XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III

CELSO HIROSHI IOCOHAMA

LUIZ GUSTAVO GONÇALVES RIBEIRO

MATHEUS FELIPE DE CASTRO

D597

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Celso Hiroshi Iocohama, Luiz Gustavo Gonçalves Ribeiro, Matheus Felipe De Castro – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-65-5274-054-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal e constituição. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III

Apresentação

A edição do XXXI CONGRESSO NACIONAL DO CONPEDI – BRASÍLIA nos ofereceu produções cientificas inestimáveis, no âmbito da visão constitucional do Direito Penal e do Processo Penal. Os trabalhos apresentados abordam uma conjuntura de temas e ideias necessárias à reflexão da comunidade cientifica sobre os problemas relacionados ao grupo temático. Dentro desse contexto, no Grupo de Trabalho - DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III constatou-se qualificadas contribuições para o campo das Ciências Sociais Aplicadas, além de profícuo debate de todos os presentes na sala.

A obra ora apresentada reúne os artigos selecionados através do sistema de dupla revisão cega, de modo a nos permitir certeza de que os temas a seguir apresentados são instigantes e apresentam significativas contribuições para as reflexões dos Programas de Pós-graduação em Direito reunidos no CONPEDI.

São os seguintes, por título e objeto, os trabalhos que compõem o livro:

- “A implementação da delegacia especializada de atendimento à mulher em Viçosa-MG: da law on the books à law in action”, que traz os resultados de uma pesquisa que objetivou identificar o impacto da implantação da Delegacia Especializada de Atendimento à Mulher na proteção à mulher e no combate à violência de gênero e doméstica na Comarca de Viçosa-MG, tomando por corte temporal o intervalo entre os anos de 2019 e 2022. Partindo desse objetivo geral, a pesquisa buscou os seguintes objetivos específicos: a) coletar os dados referentes ao processo de implantação da Delegacia Especializada de Atendimento à Mulher em Viçosa-MG; b) verificar se, desde sua implantação até o corrente ano de 2022, a DEAM em Viçosa-MG foi provida das estruturas física, material e humana necessárias ao desenvolvimento de suas tarefas; c) identificar o perfil e o quantitativo de casos por ela atendidos no intervalo compreendido entre sua implantação no ano de 2019 e dezembro de 2022; d) identificar o perfil e o quantitativo de casos de violência de gênero e doméstica atendidos pela Delegacia de Polícia de Viçosa-MG entre os anos de 2015 e a véspera da implantação da DEAM, para proceder a comparação com o período subsequente; e) verificar se a DEAM em Viçosa tem funcionado dentro dos parâmetros estabelecidos pela Constituição Federal de 1988 e pela Lei n. 11.340/2006 e para além do exercício de mera tarefa de polícia investigativa ou judiciária na promoção e proteção das mulheres vítimas de violência de gênero e doméstica.

- “Homicídio culposo e o arrependimento posterior: uma crítica ao entendimento do STJ e ênfase ao alcance extrapatrimonial do instituto”. O trabalho busca questionar a interpretação dada pelo Superior Tribunal de Justiça à aplicabilidade do instituto do arrependimento posterior ao homicídio culposo. No julgamento do Recurso Especial número 1.561.276/BA, a Corte Cidadã fixou o entendimento de que a causa de diminuição prevista no artigo 16 do Código Penal só incidiria em crimes contra o patrimônio ou com efeitos exclusivamente patrimoniais. Em perspectiva contrária, a pesquisa sustenta que tal interpretação é restritiva e destoa da própria razão de ser do instituto. Entende-se que a reparação do dano na seara penal é uma medida de política criminal, frequentemente estimulada pelo legislador. Deste modo, em atenção aos requisitos expostos no Código Penal, defende-se que a violência no resultado não obstaria a aplicação do instituto, sendo a aplicabilidade aqui sustentada amparada em três principais argumentos. Inicialmente, tem-se que, em uma interpretação sistemática do ordenamento brasileiro, a reparação do dano à vida é possível (e desejável), tendo em conta a ideia de reparação por ato ilícito disposta no Código Civil. Em seguida, destaca-se que a própria razão de ser do instituto do arrependimento posterior, constante na exposição de motivos da Parte Geral do Código, indica que a preocupação se volta sobretudo à vítima (se estendendo aos seus familiares, por consectário lógico). Nessa linha, conclui-se que a interpretação conferida pelo Superior Tribunal de Justiça revela-se contrária aos princípios da legalidade e proporcionalidade, sendo defendida a revisão do entendimento.

- “A função da pena na sociedade Pós-Moderna sob o prisma do paradigma do Estado Democrático de Direito”. O trabalho em questão aborda as teorias retributiva e prevencionista das penas, com foco especial na pena privativa de liberdade e sua função em uma sociedade globalizada e pós-moderna. A teoria retributiva defende que a punição é uma resposta justa ao crime, proporcional à gravidade da infração cometida. Por outro lado, a teoria prevencionista busca evitar futuros crimes por meio da dissuasão, incapacitação do criminoso ou sua reabilitação. Na sociedade pós-moderna, caracterizada por uma interconectividade e complexidade crescentes, o papel da pena privativa de liberdade é amplamente debatido. Embora a retribuição ainda seja vista como crucial para manter a ordem e a justiça social, a prevenção, especialmente com ênfase na reabilitação e reintegração social, ganha destaque. Evidências mostram que penas severas nem sempre resultam em menores taxas de reincidência, o que reforça a necessidade de uma abordagem equilibrada. A globalização apresenta novos desafios e perspectivas, exigindo uma ponderação entre punir e promover uma sociedade mais justa e segura. O artigo conclui que a pena privativa de liberdade, como ferramenta punitiva, deve ser reavaliada à luz dos direitos humanos e das evidências empíricas sobre sua eficácia, destacando a importância de políticas penais que integrem justiça retributiva, prevenção e reintegração social.

