Hacking **Governamental**

uma revisão sistemática

Comunicações privadas, investigações e **direitos**

iris
INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

Hacking **Governamental**

uma revisão sistemática

AUTORIA

Luiza Correa de Magalhães Dutra

Paulo Renã da Silva Santarém

Victor Barbieri Rodrigues Vieira

Wilson Guilherme Dias Pereira

REVISÃO

Gustavo Ramos Rodrigues

Paloma Rocillo Rolim do Carmo

REVISÃO EXTERNA

Mariana Canto

Carlos Liguori

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO

Felipe Duarte

PRODUÇÃO EDITORIAL

Instituto de Referência em Internet e Sociedade

COMO CITAR EM ABNT

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

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

DIREÇÃO

Gustavo Rodrigues

Paloma Rocillo

MEMBROS

Ana Bárbara Gomes | Coordenadora de Políticas Públicas e Pesquisadora

Felipe Duarte | Coordenador de Comunicação

Fernanda Rodrigues | Coordenadora de Pesquisa e Pesquisadora

Juliana Roman | Pesquisadora

Júlia Caldeira | Pesquisadora

Lucas Samuel | Estagiário de pesquisa

Luiza Correa de Magalhães Dutra | Pesquisadora

Paulo Rená da Silva Santarém | Pesquisador

Rafaela Ferreira | Estagiária de pesquisa

Thais Moreira | Estagiária de comunicação

Victor Barbieri Rodrigues Vieira | Pesquisador

Wilson Guilherme | Pesquisadore

irisbh.com.br

SUMÁRIO

Sumário

Resumo executivo

O projeto **Comunicações privadas, investigações e direitos**, do Instituto de Referência em Internet e Sociedade – IRIS, busca oferecer subsídios confiáveis para o debate político e jurídico de investigações em comunicações privadas no Brasil. Busca-se, com isso, combinar segurança de tecnologias da informação e comunicação com proteção de direitos humanos e de garantias democráticas. Pretende-se analisar impactos e riscos; sistematizar conhecimento científico; e, ao final, produzir recomendações para setores público e privado. O objeto de análise são três mecanismos para investigações sobre comunicações privadas: rastreabilidade de mensagens instantâneas, *hacking* governamental, e varredura pelo lado do cliente.

Neste terceiro relatório,[1] avaliou-se o cenário do **hacking governamental** . O termo se refere a meios de exploração de vulnerabilidades e falhas em sistemas, acessando dados pessoais e privados em dispositivos eletrônicos, por instituições e autoridades estatais para fins de investigação e persecução penal. Por meio de uma revisão sistemática, investigou-se um total de 37 publicações selecionadas.

A seleção seguiu três etapas de buscas: palavras-chave; contribuições recentes ao camp; e avaliação de relevância. Os achados foram organizados em 04 eixos: sistematização conceitual; contexto; aspectos jurídicos; e argumentos favoráveis e contrários ao hacking governamental.

Primeiro, a análise conceitual apontou para uma não linearidade na utilização do conceito proposto; isso, pois, os termos utilizados vão desde termos mais amplos, como “lawful hacking”, até termos mais específicos, como “network investigative techniques”. Optou-se, então, pelo termo “hacking governamental” que, no âmbito das investigações criminais realizadas pelo poder público, denota as medidas sociais e tecnológicas de exploração de vulnerabilidades em bancos de dados, programas de computador, sistemas computacionais, redes de comunicação ou dispositivos eletrônicos a fim de acessar dados digitais sem a autorização do responsável pelo ambiente digital ou da pessoa afetada.

No segundo aspecto, há registros da existência de softwares de hacking governamental — ao menos com a acepção atual que se tem termo — desde o ano de 1998, quando o FBI explorou portas clandestinas para acesso a metadados de indivíduos vigiados. Mas foi em 2013 que o debate do tema cresceu, a partir das denúncias de Edward Snowden sobre a vigilância massiva realizada pelo governo dos EUA, chegando ao porte atual com o caso Pegasus. *Spyware* fornecido pela empresa de cibersegurança israelense NSO Group, dotado de uma diversidade ampla de recursos de coleta e monitoramento de dados, inclusive em tempo real. Trata-se, contudo, de apenas um dos muitos programas do tipo, oferecidos por empresas do setor, com larga atuação demonstrada contra potencialmente milhões de pessoas em vários países, inclusive no Brasil, a despeito da

falta de regras legais específicas.

Terceiro, para uma análise mais minuciosa acerca dos aspectos jurídicos, que envolvem a proteção de direitos individuais fundamentais, como direito à privacidade e à proteção de dados pessoais, entre outros, foram examinados seis pontos principais: a legalidade e a legitimidade; a observância de princípios da proporcionalidade, necessidade e adequação; o devido processo legal; a notificação de usuários, transparência e o escrutínio público; a integridade dos sistemas de comunicação; e as salvaguardas à cooperação internacional.

E, no último eixo, foram identificados argumentos favoráveis e contrários ao hacking governamental. Os posicionamentos favoráveis mais restritivos se atêm a sua utilização pelo Estado para monitoramento e investigação de alvos específicos, sob autorização judicial e com exploração exclusiva de vulnerabilidades já existentes. Por outro lado, as perspectivas contrárias apontam os demonstrados riscos à privacidade e outros direitos humanos, considerando os muitos casos de práticas de vigilância em massa que afrontaram até a democracia dos países, além da carência de regulação própria para o uso de spywares.

Os resultados confirmam a utilização das técnicas por diferentes países, a partir de perspectivas que envolvem,por um lado, a escassa regulação da utilização, mas, de outro, o uso indiscriminado das ferramentas. Desse modo, para a utilização de hacking governamental se faz urgente a criação de regulamentos legais que versem sobre a real demanda de seu uso, respeitando princípios da reserva legal e da finalidade, apontando para os riscos de seu uso indevido e sem ordem judicial, que podem gerar um campo de vigilância massiva sem qualquer controle democrático. O Brasil, por suas políticas de segurança pública, sistema de justiça e propostas normativas em exame, parece ser um cenário particularmente grave em relação à gama de direitos humanos em risco por decorrência do hacking governamental.

Apresentação

Os primeiros debates sobre a regulação de criptografia forte envolviam a inserção de mecanismos para acesso excepcional das agências estatais de investigação e persecução penal aos algoritmos criptográficos. Mas a sociedade civil e a comunidade técnico-científica foram bem sucedidas na defesa de que políticas de segurança pública considerem riscos tecnológicos, jurídicos e econômicos.

Esses setores demonstraram que as ferramentas de quebra da criptografia para investigações por agentes públicos seriam inevitavelmente acessíveis também por terceiros mal intencionados, que tanto poderiam acessar as comunicações de pessoas inocentes (e até mesmo dos agentes públicos) quanto migrar as suas comunicações ilícitas para plataformas livres de qualquer acesso excepcional. O resultado seria a

redução da segurança para a população em geral e a ineficácia das medidas em conter agentes maliciosos.[2] Essa linha de argumentação enfraqueceu as demandas estatais por soluções do tipo portas clandestinas. Porém, alternativas legislativas à quebra da criptografia surgiram, a fim de dar às autoridades acessos a dados e informações supostamente necessárias para identificar e punir criminosos.

O projeto **Comunicações privadas, investigações e direitos** busca sistematizar a literatura sobre tais métodos alegadamente alternativos à quebra da criptografia, para nutrir o debate científico, político e jurídico sobre o tema no Brasil. Pretende-se oferecer subsídios confiáveis para decisões políticas, regulatórias e judiciais combinarem a segurança das tecnologias de informação e comunicação com a proteção de direitos humanos e garantias democráticas. Em específico, objetiva-se: 1) analisar impactos e riscos à segurança de dados e informações digitais, e direitos envolvidos; 2) sistematizar conhecimento sobre técnicas de investigação; 3) produzir recomendações para o Estado e empresas.

Os Relatórios científicos analisam três métodos alternativos: rastreabilidade de mensagens instantâneas, na qual se guardam metadados da comunicação para futura identificação do caminho ou da origem de um eventual conteúdo ilícito; *hacking* governamental, pelo qual se exploram vulnerabilidades ocultas e não-intencionais de um sistema; e varredura pelo lado do cliente, pelo qual se analisa e compara um dado conteúdo em um dispositivo com bases de dados prévias, em busca de um padrão específico.

A partir dos resultados, o Instituto de Referência em Internet e Sociedade – IRIS pretende dialogar com diversos setores e construir posicionamentos sobre esses métodos, com base em evidências científicas e no respeito aos direitos humanos. O material será disponibilizado online, para consulta e uso geral.

1. Introdução

No final do século XX, o debate sobre a disponibilidade pública de criptografia forte para a proteção de comunicações privadas tem como centro a inserção de mecanismos para seu acesso por agências estatais de investigação e persecução penal. Esses esforços, todavia, renderam grandes controvérsias públicas quanto a seus efeitos jurídicos, políticos e econômicos. Tais conflitos na governança da criptografia forte ficaram conhecidos como guerras criptográficas (*crypto wars*)[3] e foram marcados pela resistência da comunidade técnico-científica, do setor privado e de ativistas de direitos humanos na área digital aos arranjos de acesso excepcional.[4]

Conquanto persista a pressão pública de autoridades, de diversos países, por tais mecanismos,[5] surgiram na década de 2010 novos tipos de propostas, que alegadamente não envolvem acesso excepcional, no sentido convencional do termo, ao teor das comunicações cifradas. Com a promessa de combinar a segurança dos sistemas com

os meios para investigações de dados e informações exigidos para identificar e punir criminosos, elas abarcam técnicas de rastreabilidade de mensagens instantâneas com criptografia, varredura pelo lado do cliente e hacking governamental, que é o objeto deste estudo.

A discussão contemporânea sobre mecanismos de *Hacking* Governamental foi impulsionada de modo particular por duas situações. Em 2015, o caso *Apple vs. FBI*[6] tencionou a posição da empresa (de defender a proteção criptográfica forte dos dados armazenados nos telefones de sua marca) contra o interesse da unidade de polícia (em investigar o telefone de um terrorista morto).[7] Antes, as denúncias de Edward Snowden, em 2013,[8] revelaram práticas sistemáticas de espionagem dos Estados Unidos contra potencialmente qualquer pessoa usuária da Internet, incluindo a efetiva vigilância de autoridades de países tidos como aliados ou "considerados amigos",[9] a exemplo de Ângela Merkel, então Primeira-Ministra da Alemanha, e Dilma Rousseff, Presidenta do Brasil à época, mas alvo desde que ocupou o cargo de Ministra das Minas e Energia.

Mas pode-se afirmar que o caso Pegasus elevou a um outro patamar a atenção mundial para o tema da suplantação de mecanismos de segurança em dispositivos pessoais realizada pelo poder público. A escala de riscos impostos à população mundial subiu: mais que uma superpotência abusando politicamente de seu poder tecnológico, o cenário envolve ferramentas opacas, de recursos ilimitados, vendidas por empresas privadas a quaisquer governos, sem restrições quanto à legitimidade ou humanidade dos interesses. Desde então, o hacking governamental tem sido objeto de discussões ainda mais intensas, em vários países, com destaque para a Comissão de Inquérito sobre o tema criada no âmbito da União Europeia.[10]

Trata-se de um conjunto amplo de práticas tecnológicas, sem uma definição conceitual precisa, mas que consensualmente envolvem o acesso não autorizado a dados mediante a exploração de alguma vulnerabilidade por agentes públicos em superação a mecanismos de segurança. A possibilidade de monitoramento permanente do conteúdo de comunicações privadas pelo poder público impacta a confidencialidade protegida pela criptografia. Mesmo que essa prática, possivelmente, não quebre os padrões de segurança criptográfica forte, questionamentos emergem sobre a legalidade, consistência e eficiência dos os procedimentos e ferramentas adotados no hacking governamental?

Assim, coloca-se como questão central saber se a literatura acadêmica pertinente corrobora o uso de Hacking Governamental como um meio adequado para, sem mecanismos de acesso excepcional, permitir investigações em sistemas com criptografia forte. Ao investigar riscos e desafios políticos, jurídicos e tecnológicos, este estudo busca organizar os principais pontos de defesa e crítica à proposta e avaliar sua viabilidade técnica e jurídica, mediante revisão bibliográfica sistemática de 37 textos selecionados. Definiu-se o *corpus* final à luz do cenário político, jurídico, legislativo e social brasileiro, europeu e estadunidense, e da técnica computacional.

Refletindo o peso político e os parâmetros legais do debate, os resultados compõem quatro seções: sistematização conceitual; contexto; aspectos jurídicos; e argumentos favoráveis e contrários ao uso de hacking governamental. Ainda, as obras analisadas estão listadas no Apêndice 1, e o formulário de análise (o mesmo dos relatórios anteriores, sobre rastreabilidade de mensagens instantâneas e varredura pelo lado do cliente) replicado no Apêndice 2.

2. Metodologia

O hacking governamental possui um amplo debate com acúmulos que apontam para seu risco, impactos e possibilidades de utilização. Demonstra-se especial atenção para dois contextos práticos que trouxeram as práticas de HG ao debate público, e marcam pontos de referência para o debate científico: a) o caso Pegasus; b) e as tentativas de adquirir e incorporar o HG no ordenamento jurídico nacional. É a partir desses dois referenciais centrais de debate teórico que se constrói o referido de pesquisa, perpassando por apontamentos sobre os riscos e garantias ou benefícios de utilização do HG, embates e implicações jurídicas, além de discussões críticas.

Para esse exame, realizou-se revisão sistemática de literatura, abordagem que investiga o estado da arte sobre determinado tema, com recorte empírico em um grupo de obras selecionadas e avaliadas por preceitos e procedimentos explícitos e metódicos. Ela pode ajudar a identificar lacunas em estudos acadêmicos de certo campo ou temática,[11] bem como questões e subtemas para novas investigações e projetos. Pesquisas assim

> *[...] são particularmente úteis para integrar as informações de um conjunto de estudos realizados separadamente sobre determinada terapêutica/intervenção, que podem apresentar resultados conflitantes e/ou coincidentes, bem como identificar temas que necessitam de evidência, auxiliando na orientação para investigações futuras.*[12]

Aqui, o *corpus* documental analisado tem duas fontes: pesquisa por palavras-chave; e obras relevantes selecionadas discricionariamente.

Primeiro, realizaram-se buscas em cinco bases de dados, pesquisando por termos equivalentes. Na plataforma Scopus,[13] as palavras-chave foram: 1) “lawful hacking”; 2) “pegasus” + “spyware”; 3) “government hacking”; na plataforma SSRN foram: 4) “government hacking”; 5) “spyware pegasus”; 6) “lawful hacking”. Nas plataformas Science Direct e na Mendeley: 7) “government hacking” + “encryption”; 8) “lawful hacking” + “encryption”; 9) “spyware pegasus”. E no Google Acadêmico, buscou-se por 10) “hacking governamental” + “criptografia”.

Quanto ao idioma, nas bases estrangeiras foram usados os termos em inglês para hacking governamental (*government hacking + lawful hacking)*, criptografia (*encryption*)

e aplicativo ou programa espião (*spyware*, junção dos termos em inglês *spy* e *software*). O motivo foi ampliar os resultados da pesquisa bibliográfica e expandir os estudos, diante da falta de bibliografia brasileira sobre o contexto internacional, em especial o caso Pegasus. E a combinação do hacking governamental com criptografia serviu como direcionador, mantendo a pertinência dos resultados com o escopo do projeto.

Do total de 87 resultados, foram excluídas as repetições e chegou-se a 66 referências, que foram avaliadas preliminarmente por pertinência temática. Título, resumo (se presente) e início de cada obra foram lidos por duas pessoas da equipe de pesquisa, que votavam pela inclusão ou exclusão. Havendo dissenso, a decisão cabia uma terceira pessoa. Filtrados os textos com temas alheios ao estudo, sem natureza acadêmica, restritos ou apenas à criptografia ou apenas ao hacking governamental, chegou-se a 25 aprovações por consenso e 8 por desempate. Assim, as buscas de palavras-chave geraram um subconjunto de 33 obras.

O segundo subconjunto veio da adição discricionária de quatro textos ao *corpus*, em função de sua relevância acadêmica e institucional sobre a temática, ao debaterem de forma detalhada a conceitualização de hacking governamental, ou ao apontarem dados relevantes para o contexto brasileiro atual, com apontamentos críticos sobre a prática. Foram selecionados: a) "The right to privacy in the digital age", do ACNUDH, lançado em agosto de 2022[14]; b) "A Human Rights Response To Government Hacking", da Access Now, em 2016;[15] c) "Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil", do IP.rec, em novembro de 2022[16]; e d) "O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro", de Gustavo Alves Magalhães Ribeiros e outros, em dezembro de 2022.

