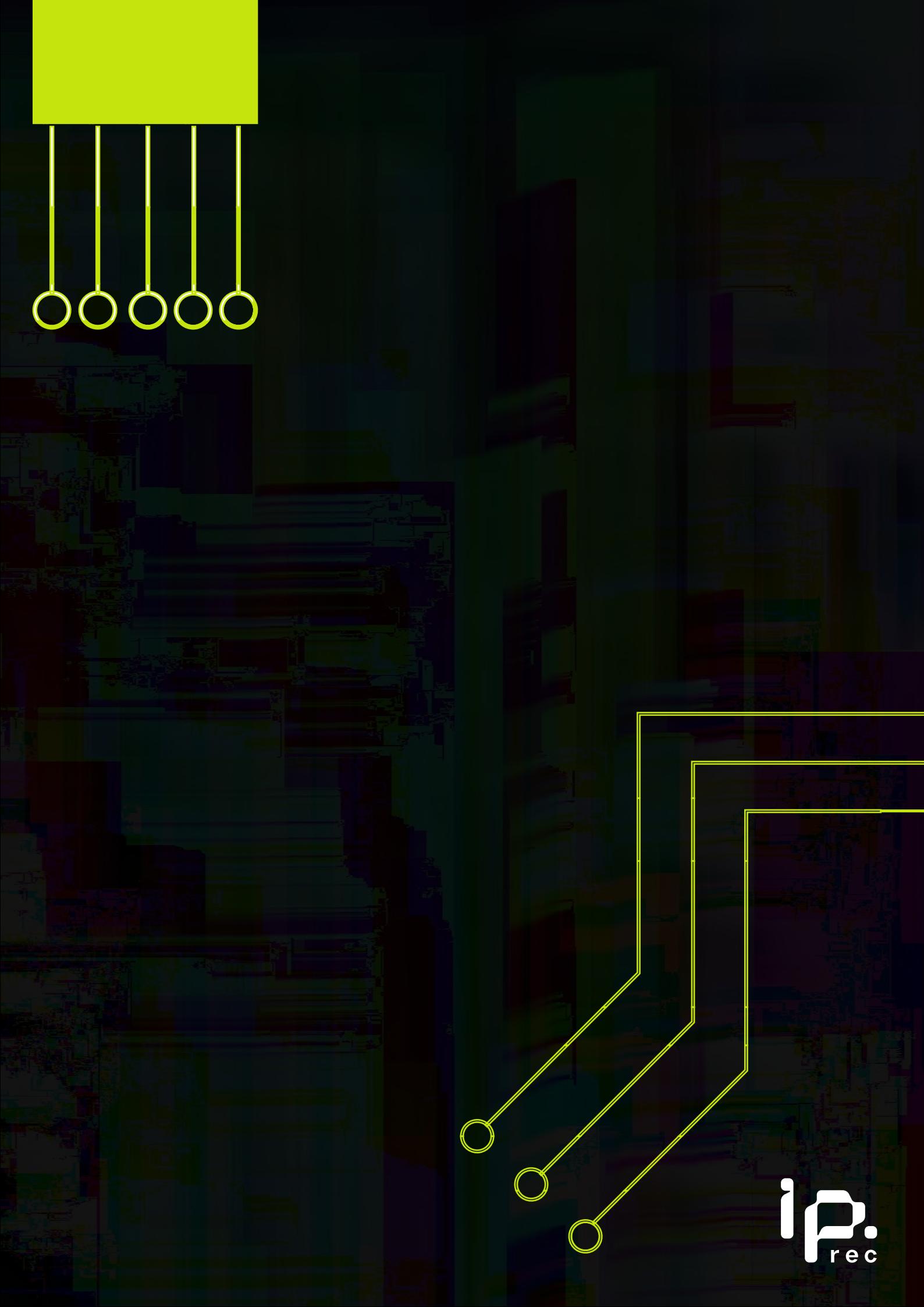
Dos 209 contratos encontrados, as principais empresas contratadas enfrentam escrutínio social e político nacional e internacionalmente. Fabricantes como a Cellebrite e a Verint são vinculadas a escândalos de vigilância governamental abusiva que envolvem a perseguição, prisão e até mesmo tortura de críticos e dissidentes políticos como defensores de direitos humanos e jornalistas. No Brasil, empresas centrais na conjuntura aqui apresentada, como a Suntech, tem sócios investigados e presos em crimes federais que envolvem vigilância e tráfico de informações. Ou seja, antes de auxiliarem no combate ao crime organizado, carregam o potencial de favorecer facções criminosas caso operem sem supervisão e regulação prévia.

Quanto ao “estado da arte” em termos de tecnologias e investigações criminais, ao contrário da narrativa historicamente veiculada por representações de agências de investigações de que haveria um obscurecimento das capacidades investigativas em razão do amplo emprego da criptografia em dispositivos pessoais, percebe-se que, a grosso modo, não há recurso de segurança que resista ao arsenal forense aqui encontrado. Dados constantes em computadores pessoais, tablets, smartphones, tecnologias vestíveis e drones, inclusive deletados, seriam plenamente acessíveis mediante uso de grande parte dos serviços dos quais lançam mão agências de investigação no Brasil. Uma ampla gama de recursos usados para proteger informações sensíveis, inclusive por boa parte da sociedade civil organizada, como o PGP, criptografia de disco e outros recursos adicionais de segurança, também seriam facilmente superados se diante de ferramentas de extração de dados. Como consequência, é gerado um efeito de inibição à população civil, impactando a segurança física e tecnológica necessária ao exercício de direitos políticos. Da mesma forma, amplia-se a possibilidade de incidentes de segurança envolvendo o vazamento dessas ferramentas, contribuindo para um sintoma coletivo de insegurança e pondo em risco recursos econômicos pessoais e públicos.

Sendo assim, uma proposta regulatória é urgente, uma vez que a legislação vigente atinente a técnicas de investigação não prevê análises de risco quanto a técnicas de *hacking* que ensejam parâmetros de proporcionabilidade, legalidade e necessidade sobre seu uso. No que pese técnicas de acesso a dados em dispositivos pessoais serem importantes para a condução de atividades de segurança pública e investigação, os riscos colocados devem ser antecipados em avaliações de impacto aos direitos e à segurança tanto de indivíduos investigados quanto da sociedade de forma ampla. Uma eventual proposta legislativa deverá ser desenhada com base nos princípios acima propostos e abarcando contribuições multisectoriais, mediante amplos debates públicos que antecipem cálculos de benefícios em detrimento dos riscos sobre o uso de tecnologias de *hacking*.

Esperamos que este estudo possa contribuir enquanto insumo ao debate público e como material que auxilie formuladores de políticas públicas. O fenômeno do hacking governamental é um desafio premente que deve ser endereçado como prioridade, como forma do interesse público - e não o mero interesse econômico ou unicamente setoriais - nortear os princípios e procedimentos que deverão ser estabelecidos. Assim, a eficácia da jurisdição e processual na esfera criminal, bem como as garantias constitucionais estabelecidas aos direitos fundamentais e à segurança do ecossistema conectado serão parte de uma mesma sociedade.





ip
rec