- “A atuação do poder público na defesa dos direitos da mulher presidiária”. No trabalho são abordados estudos sobre o estabelecimento penal, função da pena, prisão de mulheres, direitos fundamentais das mulheres, princípio da dignidade da pessoa humana, medidas alternativas da pena, direitos humanos e direitos fundamentais e a violação dos direitos e interesses da mulher presidiária pelo Poder Público. Busca-se a análise das situações prisionais e estatísticas com base de dados em relação ao encarceramento de mulheres no Brasil. Também é abordada a situação de mulheres na situação especial de prisão em tempos de gravidez e a violação de seus direitos enquanto pessoa do sexo feminino.

- “O reconhecimento de pessoas como meio de prova no processo penal: uma análise de erros judiciais”. O texto aborda o reconhecimento de pessoas como meio de prova no processo penal, que apesar de sua importância, é considerada uma prova frágil, pois depende da memória humana, que se demonstrou falha e influenciável, tornando esse meio probatório suscetível a erros. Diante disso, questiona-se: o reconhecimento pessoal ou fotográfico pode ser utilizado como único meio de prova para fundamentar uma condenação no processo penal brasileiro, consequentemente violando o standard de prova além da Dúvida Razoável? Para responder o questionamento feito, foram analisados os procedimentos de reconhecimento no processo penal e os erros judiciais causados por reconhecimentos equivocados, bem como, o posicionamento do STJ em relação à problemática. O trabalho inicia discorrendo acerca da importância desse meio prova, que é amplamente utilizado, mas que pode ser falho, dessa forma, levando a condenações injustas de inocentes. Além disso, foi externado como essa problemática acaba por evidenciar o racismo estrutural e institucional no Brasil. Ao final constatou-se que o reconhecimento deve ser realizado com cautela e de acordo com a previsão legal e não deverá ser utilizado como único meio probatório.

- “Tornozeleiras eletrônicas como instrumento de monitoramento: estigmatização, desafios e implicações para o sistema penal”. No trabalho ora apresentado, o objetivo foi analisar criticamente o uso das tornozeleiras eletrônicas no sistema penal brasileiro, enquanto instrumento de monitoramento de indivíduos em cumprimento de penas alternativas. Inicialmente, discute-se a estigmatização social que recai sobre os usuários desses dispositivos, evidenciando os impactos sociais e as barreiras para a reintegração dos monitorados. Em seguida, aborda-se os desafios inerentes à implementação dessas tecnologias, destacando as falhas operacionais, os custos elevados e as lacunas no arcabouço normativo que regem seu uso. A investigação fundamenta-se em uma revisão bibliográfica abrangente, complementada por análises de casos emblemáticos que ilustram aspectos positivos e negativos da utilização dos dispositivos eletrônicos, frente ao contexto penal e social. Conclui-se que, embora essas ferramentas representem uma inovação importante na mitigação da superlotação carcerária e na promoção de penas alternativas, há reflexos

sensíveis, na relativização da dignidade da pessoa humana dos monitorados, além de uma eficácia limitada pela carga estigmatizante e pelos obstáculos práticos à sua aplicação. O trabalho propõe, portanto, o aperfeiçoamento dessas tecnologias e sua integração com outras estratégias de reintegração social enquanto imperativos para o cumprimento das funções declaradas dos serviços de monitoração eletrônica no país.

- “Divergências entre os posicionamentos de Gunther Jakobs e Manuel Cancio Meliá sobre a teoria do direito penal do inimigo e sua incompatibilidade com o garantismo penal”. No trabalho são abordadas noções sobre a Teoria do Direito Penal do Inimigo, seu surgimento e aplicabilidade, bem como sua incompatibilidade com o garantismo penal de Ferrajoli. Apresenta-se a biografia de Gunther Jakobs e breves considerações abordando as divergências entre o seu posicionamento e o de Claus Roxin em relação à teoria da imputação objetiva, já que se trata de uma temática bastante trabalhada por Gunther Jakobs em suas produções científicas. Também apresenta-se a biografia de Manuel Cancio Meliá e as posições doutrinárias divergentes entre ele e Gunther Jakobs sobre a teoria do direito penal do inimigo.