O impacto sobre o resultado final é limitado, pois a ampla maioria dos textos analisados (89,19%) seguiu métodos não-discricionários, como descrito acima e detalhados no Apêndice 1. Essa indicação específica – de quais textos foram selecionados conforme um dado método, e quais foram inseridos por via discricionária – mitiga o dano à sistematicidade e preserva a replicabilidade: o estudo pode ser reproduzido sem essas obras, ou na íntegra.

O *corpus* documental final abrange 37 publicações, listadas no Apêndice 1: 22 artigos científicos; 01 capítulo de livro; 03 trabalhos publicados em anais de evento científico; 03 teses, dissertações ou monografias; e 08 relatórios de pesquisa.

Todas as 37 obras foram integralmente lidas, analisadas e inseridas em um formulário (apêndice 2), com categorização (artigo, dissertação, capítulo de livro, etc); resumo; observações e comentários do pesquisador responsável; e citações em destaque. Gerou-se, assim, uma síntese descritiva, orientada a identificar, em cada obra: proposta, metodologia (ou sua ausência), eventuais referências relevantes (citadas como base para o conceito ou posicionamento do trabalho); e qual a conceitualização e abordagem sobre o hacking governamental, com apontamentos positivos e negativos do seu uso.

3. Resultados

Os resultados da revisão sistemática da literatura selecionada foram organizados em quatro tópicos: sistematização conceitual; contexto; aspectos jurídicos; e argumentos favoráveis e contrários ao hacking governamental.

A partir de uma leitura conjunta e integrativa de consensos e dissensos das obras analisadas: primeiro, extrai-se uma definição do termo, adotando-se uma classificação e organizando uma tipologia de modalidades. Em seguida, é descrito o contexto em que se insere o debate acadêmico contemporâneo sobre o hacking governamental, com descrição dos eventos relevantes que impulsionam discussões internacionais e no Brasil. São, então, descritas as questões jurídicas emergentes quando o Estado adota práticas de exploração de vulnerabilidades tecnológicas. E, finalmente, são mapeados os prós e contras sobre o hacking governamental.

3.1. Sistematização conceitual de Hacking Governamental

O debate e conceitualização de hacking governamental começa pela própria escolha de palavras, perpassando por um profundo debate sobre direitos humanos, vigilância de comunicações privadas, proteção de dados pessoais e criptografia como meio de garantia do direito à privacidade e outros direitos fundamentais. As ferramentas de hacking se apresentam em um contexto no qual as instituições de segurança pública e persecução penal se insurgem contra o que chamam de impedimentos, entraves ou obscurecimento (“*going dark*”) das investigações contra criminosos em ambientes cibernéticos.[17]

3.1.1. Terminologia e significado

A literatura aponta que o primeiro desafio no campo é o conceito de hacking governamental. Além das diversas conotações da palavra *hacking*,[18] os trabalhos sobre o tema adotam desde termos mais abrangentes como “*government hacking*”, “*law enforcement hacking*” e “*lawful hacking*”[19] até termos mais específicos, como “*network investigative techniques*” (restrito ao acesso a redes) e “uso de *malware* em investigação criminal” (restringindo a ferramenta de hacking aos chamados “programas maliciosos”). Ainda, caberia considerar como mais exata uma referência ao Estado, pois o Poder Judiciário, por exemplo, pode não se enquadrar propriamente como “governo” a depender do contexto de discussão.[20]

Diante das abordagens cabíveis em circulação, este estudo adere à opção por “hacking governamental”, termo que denota, no âmbito das investigações criminais realizadas

pelo poder público, as medidas sociais e tecnológicas de exploração de vulnerabilidades em bancos de dados, programas de computador, sistemas computacionais, redes de comunicação ou dispositivos eletrônicos a fim de acessar dados digitais sem a autorização do responsável pelo ambiente digital ou da pessoa afetada.[21]

Pensar o hacking governamental como alternativa para contornar proteções criptográficas de comunicações privadas, no contexto tecnológico da sociedade da informação, pode direcionar o olhar e o imaginário para modalidades e ferramentas de espionagem e extração de dados digitais, que podem operar tanto via acesso remoto quanto via acesso físico ao dispositivo de armazenamento. Entretanto, essa definição conceitual abarca também modalidades de engenharia social, em que o sistema, a rede ou dispositivo têm preservada suas funcionalidades, mas a pessoa humana é ludibriada a auxiliar ou permitir o acesso aos dados digitais; além de considerar iniciativas de "força bruta", que podem ocorrer mediante a posse física de um dispositivo eletrônico – apreendido em sede de investigação criminal, como no exemplo do FBI vs. Apple em San Bernardino.[22]

A literatura internacional aponta que pelo menos desde 1998 agências policiais de investigação usam o hacking governamental como forma de vigilância. A maior mudança tecnológica decorre da criptografia nos canais de comunicação, que dificultou a instalação de ferramentas de vigilância nos dispositivos. Nesse cenário, programas espiões são utilizados para obter comunicações e dados de pessoas suspeitas, estejam eles armazenados em um dispositivo ou em trânsito.

> *De um modo geral, o hacking governamental envolve o uso de malware desenvolvido ou adquirido pelo governo para interceptar comunicações de um suspeito ou acessar suas informações. Nesse contexto, malware refere-se a um programa usado para interromper a operação ou obter autoridade operacional sobre um sistema de computador.*[23]

As ferramentas de hacking governamental surgem a partir da existência de vulnerabilidades de sistemas, redes ou sistemas no que tange à segurança, disponibilidade, integridade e proteção de dados e informações pessoais, dando novos contornos à atuação de instituições que operam nas áreas de inteligência e persecução penal, com novos impactos na privacidade e segurança.

> *À medida que melhores mecanismos de criptografia são desenvolvidos e difundidos, a polícia e os investigadores aumentam seu medo de que os esforços para reunir evidências para processar e prevenir crimes estejam se tornando mais difíceis e às vezes até impossíveis.*[24]

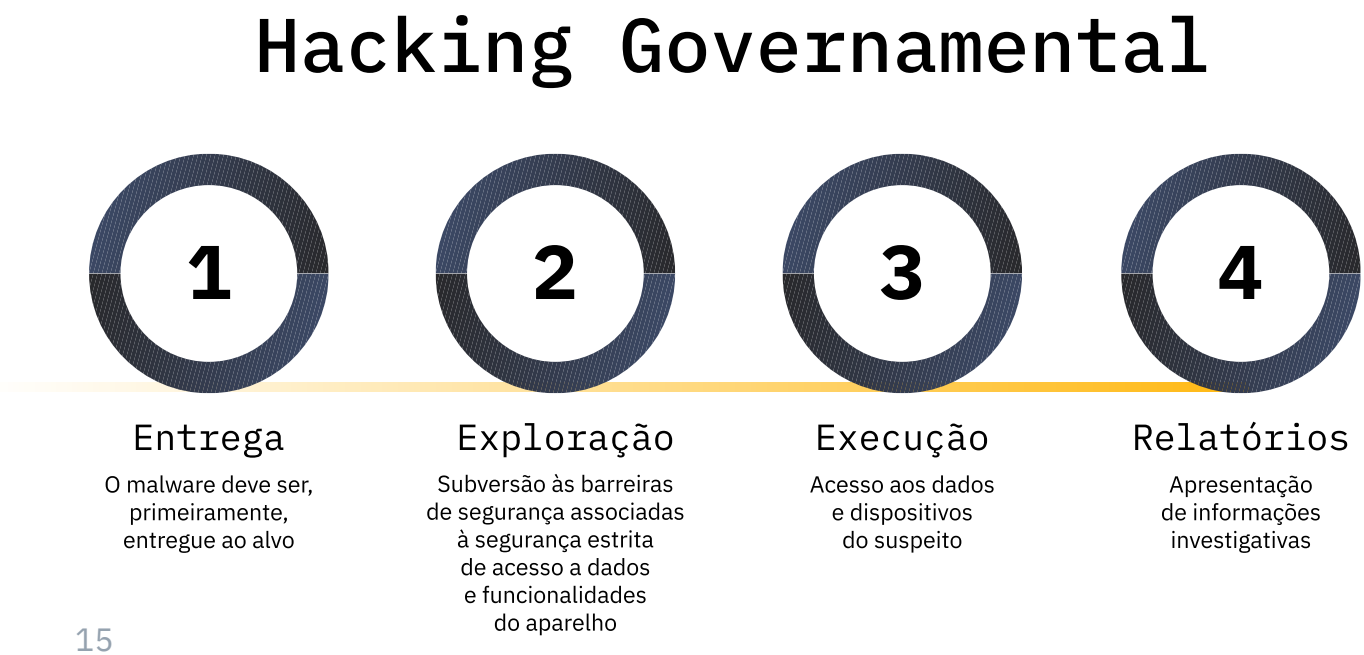
Essas ferramentas podem ser definidas como recursos de programas espiões, usados para monitorar e até controlar o uso de dispositivos, redes ou sistemas eletrônicos. Instalado

o spyware, elas oferecem acesso a dados pessoais e conteúdo de comunicações, além do monitoramento das atividades realizadas no dispositivo.[25]

A utilização do hacking governamental, nessa ótica, pode envolver a quebra ativa da criptografia e outras formas de superar barreiras de segurança,[26] a fim de realizar, por exemplo, a vigilância secreta e direcionada de dispositivos digitais. Assim, pode-se aprofundar a análise dos poderes estatais de vigilância dentro de toda uma estrutura tecnológica criada ou explorada:

> *Esses poderes permitem que as autoridades instalem remotamente malware no dispositivo de um suspeito (ou, às vezes, de uma terceira pessoa), que pode gravar secretamente mensagens enviadas antes de serem criptografadas e mensagens recebidas após serem descriptografadas no dispositivo. [...] A criação de legislação permitindo que a polícia invada computadores e smartphones (também chamado de "hacking legal" para distingui-lo de "invasão ilegal de computador"), portanto, surgiu como o novo campo de batalha no (resultado de) Cryptowars II.*[27]

Com relação à dinâmica das ferramentas de hacking governamental, podem-se listar 04 etapas existentes para utilização:[28] a) na entrega (que pode ser do tipo *watering hole*, direcionada a indivíduos envolvidos em comportamentos específicos; ou *phishing*, sem direcionamento a indivíduos específicos), o malware deve chegar ao alvo, normalmente por mensagem enviada a alguma conta digital do suspeito, induzido a clicar em um link que o direciona para um site ou navegador, a partir de quando se inicia o acesso ao dispositivo alvejado; b) na exploração, subvertem-se as barreiras de segurança para acesso a dados e funcionalidades do aparelho, por exemplo, para dar aos investigadores acesso aos dados e recursos de que precisam, por meio de vulnerabilidades – identificadas ou adquiridas; c) na execução, são efetivamente acessados ou controlados os dados e dispositivos da pessoa investigada; e d) nos relatórios, o software gera e organiza informações investigativas à medida em que se executa ação.



Contudo, já se identificou, por exemplo, no Pegasus (detalhado no ponto 5.2.1 deste relatório), o acesso a dispositivos pelo "clique zero": a pessoa investigada nem precisa clicar em um link malicioso ou realizar qualquer ação para que o spyware interaja com o software alvejado, tornando a primeira etapa desnecessária. Aliás, podem-se explorar vulnerabilidades até mesmo desconhecidas pelo fabricante do aparelho ou desenvolvedor do sistema computacional que, portanto, nem sequer tiveram a oportunidade de corrigir, no que se chama de "zero-day", em referência a essa ausência de tempo.[29]

De todo modo, o hacking governamental passa longe da voluntariedade de divulgação e ou qualquer autonomia no compartilhamento de dados e informações de um cidadão, estruturando-se na ausência de consentimento e na burla a proteções de segurança e privacidade. Exatamente nesse sentido que a literatura aponta preocupações de que essas ferramentas são usadas para motivos ilegítimos para reprimir opiniões ou ações críticas de jornalistas, figuras públicas e defensores de direitos humanos.[30]

Resumidamente, o uso do hacking governamental pressupõe uma exploração às vulnerabilidades já existentes nos sistemas de segurança, e é incitado como alternativa para possibilidade de acesso aos dados criptografados. Por meio de ferramentas tecnológicas próprias ou contratadas, órgãos de investigação poderiam transpor as barreiras de segurança e proteção de eventual prova encriptada, sem precisarem recorrer a um provedor, iniciando novas formas de produção de prova e vigilância.[31] Nesse sentido, o hacking governamental seria um "meio termo pelo qual a aplicação da lei é capaz de acessar uma quantidade suficiente de comunicações e as empresas não são impedidas de projetar sistemas seguros".[32]

3.1.2. Classificações

Uma dificuldade crescente na análise do hacking governamental decorre da soma da finalidade ampla de inteligência estatal e produção de provas em processos judiciais; da diversidade de mecanismos para realização das etapas de entrega, exploração e execução; da multiplicidade de ferramentas e recursos disponíveis; e da ausência de uniformização terminológica.

Para viabilizar o entendimento desse ecossistema e permitir uma análise crítica dos diversos questionamentos e defesas ao emprego de cada modalidade e ferramenta envolvida, o hacking governamental pode ser classificado em função da sua finalidade ou das estratégias para sua implementação.

3.1.2.1. Finalidades

O hacking governamental pode ser categorizado em três grupos, de acordo com o propósito almejado na sua adoção:[33] a) controle de mensagem, b) geração de danos, ou c) vigilância e inteligência. Ressalte-se que algumas práticas podem ser realizadas para mais de uma finalidade.

3.1.2.1.1. Controle de mensagem

A finalidade de controlar mensagens equivale à censura prévia e abarca a propaganda de guerra. Esse tipo de objetivo – direcionado a dificultar o recebimento ou difusão de informações por determinadas pessoas – já foi reputado proibido pela Corte Europeia de Direitos Humanos à luz da Convenção Europeia para a Proteção de Direitos Humanos e Liberdades Fundamentais, por ausência de previsão em lei, de interesse legítimo, de necessidade e de proporcionalidade.[34]

Nesse grupo entram, por exemplo, os propósitos de i) evitar a disseminação de mensagens, ii) manipular o DNS, iii) reescrever conteúdo, iv) sobrecarregar canais de comunicação, e v) desfiguração de sites.

3.1.2.1.2. Geração de danos

Para a finalidade de gerar danos adotam-se ações profundamente invasivas, analogicamente comparáveis ao instituto jurídico da desapropriação, ao tornarem inoperantes as tecnologias alvejadas. Os danos não são efeitos colaterais, mas deliberadamente provocados, e podem ser tão graves a ponto de colocar em risco o bem-estar ou até mesmo a vida de pessoas que nem estejam sendo investigadas, como o caso em que o Pegasus foi utilizado para atingir a esposa de um jornalista assassinado no México.[35] Diante de tal risco, o interesse público a ser promovido precisaria ser muito valoroso e convincente para compensar os danos privados.[36]

Nesse segundo grupo estão os propósitos de: i) modificar internamente a parte física de sistemas ou dispositivos; ii) modificar externamente a parte física de sistemas ou dispositivos; iii) modificar banco de dados; iv) gerar negação de serviço.

3.1.2.1.3. Vigilância e inteligência

A fim de realizar vigilância ou angariar informações de inteligência, o hacking governamental, com ferramentas de custo decrescente e operadas remotamente ou presencialmente, pode promover uma atividade investigativa contínua e mais invasiva que as formas tradicionais.[37]

Nessa terceira categoria estão: i) comprometer usuário ou intermediário, incluindo engenharia social; ii) monitorar canais públicos ou privados de comunicação; iii) comprometer propriedades de um sistema protegido por criptografia.

3.1.2.2. Modalidades

Considerando as estratégias de implementação do hacking governamental na fase de entrega ou exploração, podem-se listar, entre outras, as seguintes modalidades

ou *exploits*:[38] a) ataques *man in the middle* (inglês para "homem no meio"), b) vulnerabilidades *zero-day* ("dia zero"), c) ataques *click-zero* ("zero cliques"); d) *spoofing* ("falsificação") e e) phishing.

3.1.2.2.1. Ataques *man in the middle*

Os ataques *man in the middle* envolvem a inserção da entidade atacante entre as pontas da comunicação, estando a pessoa-alvo em uma das extremidades. O atacante então se coloca como intermediário oculto das comunicações e consegue trocar informações com a pessoa alvo aparentando ser a outra parte da comunicação – e vice-versa.[39]

3.1.2.2.2. Vulnerabilidades *zero-day*

O termo "*zero-day*" diz respeito à exploração de uma vulnerabilidade ainda não conhecida publicamente ou pelo fabricante do respectivo software ou dispositivo, de modo que antes da percepção da falha não tenha havido nenhum dia hábil para se buscar solucionar o problema. E a invasão do dispositivo da pessoa alvo decorre dessa fraqueza ainda não contingenciada:[40] "[...] eles exploram bugs no sistema operacional do telefone que a própria empresa nem conhece e, portanto, não começou a corrigir."[41]

3.1.2.2.3. Ataques click-zero

Outros ataques adotam uma estratégia *click-zero*: o acesso ao dispositivo acontece automaticamente, sem a necessidade de qualquer ação da pessoa alvo, como baixar um arquivo ou mesmo acione qualquer comando que "permita" esse o acesso involuntariamente. Essa abordagem dispensa o uso de técnicas de engenharia social para enganar e manipular o comportamento da pessoa alvo.[42]

3.1.2.2.4. Spoofing

No *spoofing*, semelhante de certa forma, ao ataque *man-in-the-middle*, o atacante se "disfarça" como um terceiro confiável para a vítima, mas sem a necessária interrupção das comunicações entre as partes legítimas.[43] O *spoofing* também pode ocorrer no sistema de nomes de domínio (DNS), com a criação de uma versão falsa de um website a fim de que a vítima insira seus dados, por exemplo. Isso pode ocorrer através da usurpação do nome de domínio real do site legítimo, da criação de um endereço de URL similar que confunda o alvo, ou mesmo da priorização do domínio falso em motores de busca, entre outras possibilidades.[44]

3.1.2.2.5. Phishing

No phishing, que pode ser direcionado a indivíduos específicos, envia-se para o alvo uma mensagem, por exemplo de e-mail ou mensageiro instantâneo, um link e um texto ou imagem atrativa que sirva de anzol e o leve a acessar um site controlado pela autoridade.[45]

3.2. Contexto

Há notável acúmulo histórico de estudos detalhando[46] riscos e impactos do acesso excepcional às comunicações eletrônicas protegidas por criptografia, mas as alegadas alternativas, em regra, carecem do mesmo escrutínio. Em específico, o hacking governamental tem tido proeminente debate internacional, principalmente a partir da divulgação sobre o Pegasus, programa computacional de espionagem. As notícias sobre o monitoramento e repressão política, inclusive contra jornalistas, renderam grande notoriedade midiática.[47]

Apesar dessa evidência com o caso Pegasus, o hacking governamental não é uma novidade. Em 2001, o FBI (*Federal Bureau of Investigation*) dos EUA invadiu o escritório de um mafioso e instalou um sistema para registrar as teclas digitadas. E existem indícios de que já em 1998 ele tenha explorado portas clandestinas, a partir do seu sistema Carnivore, capaz de filtrar e copiar metadados, tendo acessado ao menos 25 vezes dados de pessoas investigadas desavisadas, com a permissão de provedores de internet, conforme divulgado no ano 2000, quando a empresa Earthlink se recusou a cooperar e abriu uma disputa judicial[48].

A temática ganhou uma nova atmosfera em 2013, quando Edward Snowden – um ex-funcionário da CIA, prestando serviços a uma empresa terceirizada contratada pela NSA – revelou ao mundo detalhes sobre a prática de espionagem generalizada pelos EUA, incluindo a vigilância desde cidadãos estadunidenses até autoridades de países considerados amigos, como a Primeira-Ministra da Alemanha Angela Merkel, e a então Presidenta do Brasil Dilma Rousseff – que vinha sendo alvo desde quando exercia o cargo de Ministra das Minas e Energia. Com um conjunto de projetos estratégicos e programas de computador, contratados ou desenvolvidos para explorar sistemas, a agência de segurança monitorou dados oriundos de programas fornecidos por grandes empresas como Microsoft, Facebook e Apple.

Dois anos depois, em 2015, veio à tona o caso FBI *vs* APPLE: uma ação judicial proposta contra a empresa de tecnologia que se negou a burlar a criptografia de segurança e fornecer ao escritório o acesso para desbloquear um Iphone 5C, propriedade de um terrorista assassinado na cidade californiana de San Bernardino. O FBI se apoiava na justificativa de segurança nacional, e a Apple alegava que a pretensão enfraqueceria a segurança dos aparelhos, pois implementar uma vulnerabilidade no sistema daquele telefone em específico colocaria em risco o direito à privacidade de todos os demais usuários cujos telefones rodassem o mesmo sistema. Antes de qualquer julgamento, o FBI contratou uma terceira empresa, que burlou o sistema operacional e acessou ao dispositivo, levando a autoridade a desistir da ação.[49]

No Brasil, o debate sobre o hacking governamental se densificou por três fatores: a) a reforma do Código de Processo Penal, que disciplina investigações criminais, foi

criticada, entre outros pontos,[50] pois incluiria no art. 304 a previsão expressa do hacking governamental como meio probatório, podendo permitir o uso do Pegasus, por exemplo;[51] b) práticas contrapostas à Lei Geral de Proteção aos Dados e ao Marco Civil da internet que contém previsões pertinentes ao uso da criptografia; e c) as reveladas tentativas do governo federal brasileiro em adquirir o Pegasus.[52] Porém, a partir de nosso recorte metodológico previamente apresentado, as pesquisas nacionais na temática foram escassas. Apesar do tema já ser debatido em alguns espaços acadêmicos e institucionais, não foram identificados tantos estudos aprofundados.

Se a ideia do hacking governamental é viabilizar a responsabilização penal por ilícitos, a consistência das bases técnicas e acadêmicas das práticas é crucial para a discussão política e jurídica sobre quais as condições ou requisitos de necessidade e os critérios ou parâmetros de proporcionalidade que podem traçar os limites entre a repressão e vigilância sistemática a defensores de direitos humanos, a ameaça aos direitos humanos pelo monitoramento ilegal pelo governo, ou seja, entre o tecnoautoritarismo, e a efetiva possibilidade de as investigações legítimas de comunicações privadas combinarem a proteção de direitos humanos com a segurança nas tecnologias digitais de informação e comunicação.

3.2.1. Caso Pegasus

O Pegasus é um programa espião desenvolvido pela empresa israelense NSO Group, especializada no desenvolvimento de armas cibernéticas.[53] Em operação desde 2013, esse spyware ficou famoso em agosto de 2016, quando um ativista de direitos humanos dos Emirados Árabes Unidos, Ahmed Mansoor, identificou uma tentativa de infecção em seu iPhone, no caso que chegou a ser denominado de “o ataque de smartphone ‘mais sofisticado’ de todos os tempos”.[54] Depois, apurou-se que um grande número de atentados à democracia, à soberania dos países e aos direitos humanos foi praticado com o seu uso. Em setembro de 2021, a Apple lançou atualizações para corrigir a vulnerabilidade explorada, e em novembro do mesmo ano o Departamento de Comércio dos EUA incluiu o NSO Group numa lista de entidades com atividades cibernéticas maliciosas,[55] proibindo que empresas do país possam vender tecnologia para a israelense e suas subsidiárias.[56]

Essa forte arma de espionagem e vigilância consiste em uma suíte de ferramentas que, sem serem percebidas, permitem coletar dados armazenados e monitorar constantemente as atividades de um dispositivo ao ouvir chamadas, fazer capturas de tela, registrar os pressionamentos de teclas, acompanhar vídeos chamadas de aplicativos como o Facetime e o Skype, além de ativar câmeras e microfones, e esvaziar informações de um aparelho, mediante o registro de teclas e a gravação de áudio, que captam mensagens antes que sejam criptografadas.[57]

Quanto a infecção do dispositivo, as primeiras versões do Pegasus operavam a partir de um link, que era enviado em uma mensagem de SMS personalizada para a vítima, de modo a convencê-la a clicar,[58] afetando iOS e Androids[59] – não havendo distinção no nível de segurança dos sistemas operacionais móveis.[60] Em iPhones,[61] um código JavaScript

oculto era baixado e instalado no aparelho da vítima, a fim de explorar a vulnerabilidade de memória do WebKit da Apple, responsável pelo navegador padrão Safari. Em seguida, o spyware explorava uma vulnerabilidade que permitia identificar a memória do Kernel – núcleo do sistema operacional – e corromper seu código principal, desabilitando a assinatura de códigos. Ao final desse processo de instalação, o Pegasus baixa outras ferramentas, que permitem a efetiva vigilância do alvo.

No contexto atual, o spyware tem explorado vulnerabilidades outras, como a utilização de vulnerabilidades zero-day. Nos raros casos em que nenhuma das possibilidades de ataques funcionem, podem ainda instalá-lo por um transceptor próximo à vítima, ou manualmente.

Em 2016, para investigar as práticas de espionagem com o spyware, foi criado o Projeto Pegasus: uma iniciativa de jornalismo investigativo da ONG francesa Forbidden Stories e da Anistia Internacional.[62] Essa iniciativa apurou ter havido o vazamento de mais de 50.000 números de telefones, infectados ou ameaçados pelo Pegasus, utilizado em países como a Índia, Marrocos, Itália, México, Arábia Saudita, Hungria, Emirados Árabes Unidos e Azerbaijão.[63]

O Citizen Lab, do Canadá, publicou ainda em 2016 a primeira pesquisa sobre o Pegasus,[64] revelando que 12 indivíduos nos Estados Unidos e no México receberam cerca de 76 mensagens, em tentativas de infecção.[65] A maioria dessas pessoas estava envolvida de forma direta com a vida pública: jornalistas proeminentes, advogados, cientistas, defensores da saúde e políticos.[66] E descobriu-se que o Pegasus podia ter sido utilizado pelo governo da Arábia Saudita para investigar o jovem universitário e ativista, residente em asilo político na cidade de Quebec, Omar Abdulaziz, conhecido por criticar o governo saudita.[67]

Em termos quantitativos, "O NSO Group (...) admitiu que seus clientes visam de 12.000 a 13.000 indivíduos anualmente".[68], tendo sido adquirido por cerca de 65 países, tendo como contratantes 60 agências governamentais, de 45 países.[69] As revelações contradizem a alegação da fabricante, de que o Pegasus seria comercializado para segurança pública dos países contratantes[70] – afirmação que aparenta apenas buscar eximi-la de responsabilidades por práticas de vigilância autoritária, ao delimitar funcionalidade e proposta legítimas para o produto.

As respostas internacionais ao caso incluem, no âmbito da União Europeia, a formação de uma Comissão de Inquérito para Investigar o Uso de Pegasus e Programas Espiões de Vigilância Equivalentes (PEGA). Um estudo foi encomendado para avaliar "o impacto do uso de Pegasus e spywares semelhantes sobre os valores do Artigo 2.º do Tratado da União Europeia, sobre privacidade e proteção de dados, e sobre processos democráticos nos Estados-Membros",[71] bem como um estudo amplo sobre o caso e suas repercussões,[72]

que servirão de insumo para os trabalhos da Comissão.

O caso Pegasus marca contexto e época importantes no debate sobre hacking governamental, mas não é seu o único instrumento. Nem a NSO Group é a única empresa de desenvolvimento de tecnologias de espionagem: FinFisher, Hacking Team e Cyberbit também fazem parte do campo, além de outras menores. E todas caminham na mesma linha carente de nitidez informacional e de transparência.[73]

3.2.2. Hacking Governamental no Brasil

Pode-se dizer que um episódio envolvendo o NSO Group e o governo federal abriu as portas para uma nova percepção sobre o hacking governamental no Brasil. Ainda em 2022, poderia se afirmar que faltava conhecimento sobre o uso efetivo de spywares como meio investigativo no país.[74] Mas, ao final desse ano, a publicação de um robusto relatório pelo IP.rec revelou evidências empíricas sobre 228 acordos comerciais negociados pelo menos desde 2013 entre autoridades investigativas (federais e estaduais) e fornecedores privados,[75] com gastos públicos crescentes em soluções de hacking governamental, subindo de 6 milhões em 2015 para 55 milhões em 2021, com pico de 74 milhões em 2020.

O caso mais notório veio a público em meados de 2021. Noticiou-se uma crise militar que teria sido gerada pela tentativa de Carlos Bolsonaro (vereador na cidade do Rio de Janeiro, e filho do Presidente Jair Bolsonaro) intervir na licitação nº 03/2021 do Ministério da Justiça, atropelando as atribuições do Gabinete de Segurança Institucional e da Agência Brasileira de Inteligência, a fim de direcionar a aquisição dos programas Pegasus,[76] do NSO Group, e Sherlock,[77] da empresa Candiru, pelo valor de R$ 25,4 milhões. E no mesmo ano, foram identificados sinais de que a operação Lava-Jato teria tentado a contratação do Pegasus desde 2017.

Mas na verdade, como demonstrado pelo estudo do IP.rec, havia muitos anos que acordos comerciais para municiar agências governamentais já estavam se estabelecendo como parte das políticas de segurança pública, por dispensa de licitação e acobertadas por sigilo. Ou seja, as "*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*".[78]

Em quantidade de empresas e spywares, além do NSO Group e do Pegasus, "*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*".[79] Apesar do destaque alcançado na mídia pelo NSO Group, especialmente durante o escândalo do Pegasus, a empresa não é a mais contratada para hackeamento no Brasil. [80]

No âmbito do poder público, tanto federal quanto estadual e distrital, o hacking é empregado pela Polícia Civil, Ministérios Públicos, que têm atribuição de investigação, mas também pela Polícia Militar e Ministério da Defesa. Ainda, entidades e órgãos que não possuem poder de investigação também firmaram contrato com essas empresas, como por exemplo a polícia militar dos estados e o CADE (Conselho Administrativo de Defesa Econômica).[81]

A despeito de tal "*estágio surpreendentemente avançado de assimilação*"[82] na cultura investigativa brasileira – reforçada pela visão tecnoutopista de agilidade e eficiência – não há regras legais específicas sobre hacking governamental no Brasil. A atipicidade decorre tanto da ausência de previsão de hipóteses de cabimento, pressupostos e limites, quanto da falta de autorização específica. E há divergência doutrinária sobre a possível licitude via enquadramento analógico em abordagens tecnológicas distintas (interceptação telefônica ou telemática; captação de sinais sonoros) ou em modalidades genéricas de ação investigativa (busca e apreensão).

Entre pensadores a favor da legalidade do hacking governamental à luz do ordenamento jurídico vigente no Brasil, constam David Silva Ramalho, Diego Roberto Barbiero, Gustavo Soares Torres, Paulo Pinto de Albuquerque, Tiago Misael, todos considerando se tratar de uma possibilidade a ser empregada excepcionalmente e sob restrições.[83] Do outro lado, Aury Lopes Jr., Carina Quito, Carlos Hélder Carvalho Furtado, Débora Moretti Fumach, Dennys Antonialli, Gianluca Martins Smanio, Gregório Eduardo R. S. Guardia, Gustavo Alves Magalhães Ribeiro, Jacqueline de Souza Abreu, Laura Schertel Mendes, Luiz Greco, Luiz Augusto Sartori de Castro, Maurício Zanoide de Moraes, Orlandino Gleizer, e Pedro Ivo Rodrigues Velloso Cordeiro[84] reputam ilícita essa forma de investigar e produzir provas, por falta de previsão legal de um regime jurídico próprio, com garantias processuais adequadas, e em razão da permissividade à "*massificação do uso e a consolidação de uma cultura investigativa de risco ao ecossistema de segurança e de direitos fundamentais*".[85]

3.3. Aspectos jurídicos do uso de Hacking Governamental

Há numerosas considerações jurídicas pertinentes à legitimação do uso de técnicas de hacking governamental, com embates relacionados, por exemplo, à proteção de direitos e garantias individuais fundamentais, tais qual a proteção à privacidade, à proteção de dados pessoais, à segurança e à liberdade de expressão.