- “A sociedade de risco e as velocidades do direito penal”. O texto propõe uma análise acerca do fenômeno da Expansão do Direito Penal sob a ótica da teoria desenvolvida por Jesús-María Silva Sánchez, denominada “Velocidades do Direito Penal”, da Teoria Pessoal do Bem Jurídico e o Direito Penal de Intervenção de Winfried Hassemer e da teoria da Sociedade de Risco de Ulrick Beck. O objetivo geral consiste na reflexão sobre as principais características da sociedade do risco investigada por Ulrich Beck e sua relação com o expansionismo penal e as possíveis influências que esse modelo de organização social exerce sobre o Direito Penal. A metodologia utilizada foi a pesquisa bibliográfica e documental a partir de obras relacionadas ao tema, o método jurídico dedutivo, com abordagem qualitativa. Entre as conclusões obtidas por meio deste trabalho, pode-se destacar que a diminuição da criminalidade não está relacionada ao expansionismo penal imoderado, nem ao endurecimento do Direito Penal, mas sim a uma política social igualitária, que deve assegurar que as leis penais respeitem os limites constitucionais, notadamente as garantias constitucionais, tanto na sua criação quanto na sua aplicação. De toda sorte, a insegurança e o medo sentidos pela sociedade devem ser considerados e exigem uma resposta efetiva do Estado, que não será encontrada na reprodução de um Direito Penal meramente simbólico ou no recrudescimento das sanções penais.

- “Direitos humanos e segurança pública: o dilema das saídas temporárias”. O trabalho explora o equilíbrio entre os direitos humanos dos detentos e as preocupações com a segurança pública, no contexto das saídas temporárias previstas na Lei de Execução Penal

brasileira, debatendo também sobre as alterações introduzidas pela Lei nº 14.843, de 11 de abril de 2024. As saídas temporárias, um mecanismo que visa a ressocialização dos apenados, têm gerado debates devido aos casos de reincidência criminal durante esses períodos, levantando questões sobre sua eficácia e impacto na segurança pública. O objetivo da pesquisa é analisar como essas saídas são implementadas, seus efeitos na reintegração social dos presos e as dificuldades que apresentam para a segurança pública. As considerações finais destacam a necessidade de aprimorar as políticas de saídas temporárias por meio de uma aplicação mais rigorosa e um monitoramento eficaz, conforme preconizado pela Lei nº 14.843/2024. Além disso, enfatiza que, embora a ressocialização dos detentos seja um objetivo fim, ela não pode ocorrer em detrimento da segurança pública. A integração de medidas adicionais, como o monitoramento eletrônico e a realização de exames criminológicos, são vistas como passos importantes, mas é igualmente essencial que essas práticas sejam acompanhadas por um suporte contínuo aos detentos, garantindo que a reintegração à sociedade seja efetiva e sustentável.

- “Direitos fundamentais e a criminalização da pobreza: o impacto do direito penal nas populações vulneráveis”. Revela-se que, no Brasil, tem-se visto um aumento expressivo nas taxas de criminalidade nas últimas décadas, acompanhado por políticas de segurança pública que se baseiam cada vez mais na repressão e na militarização. Essas estratégias têm exacerbado as desigualdades sociais e ampliado a marginalização das populações vulneráveis, especialmente nas periferias urbanas. Em vez de resolver as causas estruturais da violência, como a pobreza extrema e a falta de acesso a serviços básicos, essas práticas tendem a perpetuar um ciclo de exclusão e violação dos direitos fundamentais. Diante disso, o objetivo do texto é examinar como o direito penal pode discriminar indiretamente as populações vulneráveis, explorando as políticas de criminalização da pobreza e suas implicações para os direitos fundamentais. A análise revelou que, longe de resolver os problemas de segurança pública, as práticas repressivas contribuem para a ampliação das desigualdades sociais, afetando desproporcionalmente as populações negras e pobres. Além disso, a criminalização da pobreza e a seletividade penal evidenciam que o direito penal, quando instrumentalizado de maneira inadequada, pode violar gravemente os direitos fundamentais, como dignidade humana e o devido processo legal, garantidos pela Constituição e pelos tratados internacionais.

- “Inefetividade do acesso à saúde como fundamento para a aplicação obrigatória da teoria da coculpabilidade”. O trabalho analisa a possibilidade de utilizar a inefetividade dos direitos fundamentais, especialmente o direito à saúde, como base para aplicar a atenuante inominada do artigo 66 do Código Penal em casos de infração penal. A falta de acesso aos direitos fundamentais afeta a autodeterminação do indivíduo, sendo a saúde um elemento crucial para

a vida. A vida é o direito fundamental mais importante e a saúde é essencial para mantê-la. O estudo questiona se a Teoria da Coculpabilidade deve ser aplicada em crimes que visam garantir a saúde como requisito para viabilizar a vida. Um dos objetivos é determinar se a aplicação da teoria da coculpabilidade nesses casos pode ser obrigatória, analisando fundamentos jurídicos internos. O estudo se baseia em pesquisa bibliográfica, legislativa e jurisprudencial. Conclui-se que a saúde é fundamental para a vida e a falta de acesso a ela pode levar indivíduos a cometerem crimes, como o furto famélico e desacato, para preservar a própria vida ou de terceiros. Portanto, em casos específicos, a aplicação da Teoria da Coculpabilidade pode ser juridicamente indicada após análise de critérios objetivos.