Os aspectos jurídicos do uso de hacking governamental podem então ser sistematizados em alguns tópicos: i) **a legalidade e a legitimidade**; ii) **a observância de princípios da proporcionalidade, necessidade e adequação**; iii) **o devido processo legal**; iv) **a notificação de usuários, transparência e o escrutínio público**; v) **a integridade dos**

sistemas de comunicação; e vi) **as salvaguardas à cooperação internacional**.[86]

Primeiramente, os aspectos relacionados à **legalidade e à legitimidade** das técnicas de hacking governamental dizem respeito à necessidade de que haja uma regulação específica e compreensiva sobre o tema, para que sejam evitados abusos, bem como para que haja segurança jurídica e respeito a garantias fundamentais durante o uso de técnicas dessa natureza por autoridades investigativas. Essa legislação, ainda, deve ser confeccionada segundo critérios de participação pública, com espaço para debates entre os diversos setores da sociedade, para que sejam ponderados os riscos envolvidos no uso dessas técnicas, assim como as salvaguardas e proteções necessárias na regulação da matéria.[87]

Em sentido similar, a observância de **princípios de proporcionalidade, necessidade e adequação** implica a necessidade de que o uso de técnicas de hacking governamental sejam usadas com parcimônia, respeito a garantias legais e atenção aos parâmetros e limites de aplicação legalmente definidos. A proporcionalidade refere-se a limitar o uso do hacking apenas a situações em que o benefício social pelo uso dessas tecnologias não supere os danos causados pela sua utilização. Já a necessidade diz respeito ao uso de ferramentas dessa natureza apenas como último recurso – quando alternativas menos danosas mostraram-se ineficazes para a obtenção do resultado pretendido (qual seja, a persecução de crimes de alta periculosidade). Por fim, a adequação está ligada ao princípio da legalidade estrita, segundo o qual técnicas com tamanho potencial danoso devem ser aplicadas somente mediante o mais estrito cumprimento das disposições legais e regulatórias que as autorizam.[88]

Ainda neste tópico, ressalta-se a possibilidade de que técnicas de hacking governamental causem efeitos colaterais negativos durante a busca pela responsabilização de atores mal-intencionados – o que se denomina "doutrina do efeito duplo".[89] Dessa forma, a proporcionalidade, a necessidade e a adequação unem-se aos aspectos de legitimidade, sendo necessário que os impactos negativos do uso do hacking governamental não se sobressaiam ao ganho social relacionado à punição de infratores.

Os aspectos relacionados ao **devido processo legal**, por sua vez, dizem respeito à necessidade de que a determinação de uso de ferramentas de hacking governamental seja proveniente de ordem judicial expedida em sede de processo devidamente instaurado e instruído pela autoridade judicial competente para julgar o caso. A escolha pelo uso de técnicas de hacking, nesse sentido, não pode ser exercida de ofício por autoridades investigativas. Importante também ressaltar que as ordens judiciais que permitirem o uso dessas ferramentas devem observar os quesitos supracitados de proporcionalidade, necessidade, adequação e observância de garantias fundamentais.[90]

Já os critérios de **notificação de usuários, transparência e o escrutínio público** referem-se à necessidade de que o uso de técnicas de hacking governamental – de maneira similar ao que acontece em casos de buscas e apreensões e varredura de dispositivos físicos – deve ser acompanhado da devida notificação da pessoa investigada. Nesse mesmo

sentido, a necessidade por transparência pública quanto a essas práticas também representa um aspecto jurídico relevante que permeia o hacking governamental, no sentido de que usuários de dispositivos ou softwares similares aos que foram acessados por autoridades públicas podem precisar de informações sobre essas práticas e as vulnerabilidades existentes nos sistemas que utilizam cotidianamente. A emissão de relatórios periódicos sobre o uso de técnicas de hacking, nesse sentido, representa um mecanismo de fiscalização que pode possibilitar o combate a abusos de autoridades públicas.[91]

A integridade das comunicações também representa um aspecto jurídico relevante ao se tratar de hacking governamental. Recentemente, tem-se observado ao redor do mundo tentativas de aprovação de leis que buscam instituir obrigações a provedores de serviços de comunicação privada para que sejam propositalmente inseridos mecanismos de interceptação e vulnerabilidades na segurança desses sistemas, a fim de que essas brechas sejam utilizadas por autoridades de persecução pública para identificar e mapear atividades criminosas.[92] A inserção de vulnerabilidades em sistemas de comunicação privada, contudo, representa prejuízos para a segurança de toda a base de usuários de uma plataforma – e não somente para as pessoas que sejam objeto de investigações criminais –, haja vista que vulnerabilidades inseridas a nível de sistema podem ser igualmente exploradas por terceiros mal-intencionados para fins ilícitos.[93]

Por fim, técnicas de hacking governamental apresentam questões jurídicas relevantes quanto **à cooperação internacional e compromissos jurídicos internacionais assumidos por um país**. Especificamente, quanto a pessoa alvo de uma investigação mediante técnicas de hacking está localizada em país estrangeiro, é necessária estrita observância de padrões internacionais para requerimento de investigações sobre pessoas localizadas em jurisdição diversa, a fim de que não sejam instauradas crises diplomáticas entre os países envolvidos. Isso pode significar, por exemplo, a solicitação de cooperação através de MLATs (“*Mutual Legal Assistance Treaties*”, ou Tratados de Assistência Jurídica Mútua), ou através da homologação de ordens judiciais de um país perante o Poder Judiciário de um país estrangeiro. [94]

Embora as discussões acadêmicas e práticas acerca do uso de técnicas de hacking governamental sejam relativamente incipientes no Brasil, observa-se um acúmulo considerável sobre o tema em outras jurisdições. Durante a coleta de material para a realização do presente estudo, encontrou-se, por exemplo, vasto material discutindo os aspectos jurídicos do uso do hacking governamental à luz das normativas vigentes e em confecção em diversos países.[95]

3.4. Argumentos sobre a uso de técnicas de Hacking Governamental

Antes de pensar argumentos quanto ao uso do hacking governamental, um aspecto indispensável é a necessidade de se estabelecer um diálogo cooperativo, que conecte o debate tecnológico e o debate jurídico, em que cada um avança na medida de suas fragilidades: "os advogados que logicamente são mais competentes em direito podem se concentrar na regulamentação, enquanto os especialistas em segurança podem se aprofundar nos riscos etc.".[96]

Na perspectiva jurídica, central para este relatório, podem-se sistematizar os argumentos favoráveis ou contrários ao uso de técnicas de hacking governamental, incluindo entre os primeiros os posicionamentos de que certas ressalvas podem ser superadas por certas condições.

3.4.1. Favoráveis

O pressuposto das técnicas de investigação em meios digitais é a legitimidade de o poder público inovar ao desempenhar a sua tarefa de aplicação da lei diante dos desafios decorrentes das novas tecnologias digitais, não sendo admissível a possibilidade de o Estado se manter incapaz de lidar com informações criptografadas no enfrentamento a ilícitos.[97] E embora não seja consensual, parece persistir a alegação de obscurecimento ("going dark") como justificativa ampla da adoção de novas tecnologias investigativas.[98]

Assim, em alternativa contemporânea ao grampo telefônico – tecnologia de investigação de comunicações privadas tornada obsoleta pelas mudanças tecnológicas – o hacking governamental encontra defesas de que seria um caminho viável.

Uma abordagem rigorosa e restritiva advoga a exploração estatal limitada exclusivamente a vulnerabilidades preexistentes, contra alvos específicos e sob autorização judicial.[99] Essa abordagem se opõe à previsão de obrigações legais de as empresas criarem vulnerabilidades gerais que possam viabilizar eventuais operações futuras de investigação, e propõe limitações como pontos de análise da proporcionalidade na aplicação: i) adoção de técnicas que garantam a restrição da investigação ao alvo; ii) notificação da vulnerabilidade – do Estado ao fornecedor do programa – como regra; iii) diretrizes para restringir o uso de informações encontradas.[100]

E contra outras vias, o principal argumento a favor do emprego do hacking governamental gira em torno da desnecessidade de o poder público ampliar as vulnerabilidades de segurança para desempenhar a sua tarefa de aplicação da lei, limitando-se a explorar as brechas já existentes.[101] Dado que a evolução tecnológica constante impediria a

previsão completa das ações de investigação, as brechas sempre irão existir, diante da inviabilidade de se eliminarem todas as possíveis formas de vulnerabilidade de qualquer sistema ou dispositivo,[102] aliada ao avanço tecnológico incessante, que gera novos sistemas e novos dispositivos com novas vulnerabilidades.

> *"O hacking [governamental] é um elemento necessário, embora possivelmente não suficiente, de uma solução viável sem o acesso excepcional obrigatório. Portanto, o hacking [governamental] deve ser visto como o elemento central de uma estratégia alternativa abrangente, que inclui investimentos no uso de metadados e na emergente Internet das Coisas para compensar as perdas de conteúdo de comunicação que compõem o problema do obscurecimento."*[103]

Esse aspecto o colocaria como uma solução de meio termo.[104] Entre as opções políticas para acesso a dados protegidos por criptografia, o hacking governamental é defendido como alternativa moderada e realística entre medidas tanto anteriores ao crime (como reter chaves ou exigir portas clandestinas) quanto posteriores (como determinar a descriptografia).[105] Em vez de soluções generalizadas (*ex ante* ou *ex post*), que interfiram nos canais ou sistemas e afetem todas as pessoas antes ou depois de ocorrer um ilícito, fala-se em abordagem restrita (*ex nunc*), realizada em tempo real e particularizada no alvo da ação investigativa, como ponto final da comunicação.[106]

Há afirmações de que não há vácuo regulatório, dada a possibilidade de supervisão judicial e administrativa das decisões tomadas pelos agentes de baixo escalão.[107] Há quem aponte ser suficiente o desenvolvimento de diretrizes éticas para o uso de técnicas de hacking governamental, bem como de estratégias que equilibrem as demandas de segurança estatal e privacidade individual.[108] Como exemplo, aponta-se o *Guia de Boas Práticas* da Associação de Chefes de Polícia do Reino Unido, contendo um conjunto de princípios para a prática forense no trabalho com evidências fruto de hacking.[109]

Mas, levando em conta o potencial de graves riscos graves incontroláveis ou os conhecidos danos colaterais inevitáveis, mostra-se mais consistente a visão de que seria uma exigência, até mesmo urgente, a definição objetiva em lei de dois aspectos: primeiro, a definição das excepcionais condições ou requisitos de necessidade que autorizariam usar hacking governamental; e, segundo, a definição de parâmetros ou critérios que, em cada situação, permitiriam avaliar a proporcionalidade da efetiva implementação.

Aponta-se a pertinência de uma regulamentação legal e da delimitação de metodologias entre a comunidade de técnicos forenses já desde a engenharia reversa indispensável para o poder público – sem a insegura dependência de intermediários e fornecedores externos – descobrir as vulnerabilidades pré-existentes a serem exploradas, ou mesmo validar os dados obtidos.[110]

Em termos de condições para a necessidade, o hacking governamental exigiria: a)

aplicação excepcional como última medida; e b) ordem judicial prévia; e como requisitos de validade à luz da proporcionalidade: a) fixação da duração da implementação; b) delimitação de atores, dispositivos e tipos de dados a serem obtidos.[111]

Ainda, apesar dos desafios técnicos, legais e políticos, afirma-se que o hacking governamental – no enfrentamento ao anonimato e na investigação de crimes na *dark web* – não afetaria as relações e o direito internacional, dados o interesse comum demonstrado pelos países em cooperar contra o cibercrime, e a ausência de atividades presenciais em território estrangeiro.[112]

3.4.2. Contrários

Em termos de argumentos contrários, o escopo analisado aponta como pontos principais: a) riscos a privacidade; b) risco a violações de direitos humanos; c) risco a democracia e soberania dos países; d) o obscurecimento de informações sobre as empresas de HG; e) ausência de uma política regulatória sobre comercialização e uso do HG; f) o uso de spywares por organizações criminosas; g) esquivamento de responsabilizações internacionais por parte dos países; h) alta onerosidade; i) desincentivar o investimento em novas tecnologias de privacidade e segurança; j) por fim, o hacking governamental pode ampliar abismos dialógicos entre o setor privado e poder público.

Quanto à privacidade, o Estado usar spywares, como o Pegasus, pode romper toda a lógica **de privacidade e segurança**, ao gerar numerosas informações sobre uma pessoa, sem seu conhecimento. Na mesma trilha, consegue fomentar muitas violações ao **direitos humanos**,[113] ao permitir que o governo detenha uma alta quantidade de informações sobre as pessoas as quais pretende investigar, além dos denominados "danos colaterais" a outros sujeitos não diretamente envolvidos na investigação, mas cujos dados ficam expostos pelo Hacking Governamental.[114] Nesta seara, os riscos se intensificam. Direitos humanos, como liberdade de pensamento e de convencimento, são postos em ameaça, pois sob o manto da vigilância o desenvolvimento de tais capacidades são restringidas. Ademais, os sujeitos tidos como "danos colaterais" no processo de hackeamento possuem uma fragilidade maior na confiança informacional e outros riscos, que não são mitigados com o cerceamento do hacking.

> *O ACNUDH reitera seu apelo recente, bem como de especialistas e grupos de direitos humanos, por uma moratória na venda, transferência e uso de ferramentas de hacking até que um regime de salvaguardas baseado em direitos humanos esteja em vigor.*[115]

No universo dos direitos humanos, de modo mais específico, podem ser identificadas três categorias de ameaças jurídicas generalizadas, decorrentes do hacking governamental, que colocam em risco amplo[116] a garantia de um **julgamento justo**, a **validade científica**

das provas digitais e a **presunção de inocência**:[117] a) o uso inadequado e inconsistente da tecnologia (datificação, contorno tecnológico, eleição de foro das evidências, e ampliação de poderes investigatórios, incluindo ações de hacking governamental); b) desatualização das antigas garantias processuais; c) e a ausência de testes de confiabilidade. Sem que padrões e procedimentos de validação – incluindo exigências de prestação de contas e transparência – sejam previstos em lei e aplicados, a prática atual caminha para um amálgama enviesado entre as técnicas de investigação e os métodos de análise científica forense, direcionado a produzir ao mesmo tempo as evidências e suas condições de admissibilidade como prova em juízo. Nesta perspectiva, uma pessoa pode ser alvo de investigação criminal sem autorização prévia judicial e sem viabilidade efetiva de produzir provas em sua defesa que contraponham dados de seu histórico de deslocamento, trocas de mensagens, preferências de relacionamento, uso de redes sociais e fotos armazenadas, tudo submetido à análise arbitrária e desproporcional.

Além disso, pode expor a risco profissões ou atividades que tenham um caráter mais questionador e independente, como jornalistas, advogados, ativistas e políticos. Esses riscos possuem graus diversos, chegando efetivamente a promover o risco de morte: tanto na Arábia Saudita como no México, no caso do Pegasus, "as tentativas de infecção por spyware foram vinculadas ou associadas a assassinatos direcionados".[118] Nesse sentido, aponta-se o risco para a **liberdade de expressão**, até mesmo considerando como pode ser profundamente traumática, para a pessoa e para sua família, a experiência de se descobrir alvo de hackeamento ou vítima de tortura decorrente do hackeamento, além de assassinatos extrajudiciais de alvos.[119]

A geração de efeitos inibitórios sobre jornalistas afeta diretamente a liberdade de imprensa e a liberdade de expressão, ao prejudicar a possibilidade de críticas e fiscalização pública, no que também afeta, indiretamente, a democracia.[120] Ademais, também a a **democracia** é violada diretamente**,** já que as informações obtidas por tais tecnologias podem ser utilizadas não apenas para persecuções penais, mas também para disputas políticas sob determinadas agendas, como no México, que conforme o Citizen Lab,[121] as principais tentativas de infecção do Pegasus a políticos mexicanos, se deu durante o debate da lei anticorrupção. Além de afetar **soberania dos países,**[122] promovendo uma verdadeira guerra de dados, o que pode influenciar inclusive na geopolítica internacional. O Pegasus, por exemplo, pode ter sido utilizado para hackear 14 líderes mundiais,[123] o que é capaz de gerar nos países uma necessidade de ampliação das segurança e das armas digitais, aumentando a possibilidade de uma guerra cibernética.

Apesar de muito se debater sobre a responsabilidade das empresas que desenvolvem tais aplicações utilizadas para o hacking governamental, o que prevalece na prática é um **obscurecimento de informações** sobre essas empresas. Temos como exemplo, a NSO Group Technologies, em que pouco se sabe sobre sua organização financeira, tecnológica, ética, objetivos e visão, não obstante a empresa alegar que realiza a venda a países com cláusulas que condicionam o uso da tecnologia ao combate de terrorismo, e ao apoio da segurança nacional, a prática dos países mostram outros caminhos.[124]

O relatório da Citizen Lab,[125] tem demonstrado, inclusive, que a **autorregulação** das empresas, para definir os parâmetros da venda de uma tecnologia de spyware de vigilância, não se demonstra eficaz, apesar de seus argumentos de que:[126]

> *seus produtos são usados para capturar terroristas e criminosos; [que] realizam a devida diligência antes de vender seus produtos a um cliente; e [que] investigam alegações de uso indevido, tomando medidas corretivas, se necessário. [...] os regimes autorregulatórios dessas empresas se mostraram inadequados: os produtos de cada empresa foram abusados de forma a causar danos mensuráveis a defensores de direitos humanos, jornalistas, advogados que trabalham em nome de vítimas de crimes ou mídia cívica (por exemplo, blogueiros).*

No ano de 2019, inúmeras ações judiciais foram movidas contra as empresas de spyware e seus clientes, por organizações de direitos humanos e vítimas de espionagem, apesar de a curto prazo parecer a saída[127], o escopo analisado, aponta para a necessidade de uma regulamentação do uso de tal técnica, uma vez que apesar de o Hacking Governamental ser identificado em uso desde a década de noventa, foi somente no final dos anos dois mil, que a **falta de regulamentação** tem tomado enfoque para debate[128]. Sua independência enfraquece não só a segurança de dispositivos, mas a própria segurança nacional.

Outra crítica apresentada é que a não regulação é na prática uma resposta ao poder e influência exercido pelas empresas de Hacking Governamental sob os tomadores de decisões[129]. Rememora-se, que a existência de uma regulação por parte do Estado, não serve apenas para as empresas, mas também para os governos, equilibrando o poder Estatal. O Alto Comissariado das Nações Unidas para os Direitos Humanos, já se manifestou quanto a necessidade de aplicação de uma "moratória sobre a venda, transferência e uso de ferramentas de hackeamento até que um regime de salvaguardas baseado em direitos humanos esteja em vigência"[130].

A ausência de uma regulação resulta ainda, em riscos como o **uso de spywares por organizações criminosas**. Existem acusações, que o Pegasus, pode ter sido utilizado inclusive por cartéis de drogas mexicanos[131], de modo que, em caminho inverso da ampliação da segurança nacional, o uso de tecnologias para hacking governamental não incide apenas sobre a proteção nacional, mas pode ser utilizado por caminhos escusos ao desejo dos países.

Os países podem ainda utilizar-se da técnica de hacking governamental, como uma tentativa de se **esquivar da responsabilização internacional** por práticas abusivas a direitos humanos e transnacionais. Desse modo, órgãos governamentais, utilizando de uma "maquiagem" institucional de empresas privadas, podem se eximir de serem

responsabilizados, uma vez que, “Somente os Estados soberanos e outras entidades legalmente reconhecidas como atores internacionais podem estar sujeitos ao direito internacional”[132].

Ademais, questiona-se sobre a **alta onerosidade** de tais tecnologias, uma vez que o uso de técnicas de hacking para investigações exige uma atualização contínua da ferramenta, já que, na medida que é identificada a vulnerabilidade explorada, o fornecedor pode fazer a correção, o que resultaria no emprego de esforços técnicos e econômicos para a identificação de uma nova vulnerabilidade[133]. Ressalta-se que tal correção estaria condicionada ao informe estatal sobre a vulnerabilidade explorada, podendo não ser realizado pelo Estado, colocando em risco a segurança de diversos usuários[134]. Outrossim, subsiste ainda um debate ético, se o Estado teria ou não a obrigação de informar a vulnerabilidade explorada[135], pelo justo motivo que isso implicaria na necessidade de um novo investimento econômico para a exploração de outra vulnerabilidade.

Argumenta-se ainda, que a exploração de vulnerabilidades por parte do Estado, pode **desincentivar o investimento em novas técnicas de privacidade e segurança**, uma vez que torna-se “[...] mais fácil para um provedor não oferecer produtos e serviços que impeçam o provedor (e, por extensão, as agências) de acessar o texto simples das informações criptografadas.”[136] Como resultado, tem-se um efeito de resfriamento nos avanços tecnológicos neste setor, em caminho oposto ao que pode se pensar, quando se fala sobre a possibilidade de indicação de vulnerabilidades para o desenvolvimento tecnológico.

Ou mais grave, sendo todo o mercado do Hacking baseado na fabricação sistemática e comercialização de mais insegurança digital como uma mercadoria em si mesma[137] a adesão estatal pode significar um incentivo econômico explícito. A essa lógica mercantil perversa e contraproducente.

Por fim, o hacking governamental pode ampliar **abismos dialógicos entre o setor privado e poder público** Na medida em que organizações do Estado caminharem no sentido de explorar e identificar vulnerabilidades das empresas de tecnologia digital, isso poderá tornar ainda mais difícil haver diálogo sobre dados, criptografia e segurança cibernética.[138] A privatização não é exclusiva da cibersegurança, e esse tipo de problema difícil remete ao desafio das décadas de 1990 e 2000 diante da atuação de empresas privadas militares e de segurança (PMSC), cuja falta de prestação de contas e responsabilidade decorria da ausência de um quadro legal. Suas condutas transfronteiriças, com operações sigilosas e sem treinamento formal, mostraram-se propensas a transgressões.[139]

4. Conclusão

O presente trabalho buscou evidenciar como a literatura pertinente expressa diferentes perspectivas e repercussões sobre o uso de técnicas de hacking governamental por autoridades investigativas estatais como alternativa a propostas de quebra de criptografia forte em sistemas digitais. A fim de contribuir com subsídios para harmonizar segurança de tecnologias da informação e comunicação com proteção de direitos humanos e de garantias democráticas no debate político e jurídico no Brasil sobre esse conjunto de técnicas, foram analisadas 37 publicações, a partir de 04 eixos: sistematização conceitual; contexto; aspectos jurídicos; e argumentos favoráveis e contrários ao hacking governamental.

Primeiro, a par das reflexões conceituais sobre "governo", e diante da variação entre nomenclaturas amplas, como "lawful hacking", ou específicas, como "network investigative techniques", aderiu-se ao termo "hacking governamental" que, nas investigações criminais realizadas pelo poder público, denota as medidas sociais e tecnológicas de exploração de vulnerabilidades em bancos de dados, programas de computador, sistemas computacionais, redes de comunicação ou dispositivos eletrônicos a fim de acessar dados digitais sem a autorização do responsável pelo ambiente digital ou da pessoa afetada.

No estudo do contexto, apontou-se que, não obstante a percepção de que softwares de hacking governamental – inclusive de extração de dados – existam desde 1998, e da ampliação do debate com as denúncias de Edward Snowden sobre a vigilância massiva pelo governo dos EUA, o porte atual das produções decorre das revelações sobre o spyware Pegasus, da israelense NSO Group: dotado de uma diversidade ampla de recursos de coleta e monitoramento de dados, inclusive em tempo real, que serviu para catalisar a descoberta pública de muitos programas do tipo, oferecidos por outras empresas do setor, com larga atuação demonstrada contra potencialmente milhões de pessoas em vários países, inclusive no Brasil, não obstante a ausência de regras legais específicas.

Na problematização dos aspectos jurídicos, envolvendo a proteção de direitos individuais fundamentais, como privacidade e proteção de dados pessoais, entre outros, foram examinados seis pontos principais: a legalidade e a legitimidade; a observância de princípios da proporcionalidade, necessidade e adequação; o devido processo legal; a notificação de usuários, transparência e o escrutínio público; a integridade dos sistemas de comunicação; e as salvaguardas à cooperação internacional.

E no quarto eixo os argumentos favoráveis e contrários ao uso do hacking governamental foram sistematizados. As defesas mais restritivas se circunscrevem ao monitoramento e investigação de alvos específicos pelo poder público sob autorização judicial e com exploração exclusiva de vulnerabilidades pré-existentes. As contraposições à utilização de *spywares* se fundam nos riscos à privacidade e à proteção de outros direitos humanos, como práticas de vigilância em massa que afrontam a democracia nos países, além da

falta de regulação legal específica.

A conclusão desta análise aponta que, embora haja na literatura um potencial espaço para se admitir a adoção do hacking governamental para fins investigativos legítimos, desde que sejam asseguradas condições de necessidade e requisitos de proporcionalidade, prevalecem a percepção da **inviabilidade prática do respeito a essas exigências**, e a preocupação com o **perigo real de vigilantismo estatal abusivo ou mesmo de controle estatal das comunicações privadas**. E diante dessa dupla consideração, faz sentido **defender a proibição legal ou pelo menos uma imediata moratória**, não só contra a adoção estatal de ferramentas, mas contra todo esse mercado de insegurança.

Em todo caso, constata-se a urgência de que seja iniciado um debate público direcionado à crucial positivação de salvaguardas e garantias procedimentais mínimas contra erros e excessos por parte das autoridades estatais e das empresas privadas envolvidas. Tais proteções devem incluir a criação de normas legais que ofereçam parâmetros para hipóteses autorizadoras, limites e critérios de uso do hacking governamental, de modo a possibilitar sua compatibilidade com o arcabouço de direitos humanos.

Nesse sentido, apreende-se da revisão que a legitimidade das técnicas de hacking governamental depende do uso das ferramentas se amparar em critérios de necessidade, adequação, proporcionalidade, legalidade estrita, transparência e escrutínio público, bem como em prerrogativas como a do devido processo legal e a observância de todos os compromissos assumidos internacionalmente mediante tratados e convenções.

Diversamente da rastreabilidade de mensagens instantâneas e da varredura pelo lado do cliente, objeto dos estudos anteriores dessa série, observou-se que o hacking governamental conta com uma literatura bem mais numerosa e robusta. Isso pode se dever ao diferencial de que se trata de uma prática que já conta com décadas, e não de propostas emergentes para inovar no âmbito da aplicação da lei mediante a obrigação legal ou a colaboração autônoma de empresas privadas. Com décadas de implementação, o hacking governamental – com tantas finalidades e modalidades – compõe um ecossistema bastante complexo, o que agrava a noção sobre o evidente descompasso com a ausência de regulação nacional no Brasil e com o desequilíbrio na regulação internacional.

Ao longo do presente estudo, foi realizada uma revisão bibliográfica extensiva sobre os debates que permeiam a prática de hacking governamental, bem como suas repercussões sociais, jurídicas e políticas. Espera-se que a análise realizada possa ser utilizada como base para o aprofundamento das discussões em trabalhos futuros, notadamente a fim de subsidiar o amadurecimento do sistema legal de regras que definam, à luz dos direitos humanos e com mecanismos eficientes, quando se poderia empregar o hacking governamental e sob quais condições. O Brasil se mostra particularmente carente desse tipo de previsão, com práticas de segurança pública comprovadamente injustas, com um sistema de justiça que não parece capaz de coibir erros e abusos, e com alto risco de que a situação seja agravada, diante das propostas atuais em exame no Congresso Nacional.

Referências

AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022.

BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022.

BERGMAN, Ronen. U.S. Blacklists Israeli Firm NSO Group Over Spyware. **The New York Times**, 3 nov 2021. Disponível em https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.htm.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (BRASIL). "A aprovação da reforma do novo Código de Processo Penal trará nulidades e inconstitucionalidades", diz procurador de Justiça do MP/SP. **CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO**, Brasília, 24 jun. 2021. Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/14380-a-aprovacao-da-reforma-do-novo-codigo-de-processo-penal-trara-nulidades-e-inconstitucionalidades-diz-promotor-de-justica-do-mp-sp.

COALIZÃO DIREITOS NA REDE (BRASIL). Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. **COALIZÃO DIREITOS NA REDE**, Brasília, 20 maio 2021. 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: 2 fev. 2023.

DAVIS, Peter Alexander Earls. **Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation**. ELSEVIER, [s. l.], ed. 44, 2022. DOI: 10.1016/j.clsr.2022.105659. Disponível em https://www.sciencedirect.com/science/article/pii/S0267364922000073. Acesso em 26 out. 2022. p. 17.

DONEDA, Danilo; MACHADO, Diego (orgs.). **A criptografia no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2020.

ESTADOS UNIDOS DA AMÉRICA. **Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities.** U.S. Department of Commerce, 3 nov. 2021. Disponível em https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list. Acesso em 16 dez . 2022.

FUKAMI, Aya; STOYKOVA, Radina; GERADTS, Zeno. A new model for forensic data extraction from encrypted mobile devices. **Forensic Science International: Digital Investigation**, Volume 38, set. 2021, 301169. ISSN 2666-2817. DOI: 10.1016/j.fsidi.2021.301169. Disponível em https://www.sciencedirect.com/science/article/pii/S2666281721000779. Acesso em 27 out. 2022.

GALVÃO, Maria C.; RICARTE, Ivan L. M. Revisão sistemática da literatura: conceituação, produção e publicação. **Logeion: Filosofia da Informação**, [S.l.] , v. 6, n. 1, p. 57 - 73, set. 2019. P. 58. 7 - 73. Disponível em: http://revista.ibict.br/fiinf/article/view/4835. Acesso em: 10 jun. 2021.

GREENWALD, Glenn. **Sem Lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo americano.** Tradução de Fernanda Abreu. Rio de Janeiro (RJ): Sextante, 2014.

HENNESSEY, Susan. Lawful Hacking and the Case for a Strategic Approach to 'Going Dark'. O'HANLON, Michael E. **Brookings Big Ideas for America**. Brookings Institution Press, 31 jan. 2017. Pp. 241-250. Disponível em https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/. Acesso em 28 out. 20222.

JARVIS, Craig. **Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption.** CRC Press, 2020.

JOHN, Scott-Railton; BILL, Marczak; BAHR, Abdul Razzak; MASASHI, Crete-Nishihata; RON, Deibert. Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware. **Citizen Lab Research Report nº 94**. University of Toronto, jun. 2017. Disponível em https://citizenlab.ca/2017/06/more-mexican-nso-targets/. Acesso em 24 out. 2022.

KAYE, David A., The Spyware State and the Prospects for Accountability. Global Governance, Vol. 27, Nº 4, 2021, Forthcoming, **UC Irvine School of Law Research Paper nº 2021-58**, 20 dez. 2021. Available at SSRN. Disponível em: https://ssrn.com/abstract=3990249. Acesso em 14 nov. 2022.

KERR, Orin S.; MURPHY, Sean D.. Government Hacking to Light the Dark Web: What Risks to International Relations and International Law? 24 abr. 2017. **70 Stanford Law Review Online 58 (Jul. 2017)**. Pp. 58-69. Disponível em https://ssrn.com/abstract=2957361. Acesso em: 26 out. 2022.

KOOPS, Bert-Jaap; KOSTA, Eleni. Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". **Computer law & security review**, [s. l.], v. 34, p. 8990-900, 2018. p. 898-899. Disponível em: https://drive.google.com/file/d/1YX6rHZfaMTJ2wTM2WGzv4sHCnyqkpsnd/view. Acesso em: 11 nov. 2022.

LEANDER, Anna. Parsing Pegasus: An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics. **Swiss Political Science Review**, v. 27, n. 1, p. 205-213, 2021. Disponível em https://onlinelibrary.wiley.com/doi/epdf/10.1111/spsr.12441. Acesso em 1 nov. 2022.

LI, Chen-Yu et al. A Comprehensive Overview of Government Hacking Worldwide. **IEEE Access,** [s. l.], v. 6, 24 set. 2018. DOI 10.1109/ACCESS.2018.2871762. Disponível em: https://ieeexplore.ieee.org/document/8470931. Acesso em: 24 out. 2022.

LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. **Michigan Telecommunications and Technology Law Review**, Vol. 26, No. 2, 2020, Available at SSRN. Disponível: https://ssrn.com/abstract=3606601. Acesso em: 13 de nov. de 2022.

MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. **Citizen Lab Research Report Nº 124.** University of Toronto, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Acesso em 09 nov. 2022.

MARCZAK, Bill; SCOTT-RAILTON, John; SENFT, Adam; RAZZAK, Bahr Abdul; DEIBERT, Ron. The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. **Citizen Lab Research Report nº 115**. University of Toronto, out. 2018. Disponível em: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

MARZOCCHI, Ottavio; MAZZINI, Martina. **Pegasus and surveillance spyware.** EPRS: European Parliamentary Research Service. 06 mai. 2022. Disponível em https://www.europarl.europa.eu/committees/pt/pega/supporting-analyses/latest-documents. Acesso em 10 nov. 2022.

MAYER, Jonathan. Government Hacking. **The Yale Law Journal**, 2018. Disponível em: https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf. Acesso em: 1 nov. 2022.

MORAES, Thiago. Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures. **European Data Protection Law Review**, Volume 6, Issue 1 (2020), pp. 41 - 55. DOI: https://doi.org/10.21552/edpl/2020/1/7. Disponível em https://edpl.lexxion.eu/article/EDPL/2020/1/7. Acesso em 09 nov. 2022.

ONU. Escritório do Alto Comissariado para Direitos Humanos. **The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights**. Genebra, 4 ago. 2022. Disponível em https://digitallibrary.un.org/

record/3985679?ln=es. Acesso em: 17 nov. 2022.

PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 19 de abril de 2022.

PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente: uma revisão sistemática.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, novembro de 2022. Disponível em bit.ly/3EAhEDF. Acesso em: 30 nov. 2022.

PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. **STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment**, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. doi:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375. Acesso em 12 de nov. de 2022.