- “Constituinte para valer tem que ter direitos da mulher: a Constituição cidadã e os direitos das mulheres”. O trabalho analisa o processo de elaboração da Constituição Brasileira de 1988 focando na constitucionalização dos direitos das mulheres. A partir do marco jurídico e político da Assembleia Nacional Constituinte de 1987-1988, analisa-se como se efetivou a política de combate à violência de gênero, considerando, especialmente, a atuação do movimento feminista e da advocacia. O estudo aborda, brevemente, a evolução legislativa, as conquistas jurídicas e os desafios ainda presentes na luta contra a violência de gênero no Brasil. De igual forma, o texto evidencia como a igualdade jurídica entre os gêneros trouxe impactos desde a Constituição federal de 1988 até os dias atuais, incluindo o arcabouço jurídico que vem se formando para consolidar os direitos femininos e coibir a violência contra as mulheres que, a despeito da evolução social e legislativa, segue em crescimento. As conquistas e os esforços da advocacia, sobretudo a advocacia feminina, e as medidas adotadas pelo Conselho Federal e pelas Seccionais da Ordem dos Advogados do Brasil também são objeto de estudo.

- “Reflexões sobre o direito à saúde das pessoas com deficiência privadas de liberdade sob a ótica do caso Chinchila Sandoval v. Guatemala”. O trabalho revela que, no ano de 2016, a Guatemala foi condenada pela Corte Interamericana de Direitos Humanos, em sentença responsabilizando o Estado por violações institucionalizadas aos direitos à integridade pessoal e à vida, que resultou na morte de María Inés Chinchilla Sandoval, enquanto cumpria pena privativa de liberdade. O trabalho foi desenvolvido a partir da seguinte problemática de pesquisa: sob quais aspectos o caso Chinchilla Sandoval versus Guatemala, no âmbito da Corte-IDH, afigura-se como um standard decisório importante para direcionar a efetivação do direito à saúde para pessoas com deficiência no cárcere? Como hipótese inicial, observa-se que as pessoas com deficiência não têm os direitos observados, sendo consideradas hipervulneráveis. O objetivo geral do trabalho é analisar a efetivação do direito à saúde no cárcere, com base na decisão mencionada. Para alcançar o objetivo geral, os objetivos específicos, que correspondem às seções de desenvolvimento do texto, consistem em: a)

apresentar as peculiaridades do Caso analisado, evidenciando os principais elementos; b) analisar os direitos humanos violados no caso investigado e sua repercussão na situação das pessoas com deficiência encarceradas. Conclui-se pela existência de regramento suficiente para o respeito dos direitos da pessoa com deficiência no cárcere (dimensão programadora), mas ausência de concretude desses direitos (dimensão operacional).

- “Hacking legal ou investigativo/lawful hacking: perspectivas a partir da legislação brasileira”. O texto traz uma análise detalhada das questões relacionadas ao lawful hacking ou hacking legal/investigativo e seu papel no contexto do debate conhecido como Going Dark Problem: complexidade derivada do descompasso temporal entre tecnologia e regulação e atuação em investigação criminal, frente à proteção de dados pessoais no ambiente digital. Portanto, o estudo examina as perspectivas favoráveis e contrárias ao uso de técnicas especiais de investigação, como o hacking legal/investigativo e uso das ferramentas de monitoramento remotamente controladas, explorando a complexidade das implicações legais e éticas associadas a essas práticas. É enfatizado que o uso adequado dessas técnicas pode ser compatível com a proteção dos direitos fundamentais dos cidadãos, desde que sejam observados princípios como transparência, proporcionalidade e auditabilidade. Isso inclui a necessidade de supervisão judicial rigorosa e conformidade estrita com requisitos legais. Destaca-se a importância de debate público contínuo e da participação do Poder Legislativo na regulamentação do hacking legal/investigativo, observando-se a necessidade de cooperação internacional e a conformidade com tratados e convenções, como a Convenção de Budapeste, para abordar o cibercrime em escala global.

- “Pena privativa de liberdade e monitoramento eletrônico: desafios e perspectiva na execução penal”. O texto expõe que a pena privativa de liberdade é um instrumento de punição que não tem sido efetivo no Brasil. Isso se deve, em grande parte, à superlotação carcerária, que resulta em condições precárias e indignas nos presídios. Diante da ineficácia da pena privativa de liberdade, notadamente, em razão da superlotação carcerária no Brasil, pergunta-se: a extensão da aplicabilidade do monitoramento eletrônico pode contribuir para a redução das situações precárias e indignas existentes no sistema carcerário, sem repercussão negativa em sociedade? Para isso, o trabalho objetiva verificar se a extensão da aplicabilidade do monitoramento eletrônico pode ser uma medida positiva, desde que seja utilizada de forma responsável e controlada. A medida pode ajudar a reduzir os problemas do sistema carcerário, sem prejudicar os direitos dos presos. Ao final, constatou-se que a aplicabilidade do monitoramento eletrônico deve ser aplicada de forma justa e proporcional, respeitando os direitos dos presos e evitando qualquer forma de tratamento desumano ou degradante.