RAMIRO, André; AMARAL, Pedro; PEREIRA, Marcos Cesar M. Insegurança Distribuída: Economia E Regulação Do Hacking Governamental. **IV Encontro Da Rede De Pesquisa Em Governança Da Internet - REDE 2021**, [s. l.], out. 2021. Disponível em: http://redegovernanca.net.br/index.php/encontro-anual/encontro-anual/paper/view/106. Acesso em: 14 nov. 2022.

RAMIRO, André (coord.); CANTO, Mariana; REAL, Paula Côrte; LIMA, José Paulo; AGUIAR, Thaís. **O Mosaico Legislativo da Criptografia no Brasil: uma análise de projetos de Lei.** IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 05 ago. 2020. Disponível em https://obcrypto.org/estudo/o-mosaico-legislativo-da-criptografia-no-brasil-uma-analise-de-projetos-de-lei/. Acesso em: 10 nov. 2022.

REUTERS. 'Five Eyes' security alliance calls for access to encrypted material. **Reuters**, 30 jul. 2019. Disponível em: https://www.reuters.com/article/us-security-fiveeyes-britain-idUSKCN1UP199. Acesso em: 28 abr. 2022.

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, v. 8, nº 3, Porto Alegre, set-dez. 2022, 1463-1500. DOI:10.22197/rbdpp.v8i3.723. Disponível em https://revista.ibraspp.com.br/RBDPP/article/view/723. Acesso em: 1 dez. 2022.

RODRIGUES, Gustavo Ramos. **Hacking governamental e a indústria da insegurança digital.** IRIS - Instituto de Referência em Internet e Sociedade, 23 ago. 2021. Disponível em https://irisbh.com.br/hacking-governamental-e-a-industria-da-inseguranca-digital/.

Acesso em 15 nov. 2022.

RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, maio de 2022. Disponível em https://bit.ly/3yLlb0P. Acesso em: 30 nov. 2022.

ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. **Revista de Investigación en Tecnologías de la Información**, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI: 10.36825/riti.07.14.003. Data de acesso: 24 out. 2022.

ROZENSHTEIN, Alan Z. Wicked Crypto. **U.C. Irvine Law Review**, Vol. 9, N. 5 (Jul. 2019): Women, Law, Society, & Technology, 1181-1215. Disponível em https://scholarship.law.uci.edu/ucilr/vol9/iss5/6/. Acesso em 10 nov. 2022.

RUDIE, JD; KATZ, Zach; KUHBANDER, Sam; BHUNIA, Suman. Technical Analysis of the NSO Group's Pegasus Spyware. **2021 International Conference on Computational Science and Computational Intelligence (CSCI)**, Las Vegas (NV), EUA, dez. 2021 pp. 747-752. DOI: 10.1109/CSCI54926.2021.00188. Disponível em https://ieeexplore.ieee.org/document/9799180 e https://www.computer.org/csdl/proceedings-article/csci/2021/584100a747/1EpL7AEhgxa. Acesso em: 8 nov. 2022.

SAMPAIO, R. F.; MANCINI, M. C. Estudos de Revisão Sistemática: um guia para síntese criteriosa da evidência científica. **Revista Brasileira de Fisioterapia**, São Carlos, v. 11, n. 1., p. 83-89, 2007.

SENADO FEDERAL (BRASIL). Professores criticam proposta de reforma de Código Penal em tramitação no Senado. **Agência Senado**, Brasília, 8 ago. 2017. Disponível em: https://www12.senado.leg.br/noticias/materias/2017/08/08/professores-criticam-proposta-de-reforma-de-codigo-penal-em-tramitacao-no-senado.

SCHULZE, M. Clipper meets Apple vs. FBI – a comparison of the cryptography discourses from 1993 and 2016. **Media and Communication**, v. 5, n. 1, p. 54-62, 22 mar. 2017.

SOMMER, Peter. Evidence from hacking: A few tiresome problems. **Forensic Science International: Digital Investigation**, v. 40, p. 301-333, 2022. DOI: 10.1016/j.fsidi.2022.301333. Disponível em https://www.sciencedirect.com/science/article/pii/S2666281722000026. Acesso em 31 out. 2022.

STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking.** Access Now, set. 2016. Disponível em https://www.

Notas

1 O primeiro relatório, sobre o panorama da rastreabilidade de mensagens instantâneas (RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, maio de 2022. Disponível em https://bit.ly/3yLlb0P. Acesso em: 30 nov. 2022), e o segundo, sobre varredura pelo lado do cliente (PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente: uma revisão sistemática**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, novembro de 2022. Disponível em bit.ly/3EAhEDF. Acesso em: 30 nov. 2022), foram publicados em maio e novembro de 2022.

2 Uma discussão em detalhes sobre os diversos aspectos pertinentes e as percepções quanto às propostas de inserção de mecanismos de acesso excepcional em ambientes com criptografia foi objeto de um estudo prévio conduzido pelo IRIS (PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 19 de abril de 2022).

3 "O conflito sobre o grau em que cidadãos deveriam ser autorizados a acessar criptografia, tecnologia capaz de colocar seus segredos além do alcance do Estado, é conhecido como guerras criptográficas" – Tradução para o original "The conflict over the degree to which citizens should be permitted access to encryption, to technology capable of placing their secrets beyond the reach of their governments, is known as the crypto wars" (JARVIS, Craig. **Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption**. CRC Press, 2020. P. xi).

4 SCHULZE, M. Clipper meets Apple vs. FBI – a comparison of the cryptography discourses from 1993 and 2016. **Media and Communication**, v. 5, n. 1, p. 54-62, 22 mar. 2017.

5 **REUTERS**. 'Five Eyes' security alliance calls for access to encrypted material. Reuters, 30 jul. 2019. Disponível em: https://www.reuters.com/article/us-security-fiveeyes-britain-idUSKCN1UP199. Acesso em: 28 abr. 2022.

6 SCHULZE, M. Clipper meets Apple vs. FBI – a comparison of the cryptography discourses from 1993 and 2016. **Media and Communication**, v. 5, n. 1, p. 54-62, 22 mar. 2017.

7 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil:**

mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 11 de nov. de 2022.

8 LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. **Michigan Telecommunications and Technology Law Review**, Vol. 26, No. 2, 2020, Available at SSRN. Disponível: https://ssrn.com/abstract=3606601. Acesso em: 13 de nov. de 2022.

9 GREENWALD, Glenn. **Sem Lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo americano**. Tradução de Fernanda Abreu. Rio de Janeiro (RJ): Sextante, 2014. P. 152.

10 MARZOCCHI, Ottavio; MAZZINI, Martina. **Pegasus and surveillance spyware**. **EPRS: European Parliamentary Research Service**. 06 mai. 2022. Disponível em https://www.europarl.europa.eu/committees/pt/pega/supporting-analyses/latest-documents. Acesso em 10 nov. 2022.

11 GALVÃO, Maria C.; RICARTE, Ivan L. M. Revisão sistemática da literatura: conceituação, produção e publicação. **Logeion: Filosofia da Informação**, [S.l.] , v. 6, n. 1, p. 57 - 73, set. 2019. P. 58. 7 - 73. Disponível em: http://revista.ibict.br/fiinf/article/view/4835. Acesso em: 10 jun. 2021.

12 SAMPAIO, R. F.; MANCINI, M. C. Estudos de Revisão Sistemática: um guia para síntese criteriosa da evidência científica. **Revista Brasileira de Fisioterapia**, São Carlos, v. 11, n. 1., p. 83-89, 2007. p. 84.

13 Scopus. https://www.scopus.com/search/form.uri?display=basic#.

14 ONU. Escritório do Alto Comissariado para Direitos Humanos. **The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights**. Genebra, 4 ago. 2022. Disponível em https://digitallibrary.un.org/record/3985679?ln=es. Acesso em: 17 nov. 2022.

15 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022.

16 AMARAL, Pedro; CANTO, Mariana; PEREIRA, César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022.

17 BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY. Não Entre em Pânico: Avançando no debate sobre "obscurecimento" (Going Dark). 2018. Tradução: Instituto de Tecnologia e Sociedade do Rio – ITS-Rio. Disponível em https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf. Acesso em: 01/02/2023.

18 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 10.

19 "O primeiro desafio em trazer o tópico para o debate brasileiro é a própria tradução da expressão lawful/government hacking: para abarcar corretamente o conceito, teríamos algo como 'hacking autorizado por lei e conduzido para fins de investigação criminal'" (LIGUORI, Carlos. Direito e Criptografia: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia. São Paulo : SaraivaJur, 2022. P. 250).

20 AMARAL, Pedro; CANTO, Mariana; PEREIRA, César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 6-7, nota de rodapé 16.

21 Alinham-se a essa conceituação de hacking governamental, por exemplo:

a. LI, Chen-Yu et al. A Comprehensive Overview of Government Hacking Worldwide. **IEEE Access**, [s. l.], v. 6, 24 set. 2018. DOI 10.1109/ACCESS.2018.2871762. Disponível em: https://ieeexplore.ieee.org/document/8470931. Acesso em: 24 out. 2022.

b. LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. **Michigan Telecommunications and Technology Law Review**, Vol. 26, No. 2, 2020. DOI: 10.36645/mtlr.26.2.exploring. Disponível em https://repository.law.umich.edu/mtlr/vol26/iss2/5/. Acesso em: 13 nov. 2022.

c. STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 10-11.

Especificamente sobre vulnerabilidade e outros conceitos correlatos (exploit, payload, spoofing, dropper, man-in-the-middle attack), ver BELLOVIN, Steven M.; BLAZE, Matt;

CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. Pp. 22-23.

22 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 11 de nov. de 2022.

23 LI, Chen-Yu et al. A Comprehensive Overview of Government Hacking Worldwide. **IEEE Access**, [s. l.], v. 6, 24 set. 2018, p. 7. DOI 10.1109/ACCESS.2018.2871762. Disponível em: https://ieeexplore.ieee.org/document/8470931. Acesso em: 24 out. 2022.

24 MORAES, Thiago. Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures. **European Data Protection Law Review**, Volume 6, Issue 1 (2020), pp. 41 - 55. DOI: https://doi.org/10.21552/edpl/2020/1/7. Disponível em https://edpl.lexxion.eu/article/EDPL/2020/1/7. Acesso em 09 nov. 2022.

25 PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. **STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment**, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. doi:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375. Acesso em 12 de nov. de 2022.

26 AMARAL, Pedro; CANTO, Mariana; PEREIRA, César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022.

27 KOOPS, Bert-Jaap; KOSTA, Eleni. Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". **Computer law & security review**, [s. l.], v. 34, p. 8990-900, 2018. p. 898-899. Disponível em: https://drive.google.com/file/d/1YX6rHZfaMTJ2wTM2WGzv4sHCnyqkpsnd/view. Acesso em: 11 nov. 2022.

28 MAYER, Jonathan. Government Hacking. **The Yale Law Journal**, 2018. Disponível em: https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf. Acesso em: 1 nov. 2022.

29 RUDIE, JD; KATZ, Zach; KUHBANDER, Sam; BHUNIA, Suman. Technical Analysis of

the NSO Group's Pegasus Spyware. **2021 International Conference on Computational Science and Computational Intelligence (CSCI)**, Las Vegas (NV), EUA, dez. 2021 pp. 747-752. DOI: 10.1109/CSCI54926.2021.00188. Disponível em https://ieeexplore.ieee.org/document/9799180 e https://www.computer.org/csdl/proceedings-article/csci/2021/584100a747/1EpL7AEhgxa. Acesso em: 8 nov. 2022.

30 ONU. Escritório do Alto Comissariado para Direitos Humanos. **The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights**. Genebra, 4 ago. 2022. Disponível em https://digitallibrary.un.org/record/3985679?ln=es. Acesso em: 17 nov. 2022.

31 RAMIRO, André; AMARAL, Pedro; PEREIRA, Marcos Cesar M. Insegurança Distribuída: Economia E Regulação Do Hacking Governamental. **IV Encontro Da Rede De Pesquisa Em Governança Da Internet - REDE 2021**, [s. l.], out. 2021. Disponível em: http://redegovernanca.net.br/index.php/encontro-anual/encontro-anual/paper/view/106. Acesso em: 14 nov. 2022.

32 HENNESSEY, Susan. Lawful Hacking and the Case for a Strategic Approach to 'Going Dark'. O'HANLON, Michael E. **Brookings Big Ideas for America**. Brookings Institution Press, 31 jan. 2017. Pp. 241-250. Disponível em https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/. Acesso em 28 out. 20222.

33 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 11.

34 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. Pp. 17-18.

35 MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. **Citizen Lab Research Report Nº 124 University of Toronto**, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Acesso em 09 nov. 2022.

36 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights**

Response to Government Hacking. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. Pp. 17-18.

37 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. Pp. 19-22.

38 No contexto específico do hacking, exploit se refere ao meio – um programa de computador, um conjunto de comandos ou um conjunto de ações – para se explorar uma determinada vulnerabilidade e obter o desejado acesso não autorizado (BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. Pp. 23.).

39 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. Pp. 25.

40 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. P. 25.

41 RUDIE, JD; KATZ, Zach; KUHBANDER, Sam; BHUNIA, Suman. Technical Analysis of the NSO Group's Pegasus Spyware. **2021 International Conference on Computational Science and Computational Intelligence (CSCI)**, Las Vegas (NV), EUA, dez. 2021 pp. 747-752. DOI: 10.1109/CSCI54926.2021.00188. Disponível em https://ieeexplore.ieee.org/document/9799180 e https://www.computer.org/csdl/proceedings-article/csci/2021/584100a747/1EpL7AEhgxa. Acesso em: 8 nov. 2022. P. 747-748.

42 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. Pp. 22-24.

43 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. P. 25.

44 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 11.

45 MAYER, Jonathan. Government Hacking. **The Yale Law Journal**, 2018. Disponível em: https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf. Acesso em: 1 nov. 2022. P. 13.

46 Ver DONEDA, Danilo; MACHADO, Diego (orgs.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020.

47 As denúncias tiveram cobertura pelos "jornais Washington Post, The Guardian, Le Monde e 14 outras organizações de mídia ao redor do mundo" (TORRES, Ricardo José. **Respeito ao jornalismo: a violência contra os jornalistas não pode ser naturalizada**. objETHOS - Observatório da Ética Jornalística, 2 ago. 2021. Disponível em https://objethos.wordpress.com/2021/08/02/respeito-ao-jornalismo-a-violencia-contra-os-jornalistas-nao-pode-ser-naturalizada. Acesso em 14 nov. 2022).

48 RAMIRO, André; AMARAL, Pedro; PEREIRA, Marcos Cesar M. Insegurança Distribuída: Economia E Regulação Do Hacking Governamental. **IV Encontro Da Rede De Pesquisa Em Governança Da Internet - REDE 2021**, [s. l.], out. 2021. Disponível em: http://redegovernanca.net.br/index.php/encontro-anual/encontro-anual/paper/view/106. Acesso em: 14 nov. 2022.

49 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 11 de nov. de 2022.

50 Exemplificam as críticas ao projeto de reforma ao Código de Processo Penal: SENADO FEDERAL (BRASIL). Professores criticam proposta de reforma de Código Penal em tramitação no Senado. **Agência Senado**, Brasília, 8 ago. 2017. Disponível em https://www12.senado.leg.br/noticias/materias/2017/08/08/professores-criticam-proposta-de-reforma-de-codigo-penal-em-tramitacao-no-senado. Acesso em: 01 fev. 2023.; **CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO** (BRASIL). "A aprovação da reforma do novo Código de Processo Penal trará nulidades e inconstitucionalidades", diz procurador de Justiça do MP/SP. Conselho Nacional Do Ministério Público, Brasília, 24 jun. 2021. Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/14380-a-aprovacao-da-reforma-do-novo-codigo-de-processo-penal-trara-nulidades-e-inconstitucionalidades-diz-promotor-de-justica-do-mp-sp. Acesso em: 2 fev. 2023.; COALIZÃO DIREITOS NA REDE. Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. Coalizão Direitos na Rede,

S.l., 20 mai. 2021. 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: 02 fev. 2023.

51 RODRIGUES, Gustavo. **Hacking governamental e a indústria da insegurança digital**. IRIS - Instituto de Referência em Internet e Sociedade, 23 ago. 2021. Disponível em https://irisbh.com.br/hacking-governamental-e-a-industria-da-inseguranca-digital/. Acesso em 15 nov. 2022.

52 Um estudo do IP.rec listou "sinais e tentativas de se adquirir o Pegasus" no Brasil pelo menos desde 2017: descoberta em 2018 de dispositivo infectado desde 21017; delegado anunciou entusiasmado ter recebido a oferta do spyware por 2,7 milhões de reais; denúncia de que a Operação Lava-Jato teria negociado a aquisição do Pegasus; e notícia sobre ter Carlos Bolsonaro interferido no Ministério da Justiça para municiar a ABIN (AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 8)

53 MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. **Citizen Lab Research Report Nº 124**. University of Toronto, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Acesso em 09 nov. 2022.

54 RUDIE, JD; KATZ, Zach; KUHBANDER, Sam; BHUNIA, Suman. Technical Analysis of the NSO Group's Pegasus Spyware. **2021 International Conference on Computational Science and Computational Intelligence (CSCI)**, Las Vegas (NV), EUA, dez. 2021 pp. 747-752. DOI: 10.1109/CSCI54926.2021.00188. Disponível em https://ieeexplore.ieee.org/document/9799180 e https://www.computer.org/csdl/proceedings-article/csci/2021/584100a747/1EpL7AEhgxa. Acesso em: 8 nov. 2022. p. 748.

55 ESTADOS UNIDOS DA AMÉRICA. **Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities**. U.S. Department of Commerce, 3 nov. 2021. Disponível em https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list. Acesso em 16 dez . 2022.

56 BERGMAN, Ronen. U.S. Blacklists Israeli Firm NSO Group Over Spyware. **The New York Times**, 3 nov 2021. Disponível em https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html. Acesso em 16 dez 2022.

57 ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. **Revista de Investigación en Tecnologías de la Información**, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI: 10.36825/riti.07.14.003. Data de acesso: 24 out. 2022. p. 28.

58 ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. **Revista de Investigación en Tecnologías de la Información**, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI:10.36825/riti.07.14.003. Data de acesso: 24 out. 2022. p. 28.

59 ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. **Revista de Investigación en Tecnologías de la Información**, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI:10.36825/riti.07.14.003. Data de acesso: 24 out. 2022. p. 27.

60 ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. **Revista de Investigación en Tecnologías de la Información**, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI:10.36825/riti.07.14.003. Data de acesso: 24 out. 2022. p. 28.

61 RUDIE, JD; KATZ, Zach; KUHBANDER, Sam; BHUNIA, Suman. Technical Analysis of the NSO Group's Pegasus Spyware. **2021 International Conference on Computational Science and Computational Intelligence (CSCI)**, Las Vegas (NV), EUA, dez. 2021 pp. 747-752. DOI: 10.1109/CSCI54926.2021.00188. Disponível em https://ieeexplore.ieee.org/document/9799180 e https://www.computer.org/csdl/proceedings-article/csci/2021/584100a747/1EpL7AEhgxa. Acesso em: 8 nov. 2022.

62 PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. **STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment**, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. doi:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375. Acesso em 12 de nov. de 2022. P. 265.

63 PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. **STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment**, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. doi:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375. Acesso em 12 de nov. de 2022. P. 265.

64 MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. **Citizen Lab Research Report Nº 124**. University of Toronto, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Acesso em 09 nov. 2022.

65 JOHN, Scott-Railton; BILL, Marczak; BAHR, Abdul Razzak; MASASHI, Crete-Nishihata; RON, Deibert. Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware. Citizen Lab Research Report nº 94. University of Toronto, jun. 2017. Disponível em https://citizenlab.ca/2017/06/more-mexican-nso-targets/. Acesso em 24 out. 2022.

66 JOHN, Scott-Railton; BILL, Marczak; BAHR, Abdul Razzak; MASASHI, Crete-Nishihata; RON, Deibert. Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware. Citizen Lab Research Report nº 94. University of Toronto, jun. 2017. Disponível em https://citizenlab.ca/2017/06/more-mexican-nso-targets/. Acesso em 24 out. 2022.

67 MARCZAK, Bill; SCOTT-RAILTON, John; SENFT, Adam; RAZZAK, Bahr Abdul; DEIBERT, Ron. The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. **Citizen Lab Research Report nº 115**. University of Toronto, out. 2018. Disponível em: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/. Acesso em 3 nov. 2022.

68 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 3.

69 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022.

70 MARCZAK, Bill; SCOTT-RAILTON, John; SENFT, Adam; RAZZAK, Bahr Abdul; DEIBERT, Ron. The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. **Citizen Lab Research Report nº 115**. University of Toronto, out. 2018. Disponível em: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/. Acesso em 3 nov. 2022.

71 SARTOR, Giovanni; LORREGGIA, Andrea. The impact of Pegasus on fundamental

rights and democratic processes. **European Union**, 21 dez. 2022. https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740514. Acesso em 02 fev. 2022.

72 MARZOCCHI, Ottavio; MAZZINI, Martina. Pegasus and surveillance spyware. MARZOCCHI, Ottavio; MAZZINI, Martina. Pegasus and surveillance spyware. **EPRS: European Parliamentary Research Service**, 06 mai. 2022. Disponível em https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf. Acesso em 02 fev. 2022.

73 MARCZAK, Bill; SCOTT-RAILTON, John; SENFT, Adam; RAZZAK, Bahr Abdul; DEIBERT, Ron. The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. **Citizen Lab Research Report nº 115**. University of Toronto, out. 2018. Disponível em: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/. Acesso em 3 nov. 2022.

74 RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, v. 8, nº 3, Porto Alegre, set-dez. 2022, 1463-1500. DOI:10.22197/rbdpp.v8i3.723. Disponível em https://revista.ibraspp.com.br/RBDPP/article/view/723. Acesso em: 1 dez. 2022. P. 1.465.

75 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 21.

76 VALENÇA, Lucas. Carlos Bolsonaro intervém em compra de aparelho espião e cria crise militar. **UOL Notícias**, 19 mai. 2021. Disponível em https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-orgaos-de-inteligencia.htm. Acesso em 01 dez. 2022.

77 "O Sherlock, por meio do Devi'ls Tongue, aproveita falhas no Windows, utilizando-se de "bugs" do sistema operacional para invadir as máquinas. A maioria dos computadores do governo utiliza o programa da Microsoft.

"Diferentemente do Pegasus, porém, o Sherlock não seria utilizado pelo governo como um 'spyware' contra jornalistas, ativistas e desafetos políticos. O Sherlock serviria, sim, para municiar os Bolsonaros contra possíveis problemas internos no governo." (VALENÇA, Lucas. Além do Pegasus, Carlos Bolsonaro queria sistema para monitorar o Planalto. **UOL Notícias**, 3 ago. 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. Acesso em 1 dez. 2022).

78 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 80.

79 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 1.

80 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022.

81 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 49.

82 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 2.

83 RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, v. 8, nº 3, Porto Alegre, set-dez. 2022, 1463-1500. DOI:10.22197/rbdpp.v8i3.723. Disponível em https://revista.ibraspp.com.br/RBDPP/article/view/723. Acesso em: 1 dez. 2022. Pp. 1.479.

84 RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, v. 8, nº 3, Porto Alegre, set-dez. 2022, 1463-1500. DOI:10.22197/rbdpp.v8i3.723. Disponível em https://revista.ibraspp.com.br/RBDPP/article/view/723. Acesso em: 1 dez. 2022. Pp. 1.478-1.491.

85 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 10.

86 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. PP. 19-22.

87 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 20.

88 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. PP. 20-21.

89 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. P. 44.

90 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. PP. 21.

91 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. PP. 21-22.

92 Para mais informações, ver: PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em https://bit.ly/3kGTde3. Acesso em 15 dez. 2022. E também: RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. Disponível em https://bit.ly/3yLlb0P. Acesso em: 15 dez. 2022.

93 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 22.

94 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. P. 22.

95 Foram encontrados, por exemplo, textos relacionados ao ambiente regulatório dos Estados Unidos: MAYER, Jonathan. Constitutional Malware. 14 de nov. de 2016. Available at SSRN. Disponível em: https://ssrn.com/abstract=2633247. Aceso em 09 de novembro de 2022. Da Índia: HRIVASTAVA, Sanskriti; KEJRIWAL, Muskan. PEGASUS SPYWARE:: EVALUATING THE NEED FOR SURVEILLANCE REFORM AND INTRODUCTION OF DATA PROTECTION BILL. Institute of Law Nirma University Nirma University, [s. l.], 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4171776. Acesso em: 18 nov. 2022. E também da Austrália: FARLOW, Harriet; M. EDWARDS , Belinda. Shining a light on 'going dark':: A framework to guide the co-design and communication of decryption laws based on the passage of the Telecommunications and Other Legislation (Assistance and Access) Bill 2018. **Computer law & security review**, [s. l.], 2022. DOI https://doi.org/10.1016/j.clsr.2022.105726. Disponível em: https://linkinghub.elsevier.com/retrieve/pii/S0267364922000681. Acesso em: 17 nov. 2022.

96 LEANDER, Anna. Parsing Pegasus: An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics. Swiss Political Science Review, v. 27, n. 1, p. 205-213, 2021. Disponível em https://onlinelibrary.wiley.com/doi/epdf/10.1111/spsr.12441. Acesso em 1 nov. 2022. Pp. 5-6.

97 DONAHUE, James L. A comparative analysis of international encryption policies en route to a domestic solution. 2018. 169 p. Thesis (Master Of Arts In Security Studies) - Naval Postgraduate School, [S. l.], 2018. Disponível em: https://calhoun.nps.edu/handle/10945/58291. Pp. 7-8.

98 LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. **Michigan Telecommunications and Technology Law Review**, Vol. 26, No. 2, 2020. DOI: 10.36645/mtlr.26.2.exploring. Disponível em https://repository.law.umich.edu/mtlr/vol26/iss2/5/.

99 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022.

100 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022.

101 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022.

102 BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. **12 Nw. J. Tech. & Intell. Prop. 1** (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1. Acesso em 23 nov. 2022. P. 27-31.

103 HENNESSEY, Susan. Lawful Hacking and the Case for a Strategic Approach to 'Going Dark'. O'HANLON, Michael E. **Brookings Big Ideas for America**. Brookings Institution Press, 31 jan. 2017. Pp. 241-250. Disponível em https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/. Acesso em 28 out. 20222.

104 DONAHUE, James L. A comparative analysis of international encryption policies en route to a domestic solution. 2018. 169 p. Thesis (Master Of Arts In Security Studies) - Naval Postgraduate School, [S. l.], 2018. Disponível em: https://calhoun.nps.edu/handle/10945/58291. Pp. 13-14.

105 KOOPS, Bert-Jaap; KOSTA, Eleni. Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". **Computer law & security review**, [s. l.], v. 34, p. 8990-900, 2018. p. 898-899. Disponível em: https://drive.google.com/file/d/1YX6rHZfaMTJ2wTM2WGzv4sHCnyqkpsnd/view. Acesso em: 11 nov. 2022. P. 890.

106 KOOPS, Bert-Jaap; KOSTA, Eleni. Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". **Computer law & security review**, [s. l.], v. 34, p. 8990-900, 2018. p. 898-899. Disponível em: https://drive.google.com/file/d/1YX6rHZfaMTJ2wTM2WGzv4sHCnyqkpsnd/view. Acesso em: 11 nov. 2022. P. 900.

107 KERR, Orin S.; MURPHY, Sean D.. Government Hacking to Light the Dark Web: What Risks to International Relations and International Law? 24 abr. 2017. **70 Stanford Law Review Online 58 (Jul. 2017)**. Pp. 58-69. Disponível em https://ssrn.com/abstract=2957361. Acesso em: 26 out. 2022.

108 HENNESSEY, Susan. Lawful Hacking and the Case for a Strategic Approach to 'Going Dark'. O'HANLON, Michael E. **Brookings Big Ideas for America**. Brookings Institution Press, 31 jan. 2017. Pp. 241-250. Disponível em https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/. Acesso em 28 out. 20222.

109 SOMMER, Peter. Evidence from hacking: A few tiresome problems. **Forensic Science International: Digital Investigation**, v. 40, p. 301-333, 2022. DOI: 10.1016/j.fsidi.2022.301333. Disponível em https://www.sciencedirect.com/science/article/pii/S2666281722000026. Acesso em 31 out. 2022.

110 STOYKOVA, Radina; NORDVIK, Rune; FRANKE, Katrin; AXELSSON, Stefan; AHMED, Munnazzar; TOOLAN, Fergus. Legal and technical questions of file system reverse engineering. **Computer Law & Security Review**, [s. l.], v. 46, September 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364922000693. Acesso em: 02 de fev. de 2022.

111 LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. **Michigan Telecommunications and Technology Law Review**, Vol. 26, No. 2, 2020, Available at SSRN. Disponível: https://ssrn.com/abstract=3606601. Acesso em: 13 de nov. de 2022.

112 KERR, Orin S.; MURPHY, Sean D.. Government Hacking to Light the Dark Web: What Risks to International Relations and International Law? 24 abr. 2017. **70 Stanford Law Review Online 58 (Jul. 2017)**. Pp. 58-69. Disponível em https://ssrn.com/abstract=2957361. Acesso em: 26 out. 2022.

113 PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. **STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment**, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. doi:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375. Acesso em 12 de nov. de 2022.

114 RAMIRO, André; AMARAL, Pedro; PEREIRA, Marcos Cesar M. Insegurança Distribuída: Economia E Regulação Do Hacking Governamental. **IV Encontro Da Rede De Pesquisa Em Governança Da Internet - REDE 2021**, [s. l.], out. 2021. Disponível em: http://redegovernanca.net.br/index.php/encontro-anual/encontro-anual/paper/view/106. Acesso em: 14 nov. 2022.

115 ONU. Escritório do Alto Comissariado para Direitos Humanos. **The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights**. Genebra, 4 ago. 2022. Disponível em https://digitallibrary.un.org/record/3985679?ln=es. Acesso em: 17 nov. 2022. P. 6.

116 Com relação ao impacto negativo do uso dessas ferramentas no que tange aos direitos ao devido processo e a um julgamento justo, importante destacar o precedente estabelecido pela Sexta Turma do Superior Tribunal de Justiça no julgamento do RHC 99.735 - SC11 e confirmado no julgamento do RHC nº 79.848 - PE. "A aplicação dos entendimentos firmados por esses precedentes ao emprego de ferramentas de espionagem para fins de produção probatória implica na compreensão de que é vedada a produção probatória realizada por ferramentas de software espião que permitam: i) o monitoramento simultaneamente retroativo e progressivo das comunicações; ou ii) a alteração dos conteúdos acessados. Nesse sentido, importa destacar que o processo penal deve ser regido pelo princípio da legalidade estrita: somente o que está legalmente previsto pode ser admitido, jamais o contrário.". DUTRA, Luiza Correa de Magalhães; GOMES, Ana Bárbara; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva. Recomendações sobre privacidade das comunicações, investigações e direitos digitais. Belo Horizonte: Instituto de Referência em Internet e Sociedade, dezembro de 2022. Disponível em http://bit.ly/3ViK38I. Acesso em: 02 fev. 2023. Pp. 9-11.

117 STOYKOVA, Radina. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. **Computer Law & Security Review**, v. 42, 2021. DOI: 10.1016/j.clsr.2021.105575. Disponível em https://www.sciencedirect.com/science/article/pii/S0267364921000480.

118 MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. **Citizen Lab Research Report Nº 124**. University of Toronto, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Acesso em 09 nov. 2022. p. 10.

119 ONU. Escritório do Alto Comissariado para Direitos Humanos. **The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights**. Genebra, 4 ago. 2022. Disponível em https://digitallibrary.un.org/record/3985679?ln=es. Acesso em: 17 nov. 2022. P. 4.

120 A título exemplificativo, tem-se a decisão da Suprema Corte Indiana que sugere que a existência de ferramentas como o Pegasus coloca em risco o papel de fiscalização pública da imprensa, do qual depende a democracia, pelo efeito inibitório que pode ser imposto sobre jornalistas.https://timesofindia.indiatimes.com/india/snooping-can-have-chilling-effect-on-press-freedom-sc/articleshow/87320807.cms

121 JOHN, Scott-Railton; BILL, Marczak; BAHR, Abdul Razzak; MASASHI, Crete-Nishihata; RON, Deibert. Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware. **Citizen Lab Research Report nº 94**. University of Toronto, jun. 2017. Disponível em https://citizenlab.ca/2017/06/more-mexican-nso-targets/. Acesso em 24 out. 2022.

122 ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. **Revista de Investigación en Tecnologías de la Información**, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI:10.36825/riti.07.14.003. Data de acesso: 24 out. 2022. P. 28.

123 PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. **STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment**, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. doi:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375. Acesso em 12 de nov. de 2022.

124 ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. **Revista de Investigación en Tecnologías de la Información**, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI:10.36825/riti.07.14.003. Data de acesso: 24 out. 2022. p. 28.

125 MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. **Citizen Lab Research Report Nº 124**. University of Toronto, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Acesso em 09 nov. 2022.