- “O preço de se violentar uma mulher: as decisões criminais do TJMG envolvendo reparação por danos causados pela violência doméstica contra a mulher perspectivadas pelo Tema 983 do STJ”. A violência doméstica contra a mulher, durante décadas, foi assunto naturalizado e integrado ao cotidiano familiar e relacional no Brasil: algo corriqueiro e, por vezes, justo no contexto doméstico. Graças às intensas reivindicações feministas, desembarcadas no Brasil a partir das décadas de 70 e 80, essa visão passou a ser questionada e, especialmente, neste Século XXI, a ser afastada, sendo emblemática tipificação e a definição da violência doméstica e familiar contra a mulher pela Lei n. 11.340/2006. E, ao menos no plano jurídico-normativo, ganhou força com a edição da Lei 11.719/2008 e a obrigatoriedade de fixação, na sentença condenatória criminal, do valor mínimo para a reparação civil dos danos causados pela infração e, mais recentemente, pela fixação, no Tema 983 pelo STJ do entendimento de que o dano moral, nesses casos consiste em in re ipsa. Próximos do encerramento desse primeiro quarto de século de tantas mudanças no plano jurídico-normativo, necessário faz verificar o efeito prático alcançado por essas medidas, o que justifica verificar se, a edição dos textos legais acima mencionados e da Tese 983 do STJ foram suficientes para a adequação da compreensão dos danos sofridos pela mulher vítima de violência a partir das perspectivas feministas e a sua consequente conversão em reparações judiciais em valores minimamente compatíveis com sua gravidade. O que fazemos, nesta pesquisa, a partir de uma perspectiva qualitativa e do uso do método bibliográfico-documental, por meio da leitura das decisões do TJMG.

- “Mensagens de aplicativos de mensageria como provas no processo penal: uma análise de decisões do STJ”. O trabalho analisa a utilização de mensagens de aplicativos de mensageria como prova no processo penal, com foco em decisões do Superior Tribunal de Justiça (STJ). O objetivo é analisar a eventual (in)admissibilidade e (in)validade dessas provas, examinando os parâmetros e diretrizes estabelecidos pelo tribunal, realizando uma análise técnica dos pressupostos e afirmações constantes do julgamento do Habeas Corpus n. 99.735/SC e do Agravo Regimental no Habeas Corpus n. 828.054/RN, especialmente sobre pontos tecnológicos. O estudo emprega uma análise bibliográfica e documental, utilizando métodos indutivo-dedutivo para analisar casos concretos e alcançar conclusões. A pesquisa destaca a importância do STJ na uniformização da jurisprudência e aborda as decisões colegiadas mais relevantes, apontando acertos e erros técnicos, como, por exemplo, o desconhecimento sobre os registros de conexão existentes e acessíveis ou o desconhecimento acerca do fenômeno da irrepetibilidade de hash em aparelhos celulares. Conclui-se que é imprescindível a análise técnica das decisões do STJ sobre provas digitais e a difusão de conhecimentos técnicos para melhorar a interpretação e aplicação dessas provas nos processos judiciais.

- “Estupro de vulnerável e gravidez: a dignidade da criança e do adolescente sob a perspectiva da jurisprudência”. O texto busca estudar o crime de estupro de vulnerável com enfoque na jurisprudência do Superior Tribunal de Justiça e na aplicação desta na justiça amapaense nas hipóteses em que a violência sexual resulta gravidez. A pesquisa apresenta a evolução do preceito normativo que tipifica a violência sexual contra a pessoa menor de 14 (catorze) anos, o conceito jurídico de vulnerabilidade e a possibilidade de relativização e, por fim, realiza a análise dos julgados à luz do dever de proteção integral da criança e da adolescente. Propôs-se a interpretação da norma penal em cotejo com os princípios constitucionais basilares que impõem uma postura ativa contra todas as formas de violência, em reforço ao compromisso do Estado brasileiro com as normas internacionais de proteção à infância e à adolescência.

Sendo esses os trabalhos que compõem o livro, afirma-se a certeza de que esta publicação fornece importantes instrumentos para que pesquisadores e aplicadores do Direito enriqueçam ainda mais os seus conhecimentos. Em razão disso, os organizadores desta obra prestam sua homenagem e agradecimento ao Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI) e, em especial, a todos os autores que participaram da presente coletânea.

Brasília, primavera de 2024.

Celso Hiroshi Iocohama – Universidade Paranaense – UNIPAR celso@prof.unipar.br

Luiz Gustavo Gonçalves Ribeiro – Dom Helder-Escola Superior lgribeirobh@gmail.com

Matheus Felipe de Castro – Universidade Federal de Santa Catarina matheusfelipedecastro@gmail.com

HACKING LEGAL OU INVESTIGATIVO/LAWFUL HACKING: PERSPECTIVAS A PARTIR DA LEGISLAÇÃO BRASILEIRA

LEGAL OR INVESTIGATIVE HACKING/LAWFUL HACKING: PERSPECTIVES FROM BRAZILIAN LEGISLATION

Emerson Wendt [1]
Tiago Misael de Jesus Martins [2]

Resumo

Objetiva-se uma análise detalhada das questões relacionadas ao lawful hacking ou hacking legal/investigativo e seu papel no contexto do debate conhecido como Going Dark Problem: complexidade derivada do descompasso temporal entre tecnologia e regulação e atuação em investigação criminal, frente à proteção de dados pessoais no ambiente digital. Portanto, este estudo examina as perspectivas favoráveis e contrárias ao uso de técnicas especiais de investigação, como o hacking legal/investigativo e uso das ferramentas de monitoramento remotamente controladas, explorando a complexidade das implicações legais e éticas associadas a essas práticas. É enfatizado que o uso adequado dessas técnicas pode ser compatível com a proteção dos direitos fundamentais dos cidadãos, desde que sejam observados princípios como transparência, proporcionalidade e auditabilidade. Isso inclui a necessidade de supervisão judicial rigorosa e conformidade estrita com requisitos legais. Destaca-se a importância de debate público contínuo e da participação do Poder Legislativo na regulamentação do hacking legal/investigativo, observando-se a necessidade de cooperação internacional e a conformidade com tratados e convenções, como a Convenção de Budapeste, para abordar o cibercrime em escala global. Utiliza-se, portanto, o método indutivo, partindo da análise das técnicas especiais de investigação, especialmente o uso de ferramentas de monitoramento remotamente controladas, no âmbito do sistema de persecução da criminalidade no Brasil e no mundo. Como metodologia, utiliza-se a revisão bibliográfica, com complementação em análise de documentos e da jurisprudência sobre o tema.

Palavras-chave: Convenção de budapeste, Hacking investigativo, Investigação, Lawful hacking, Legislação brasileira

Abstract/Resumen/Résumé

The objective is a detailed analysis of issues related to lawful hacking or legal/investigative hacking and its role in the context of the debate known as Going Dark Problem: complexity derived from the temporal mismatch between technology and regulation and action in

[1] Delegado de Polícia Civil no Estado do Rio Grande do Sul. Mestre e Doutor em Direito pelo PPGD da Universidade La Salle Canoas – RS. Lattes: http://lattes.cnpq.br/9475388941521093.

[2] Mestre em Direitos Humanos, especialista em Sistemas de Justiça Criminal. Procurador da República, investigador de criptoativos certificado (Chainalysis e TRM). Docente da Escola Superior do MPU. Lattes: http://lattes.cnpq.br/1652283673415980.

criminal investigation in relation to the protection of personal data in the digital environment. Therefore, this study examines the perspectives for and against the use of special investigative techniques, such as legal/investigative hacking and the use of remotely controlled monitoring tools, exploring the complexity of the legal and ethical implications associated with these practices. It is emphasized that the appropriate use of these techniques can be compatible with the protection of citizens' fundamental rights, as long as principles such as transparency, proportionality and auditability are observed. This includes the need for strict judicial oversight and strict compliance with legal requirements. The importance of a continuous public debate and the participation of the Legislative Branch in the regulation of legal/investigative hacking is highlighted, noting the need for international cooperation and compliance with treaties and conventions, such as the Budapest Convention, to address cybercrime on a global scale. Therefore, the inductive method is used, starting from the analysis of special investigation techniques, especially the use of remotely controlled monitoring tools, within the scope of the crime prosecution system in Brazil and around the world. As a methodology, a bibliographic review is used, complemented by analysis of documents and jurisprudence on the topic.

Keywords/Palabras-claves/Mots-clés: Budapest convention, Investigative hacking, Investigation, Lawful hacking, Brazilian legislation

1 INTRODUÇÃO

Nos últimos anos, o mundo testemunhou crescente debate em torno das implicações éticas, legais e tecnológicas do *hacking* legal, também conhecido como *lawful hacking*. Este fenômeno emergente é impulsionado pela necessidade das autoridades policiais e governamentais de enfrentar os crimes cibernéticos e ameaças à segurança nacional em ambiente digital cada vez mais complexo. O presente artigo busca explorar questões cruciais relacionadas ao *lawful hacking* ou *hacking* investigativo.

Esta pesquisa tem o objetivo de fornecer uma visão abrangente das práticas, desafios e implicações éticas associadas ao *hacking* legal. Abordando ampla gama de tópicos, desde a formatação e uso do(s) conceito(s) até as necessárias considerações legais e de transparência, o texto visa a proporcionar visão holística de campo de estudo que evolui rapidamente. Além disso, o artigo destaca perspectivas internacionais sobre o tema, comparando abordagens adotadas em diferentes jurisdições.

Pretende-se, então, com esta pesquisa [introdutória] dar o ponto de partida para a exploração mais profunda das complexidades do *hacking* legal / *hacking* investigativo / *lawfull hacking*, fornecendo *insights* a pesquisadores, profissionais de segurança cibernética, legisladores e aqueles interessados na interseção entre tecnologia, segurança e privacidade.

Ao longo deste artigo, pautado em revisão crítica a respeito do tema, com exploração da bibliografia existente, com base no método indutivo, as questões levantadas serão exploradas, buscando ampliar a compreensão do *hacking* legal/investigativo no mundo digital em constante transformação, especialmente a partir do cibersistema da Internet (Wendt, 2023).

2 MODALIDADES PROCEDIMENTAIS DE INVESTIGAÇÃO CRIMINAL NO ÂMBITO DA REDE DE COMPUTADORES E DA TECNOLOGIA DA INFORMAÇÃO

A investigação financeira possui estreita relação com a possibilidade de o Estado coletar evidências digitais na medida em que, atualmente, a grande maioria das transações financeiras deixam algum rastro digital.

As principais evidências em investigações financeiras contemporâneas são digitais, estão em ambientes e bancos de dados tecnológicos. E há limites legais e tecnológicos para a capacidade do Estado em coletar tais evidências digitais. Quando essas limitações

comprometem a capacidade dos órgãos de investigação e persecução penal fazerem seu trabalho, fala-se que há um problema de **obscurecimento** (*going dark*).

2.1 *Going Dark Problem*: o descompasso [temporal] entre tecnologia e a legislação

Os criminosos atualizam continuamente suas técnicas para incorporar as mais recentes tecnologias emergentes em seu *modus operandi*. O crime organizado é sempre o primeiro a adotar a tecnologia. Os criminosos adotaram o mundo *online* muito antes que a polícia pudesse ao menos ter contemplado a ideia e, desde então, estão sempre um passo à frente das autoridades (Goodman, 2015, p. 7-8).

A lei não necessariamente acompanhou e acompanha o ritmo da tecnologia e essa desconexão [temporal] tem criado significativo problema para os integrantes do sistema de Segurança Pública e, especialmente, do sistema de persecução criminal. Se, por um lado, as autoridades públicas se encontram cada vez mais no escuro, crimes graves – como terrorismo, pedofilia *online*, tráfico de drogas etc. – são cometidos, invariavelmente, com um importante componente tecnológico.

O FBI chama o descompasso entre a tecnologia e a legislação de "obscurecimento" (*going dark*). Os agentes da lei (*law enforcement agents*), que têm a responsabilidade de investigar crimes, nem sempre têm acesso às provas necessárias para processar crimes e prevenir o terrorismo e outros delitos no âmbito digital. Em muitos locais, os agentes da lei têm autorização legal para interceptar e acessar comunicações e informações de acordo com ordens judiciais, mas muitas vezes não tem a capacidade técnica para isso (Comey, 2014; Comey, 2015; Senate, 2015; Pfefferkorn, 2018).

Desde 2014, as agências de investigação se deparam com o cenário em que suas capacidades de interceptação de conversas estão ficando obscurecidas como resultado de novas formas de criptografia introduzidas por padrão em serviços e produtos de amplo consumo – tais como a criptografia de ponta-a-ponta dos mensageiros [WhatsApp, Telegram etc.] e a criptografia sobre dados em repouso de dispositivos – sem que as empresas possuam acesso às chaves de desencriptação.

Para os problemas do obscurecimento, várias soluções foram aventadas, desde o radical banimento desse tipo de criptografia, passando por obrigar as empresas a manterem um *backdoor*, que seria fornecido às autoridades à vista de ordem judicial, até obrigar o investigado a fornecer as chaves, sob pena de ser processado em caso de negativa. Nenhuma dessas soluções

avançou significativamente por esbarrarem em considerações importantes sobre os direitos fundamentais dos usuários.

Outra solução apontada para o problema advindo do obscurecimento, sem comprometer a criptografia, foi reinventar a investigação criminal. Pesquisadores entendem exagerada a *metáfora do obscurecimento* porque ela sugere que as comunicações estão ficando fora de alcance de forma inexorável: 'uma abertura está se fechando e quando fechar, estaremos cegos' (Zittrain; Olsen; O'Brien; Schneier, 2016). Essa imagem não retrata a situação atual e a trajetória do desenvolvimento tecnológico.

Serviços de criptografia e aqueles que ocultam o provedor dificultam as investigações em alguns casos, mas o cenário é muito mais variado do que sugere a metáfora do obscurecimento. Para Zittrain, Olsen, O'Brien e Schneier (2016), sempre haverá bolsões de penumbra e alguns pontos cegos – canais de comunicação que resistem à investigação estatal –, mas isso não significa que as autoridades estão ficando completamente "no escuro".

Algumas áreas estão *mais iluminadas* agora do que no passado e outras estão ficando mais claras. Em particular, eles apontam três tendências que facilitam o acesso de agentes da lei a dados: a) o modelo de negócios de muitas empresas depende do acesso a dados de usuários; b) cada vez mais, produtos são oferecidos como serviços e as arquiteturas se tornaram mais centralizadas por meio de computação em nuvem e centros de processamento de dados – serviços que implicam relação contínua entre fornecedores e usuários, prestando-se mais ao monitoramento e ao controle do que um produto (em que a tecnologia é comprada uma vez e usada sem outras interações com o fornecedor); e c) a Internet das Coisas [IoT] abriu nova fronteira para conectar em rede objetos, máquinas e ambientes.

Uma das formas promissoras de reinvenção da investigação criminal em face do problema do obscurecimento é o emprego de tecnologia de ponta por autoridades de aplicação da lei, conforme as possibilidades legais da legislação de cada país.

O emprego dessas tecnologias por agentes do Estado, dentro das possibilidades legais e sob rigorosa supervisão judicial, indica o caminho possível para que se consiga investigar criminosos cada vez mais tecnológicos. Uma dessas tecnologias são os *spywares*, sobre os quais recai, em razão da nomenclatura, a suspeita 'natural' de sua utilização. Analisa-se esse tema no próximo tópico.

2.2 *Spyware* e usabilidades investigativas: a questão da nomenclatura

Spyware é espécie de *malware* e representa um software inserido em sistema de computador, sem o conhecimento do usuário, com o objetivo de acessar dados armazenados ou interceptar dados de tráfego, emitidos ou recebidos (Communication ..., 2006, p. 2).

O mais famoso *spyware* é o Pegasus®, cujo estudo de caso, dado o grande escrutínio público a que vem sendo submetido nos últimos dois anos, representa uma oportunidade de se abordar o emprego de *spywares* em investigações criminais.

O software Pegasus® foi desenvolvido pela empresa israelense NSO Group e vendido a agências governamentais para uso antiterrorista e policial (Mendonça; Monteiro; Gaspar; Santos, 2021). O preço estimado do Pegasus, em 2016, era U$ 600.000 por ano, mais taxa de instalação de U$ 500.000, para um sistema capaz de rastrear dez alvos simultaneamente[1].

As funcionalidades do Pegasus® foram descritas em algumas fontes fidedignas de informação. O *European Data Protection Supervisor* lançou em 2022 um relatório denominado *Preliminary Remarks on Modern Spyware*, elencando as seguintes funcionalidades (European, 2022):

> Primeiro, ele **obtém privilégios de administrador** dentro do sistema de computador alvo [dispositivo]. Com isso, ele pode acessar os dados armazenados no aparelho celular (tais como textos, e-mails, pesquisas na web, fotos, vídeos etc.), realizar interceptação dos dados de tráfego do sistema de computador (tais como chamadas telefônicas, localização por GPS etc.) e acessar remotamente microfone e câmera do aparelho celular (European, 2022);
> Segundo, o Pegasus pode realizar **ataque de zero-click** (*zero-click attack*), ou seja, o software pode interagir com o sistema do dispositivo sem que o usuário alvo precise realizar nenhuma ação – sem solicitação de instalação, apresentação de telas, *download* de aplicativos ou requisição de ações. Basta que o operador da ferramenta saiba algum identificador relacionado ao alvo (número de telefone, e-mail, nome de usuário em mídia social etc.), que o Pegasus® conseguiria infectar o dispositivo utilizado (European, 2022); e
> Terceiro, a invasão do Pegasus® é **difícil de detectar**, a menos que sistema operacional seja alimentado por mecanismos seguros de registro do sistema. Pesquisadores suspeitam que as versões recentes do Pegasus® atuam apenas na memória temporária do dispositivo e não no disco rígido, significando que, uma vez desligado, os vestígios do software desaparecem. Além disso, a computação em nuvem permitiu a empresas que vendem *spyware* instalem sua infraestrutura de ataque na nuvem, sem a necessidade de o cliente do *spyware* instalar uma ferramenta específica (European, 2022).

Também em 2022, o Conselho da Europa elaborou o documento *Pegasus Spyware and its impacts on human rights*, descrevendo as formas como ele infecta dispositivos (Council,

[1] Existem outros softwares que propagam possuir funcionalidades semelhantes ao Pegasus®, tais como Omnigo, eFORCE Software Suite, Mark43 Platform, Spillman Records Management, FirstTwo, PowerDMS, Nuance, CrimeSoft, Asset Panda and Dynamic Public Safety (Software, 2023).

2022). Segundo o documento, o *spyware* pode infectar telefones dos alvos através de uma variedade de mecanismos. Alguns envolvem mensagem (SMS, iMessage, WhatsApp, e-mail) com um link para um site; quando clicado, o link fornece software malicioso que infecta o dispositivo.

Outros usam o citado ataque zero-click (*zero-click attack*), também denominado exploração zero-click (*zero-click exploit*), onde vulnerabilidades em serviços de mensagens, por exemplo, permitem a infecção simplesmente recebendo uma mensagem e nenhuma interação do usuário é necessária.

O Pegasus também usa "injeções de rede" (*network injections*). A navegação na web de um alvo pode deixá-lo vulnerável a ataques sem a necessidade de clicar em qualquer link malicioso. Essa abordagem envolve esperar que o alvo visite um site que não esteja protegido durante suas atividades online normais. Depois de visitar um site desprotegido, o software de injeção pode interceptar a transação e desencadear uma infecção.

Além desses mecanismos, há a opção manual: se um agente conseguir obter acesso físico ao telefone alvo, o *spyware* pode ser instalado manualmente. Essa opção exige procedimentos de engenharia social[2], planejados previamente.

Em todas as abordagens de infecção, o objetivo do Pegasus® é obter controle total do sistema operacional do dispositivo móvel por *root* (em dispositivos Android[3]) ou *jailbreak* (em dispositivos Apple iOS[4]). O *root* e o *jailbreak* removem os controles de segurança incorporados nos sistemas operacionais e, eventualmente, permitem que ele execute o código modificado. No caso de *spyware*, assim que um dispositivo é desbloqueado, o intruso pode implantar outro software para proteger o acesso remoto aos dados e funções do dispositivo. É provável que o usuário permaneça completamente inconsciente, a menos que ocorram comportamentos inadequados perceptíveis.

Uma vez instalado, o Pegasus® pode, teoricamente, coletar quaisquer dados do dispositivo e transmiti-los de volta ao invasor. Ele pode executar qualquer código que desejar no dispositivo do alvo, usar a câmera e o microfone do dispositivo por comandos remotos em tempo real, extrair contatos, registros de chamadas, pesquisas na web, histórico de navegação na web, mensagens de texto, fotos, vídeos, configurações, registros de localização, como bem como informações de aplicativos como iMessage, Gmail, Viber, Facebook, WhatsApp,

[2] Sobre engenharia social, ver mais em Coelho, Rasma e Morales (2013).
[3] Normalmente, o root em um dispositivo Android é feito pelo usuário para instalar aplicativos e jogos de fontes não suportadas ou habilitar funcionalidades que foram bloqueadas pelo fabricante.
[4] O *jailbreak* pode ser implantado em dispositivos Apple para permitir a instalação de aplicativos não disponíveis na Apple App Store ou para desbloquear o telefone para uso em redes celulares alternativas.

Telegram, Skype e outros. O *spyware* também monitora as teclas digitadas em um dispositivo infectado, todas as comunicações escritas, incluindo senhas, ficam