126 MARCZAK, Bill; SCOTT-RAILTON, John; SENFT, Adam; RAZZAK, Bahr Abdul; DEIBERT, Ron. The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. **Citizen Lab Research Report nº 115**. University of Toronto, out. 2018. Disponível em: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/. Acesso em 3 nov. 2022. p. 17.

127 MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. **Citizen Lab Research Report Nº 124**. University of Toronto, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Acesso em 09 nov. 2022.

128 LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. **Michigan Telecommunications and Technology Law Review**, Vol. 26, No. 2, 2020, Available at SSRN. Disponível: https://ssrn.com/abstract=3606601. Acesso em: 13 de nov. de 2022.

129 KAYE, David A., The Spyware State and the Prospects for Accountability. Global Governance, Vol. 27, Nº 4, 2021, Forthcoming, **UC Irvine School of Law Research Paper nº 2021-58**, 20 dez. 2021. Available at SSRN. Disponível em: https://ssrn.com/abstract=3990249. Acesso em 14 nov. 2022.

130 STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/. Acesso em: 11 nov. 2022. p. 6.

131 RUDIE, JD; KATZ, Zach; KUHBANDER, Sam; BHUNIA, Suman. Technical Analysis of the NSO Group's Pegasus Spyware. **2021 International Conference on Computational Science and Computational Intelligence (CSCI)**, Las Vegas (NV), EUA, dez. 2021 pp. 747-752. DOI: 10.1109/CSCI54926.2021.00188. Disponível em https://ieeexplore.ieee.org/document/9799180 e https://www.computer.org/csdl/proceedings-article/csci/2021/584100a747/1EpL7AEhgxa. Acesso em: 8 nov. 2022.

132 PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. **STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment**, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. doi:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375. Acesso em 12 de nov. de 2022. p. 266.

133 LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. **Michigan Telecommunications and Technology Law Review**, Vol. 26, No. 2, 2020, Available at SSRN. Disponível: https://ssrn.com/abstract=3606601. Acesso em: 13 de nov. de 2022.

134 FUKAMI, Aya; STOYKOVA, Radina; GERADTS, Zeno. A new model for forensic data extraction from encrypted mobile devices. **Forensic Science International: Digital**

Investigation, Volume 38, set. 2021, 301169. ISSN 2666-2817. DOI: 10.1016/j.fsidi.2021.301169. Disponível em https://www.sciencedirect.com/science/article/pii/S2666281721000779. Acesso em 27 out. 2022.

135 RAMIRO, André (coord.); CANTO, Mariana; REAL, Paula Côrte; LIMA, José Paulo; AGUIAR, Thaís. **O Mosaico Legislativo da Criptografia no Brasil: uma análise de projetos de Lei**. IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 05 ago. 2020. Disponível em https://obcrypto.org/estudo/o-mosaico-legislativo-da-criptografia-no-brasil-uma-analise-de-projetos-de-lei/. Acesso em: 10 nov. 2022.

136 DAVIS, Peter Alexander Earls. **Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation**. ELSEVIER, [s. l.], ed. 44, 2022. DOI: 10.1016/j.clsr.2022.105659. Disponível em https://www.sciencedirect.com/science/article/pii/S0267364922000073. Acesso em 26 out. 2022. p. 17.

137 AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil** [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 25 nov. 2022. P. 80.

138 ROZENSHTEIN, Alan Z. Wicked Crypto. **U.C. Irvine Law Review**, Vol. 9, N. 5 (Jul. 2019): Women, Law, Society, & Technology, 1181-1215. Disponível em https://scholarship.law.uci.edu/ucilr/vol9/iss5/6/. Acesso em 10 nov. 2022.

139 MOYAKINE, Evgeni V. The Privatized Art of War: Private Military and Security Companies and State Responsibility for their Unlawful Conduct in Conflict Areas. S.l.: Intersentia, 2014. Disponível em https://research.tilburguniversity.edu/en/publications/the-privatized-art-of-war-private-military-and-security-companies. Acesso em 02 fev. 2023.

REFERÊNCIA	CATEGORIA	FONTE
AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César M.; RAMIRO, André (coord.). Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil [livro eletrônico]. Recife, PE: IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/.	Relatório	Inclusão discricionária
BELLOVIN, Steven M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. 12 Nw. J. Tech. & Intell. Prop. 1 (2014). Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1.	Artigo científico	SSRN
CAMPOS, Juliana Filipa Sousa. O malware como meio de obtenção da prova em processo penal. 2019. Dissertação (Dissertação de Mestrado em Direito apresentada à Faculdade de Direito) - Faculdade de Direito da Universidade de Coimbra, Lisboa, 2018. Disponível em https://repositorio.ul.pt/bitstream/10451/37574/1/ulfd137535_tese.pdf.	Monografia, dissertação ou tese	Google Acadêmico
DAVIS, Peter Alexander Earls. Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation. ELSEVIER, [s. l.], ed. 44, 2022. DOI: 10.1016/j.clsr.2022.105659. Disponível em https://www.sciencedirect.com/science/article/pii/S0267364922000073.	Artigo científico	Science Direct

REFERÊNCIA	CATEGORIA	FONTE
DONAHUE, James L. A comparative analysis of international encryption policies en route to a domestic solution. 2018. 169 p. Thesis (Master Of Arts In Security Studies) - Naval Postgraduate School, [S. l.], 2018. Disponível em: https://calhoun.nps.edu/handle/10945/58291.	Monografia, dissertação ou tese	Mendeley
FARLOW, Harriet; M. EDWARDS , Belinda. Shining a light on 'going dark': A framework to guide the co-design and communication of decryption laws based on the passage of the Telecommunications and Other Legislation (Assistance and Access) Bill 2018. Computer law & security review, [s. l.], 2022. DOI:10.1016/j.clsr.2022.105726. Disponível em https://linkinghub.elsevier.com/retrieve/pii/S0267364922000681.	Artigo científico	Science Direct
FUKAMI, Aya; STOYKOVA, Radina; GERADTS, Zeno. A new model for forensic data extraction from encrypted mobile devices. Forensic Science International: Digital Investigation, Volume 38, set. 2021, 301169. ISSN 2666-2817. DOI: 10.1016/j.fsidi.2021.301169. Disponível em https://www.sciencedirect.com/science/article/pii/S2666281721000779.	Artigo científico	Science Direct
HENNESSEY, Susan. Lawful Hacking and the Case for a Strategic Approach to 'Going Dark'. O'HANLON, Michael E. Brookings Big Ideas for America. Brookings Institution Press, 31 jan. 2017. Pp. 241-250. Disponível em https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/. Acesso em 28 out. 2022.	Capítulo de livro	Mendeley, Scopus

REFERÊNCIA	CATEGORIA	FONTE
HEWSON, Eloise C.; HEWSON, Eloise C. Talking in the dark: Rules to facilitate open debate about lawful access to strongly encrypted information. Computer law & security review, [s. l.], abril 2021. Disponível em https://www.sciencedirect.com/science/article/abs/pii/S026736492030131X.	Artigo científico	Science Direct
HRIVASTAVA, Sanskriti; KEJRIWAL, Muskan. Pegasus Spyware:: Evaluating The Need For Surveillance Reform And Introduction Of Data Protection Bill. Institute of Law Nirma University Nirma University, [s. l.], 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4171776.	Artigo científico	SSRN
JOHN, Scott-Railton; BILL, Marczak; BAHR, Abdul Razzak; MASASHI, Crete-Nishihata; RON, Deibert. Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware. Citizen Lab Research Report nº 94. University of Toronto, jun. 2017. Disponível em https://citizenlab.ca/2017/06/more-mexican-nso-targets/.	Relatório	Mendeley
KAYE, David A. The Spyware State and the Prospects for Accountability. Global Governance: A Review of Multilateralism and International Organizations, Vol. 27, nº 4, 483-492. DOI:10.1163/19426720-02704005. Disponível em https://brill.com/view/journals/gg/27/4/article-p483_1.xml.	Artigo científico	SSRN

REFERÊNCIA	CATEGORIA	FONTE
KERR, Orin S.; MURPHY, Sean D.. Government Hacking to Light the Dark Web: What Risks to International Relations and International Law? 24 abr. 2017. 70 Stanford Law Review Online 58 (Jul. 2017). Pp. 58-69. Disponível em https://ssrn.com/abstract=2957361.	Artigo científico	SSRN
KOOPS, Bert-Jaap; KOSTA, Eleni. Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". Computer law & security review, [s. l.], v. 34, p. 899-900, 2018. Disponível em https://drive.google.com/file/d/1YX6rHZfaMTJ2wTM2WGzv4sHCnyqkpsnd/view.	Artigo científico	Science Direct
LEANDER, Anna. Parsing Pegasus: An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics. Swiss Political Science Review, v. 27, n. 1, p. 205-213, 2021. Disponível em https://onlinelibrary.wiley.com/doi/epdf/10.1111/spsr.12441.	Artigo científico	Mendeley, Scopus
LI, Chen-Yu et al. A Comprehensive Overview of Government Hacking Worldwide. IEEE Access, [s. l.], v. 6, 24 set. 2018. DOI 10.1109/ACCESS.2018.2871762. Disponível em: https://ieeexplore.ieee.org/document/8470931.	Artigo científico	Mendeley, Scopus
LIGUORI FILHO, Carlos Augusto. Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. 8 mai. 2020. Michigan Telecommunications and Technology Law Review, Vol. 26, No. 2, 2020. DOI: 10.36645/mtlr.26.2.exploring. Disponível em https://repository.law.umich.edu/mtlr/vol26/iss2/5/.	Artigo científico	Mendeley, SSRN

REFERÊNCIA	CATEGORIA	FONTE
LIGUORI, Carlos. Direito e Criptografia: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia. São Paulo: SaraivaJur, 2022.	Monografia, dissertação ou tese	Google Acadêmico
MARCZAK, Bill; ANSTIS, Siena; CRETE-NISHIHATA, Masashi; SCOTT-RAILTON, John; DEIBERT, Ron. Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator. Citizen Lab Research Report nº 124 University of Toronto, January 2020. Disponível em https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/.	Relatório	Mendeley
MARCZAK, Bill; SCOTT-RAILTON, John; SENFT, Adam; RAZZAK, Bahr Abdul; DEIBERT, Ron. The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. Citizen Lab Research Report nº 115. University of Toronto, out. 2018. Disponível em: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.	Relatório	Mendeley
MAXWELL, Francis. When good is not good enough: evaluating the proportionality and necessity of the Australian government hacking warrants. Current Issues in Criminal Justice, [s. l.], v. 34, ed. 2, p. 136-154, 2022. DOI 10.1080/10345329.2022.2046934. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/10345329.2022.2046934?journalCode=rcic20.	Artigo científico	Scopus

REFERÊNCIA	CATEGORIA	FONTE
MAYER, Jonathan. Constitutional Malware. 21 jul. 2015, rev. draft 14 nov. 2016. SSRN. Disponível em https://ssrn.com/abstract=2633247.	Artigo científico	SSRN
MAYER, Jonathan. Government Hacking. The Yale Law Journal, 2018. Disponível em https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf.	Artigo científico	Mendeley, Scopus
MORAES, Thiago. Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures. European Data Protection Law Review Volume 6, Issue 1 (2020), pp. 41 - 55. DOI: https://doi.org/10.21552/edpl/2020/1/7. Disponível em https://edpl.lexxion.eu/article/EDPL/2020/1/7.	Artigo científico	Mendeley, Scopus
ONU. ONU. Escritório do Alto Comissariado para Direitos Humanos. The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights. Genebra, 4 ago. 2022. Disponível em https://digitallibrary.un.org/record/3985679?ln=es.	Relatório	Inclusão discricionária
PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em https://bit.ly/3kGTde3.	Relatório	Google Acadêmico

REFERÊNCIA	CATEGORIA	FONTE
PÎRVU, Maria. The Degradation of Human Rights and Free Press Through the Pegasus Software in the Era of Surveillance, as a Threat to International Security. A Debate Of Civil Liberties And Censorship. STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment, 10 fev. 2022. Univeritatea Nationala de Aparare Carol I, 263–72. DOI:10.53477/2668-6511-22-29. Disponível em https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1375.	Trabalho publicado em anais de evento acadêmico	Mendeley
RAMIRO, André (coord.); CANTO, Mariana; REAL, Paula Côrte; LIMA, José Paulo; AGUIAR, Thaís. O Mosaico Legislativo da Criptografia no Brasil: uma análise de projetos de Lei. IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 05 ago. 2020. Disponível em https://obcrypto.org/estudo/o-mosaico-legislativo-da-criptografia-no-brasil-uma-analise-de-projetos-de-lei/.	Relatório	Google Acadêmico
RAMIRO, André; AMARAL, Pedro; PEREIRA, Marcos Cesar M. Insegurança Distribuída: Economia E Regulação Do Hacking Governamental. IV Encontro Da Rede De Pesquisa Em Governança Da Internet - Rede 2021, [s. l.], out. 2021. Disponível em http://redegovernanca.net.br/index.php/encontro-anual/encontro-anual/paper/view/106.	Trabalho publicado em anais de evento acadêmico	Google Acadêmico

REFERÊNCIA	CATEGORIA	FONTE
RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. Revista Brasileira de Direito Processual Penal, v. 8, nº 3, Porto Alegre, set-dez. 2022, 1463-1500. DOI:10.22197/rbdpp.v8i3.723. Disponível em https://revista.ibraspp.com.br/RBDPP/article/view/723.	Artigo científico	Inclusão discricionária
ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. Revista de Investigación en Tecnologías de la Información, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ojs2018/inicio/index.php/riti/article/view/185. DOI: 10.36825/riti.07.14.003.	Artigo científico	Mendeley
ROZENSHTEIN, Alan Z. Wicked Crypto. U.C. Irvine Law Review, Vol. 9, N. 5 (Jul. 2019): Women, Law, Society, & Technology, 1181-1215. Disponível em https://scholarship.law.uci.edu/ucilr/vol9/iss5/6/.	Artigo científico	SSRN
RUDIE, JD; KATZ, Zach; KUHBANDER, Sam; BHUNIA, Suman. Technical Analysis of the NSO Group's Pegasus Spyware. 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas (NV), EUA, dez. 2021 pp. 747-752. DOI: 10.1109/CSCI54926.2021.00188. Disponível em https://ieeexplore.ieee.org/document/9799180 e https://www.computer.org/csdl/proceedings-article/csci/2021/584100a747/1EpL7AEhgxa.	Trabalho publicado em anais de evento acadêmico	Scopus

REFERÊNCIA	CATEGORIA	FONTE
SOMMER, Peter. Evidence from hacking: A few tiresome problems. Forensic Science International: Digital Investigation, v. 40, p. 301-333, 2022. DOI: 10.1016/j.fsidi.2022.301333. Disponível em https://www.sciencedirect.com/science/article/pii/S2666281722000026.	Artigo científico	Science Direct
STEPANOVICH, Amie; BEDOYA-ARROYO, Daniel; BJORKSTEN, Gustaf; CARBONE, Michael; MITNICK, Drew; WENTWORTH, Donna; WHITE, Nathan. A Human Rights Response to Government Hacking. Access Now, set. 2016. Disponível em https://www.accessnow.org/report-calls-presumptive-ban-government-hacking-human-rights-protections/.	Relatório	Inclusão discricionária
STOYKOVA, Radina; NORDVIK, Rune; FRANKE, Katrin; AXELSSON, Stefan; AHMED, Munnazzar; TOOLAN, Fergus. Legal and technical questions of file system reverse engineering. Computer Law & Security Review, [s. l.], v. 46, September 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364922000693.	Artigo científico	Science Direct
STOYKOVA, Radina. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review, v. 42, 2021. DOI: 10.1016/j.clsr.2021.105575. Disponível em https://www.sciencedirect.com/science/article/pii/S0267364921000480.	Artigo científico	Science Direct

Apêndice 2 - Formulário de análise

- E-mail
- Ano
- Referência ABNT
- Link da publicação
- Categoria
  marcar apenas uma opção
  > Artigo científico
  > Declaração, carta aberta
  > Relatório
  > Nota técnica
  > Jurisprudência
  > Trabalho publicado em anais de evento acadêmico
  > Monografia, dissertação ou tese
  > Artigo de opinião
  > Matéria de jornal
  > Post de blog
- Escopo
  marcar apenas uma opção
  > Rastreabilidade
  > Hacking governamental
  > Varredura pelo lado do cliente
- Síntese
  Texto de resumo elaborado pela equipe do IRIS: deve incluir uma apresentação breve da proposta do trabalho, metodologia (ou ausência de indicação de metodologia), eventuais referências relevantes (citadas como base para o conceito ou posicionamento indicado no trabalho) e abordagem dada ao escopo analisado.
- Comentários
- Citações
- Observações

iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE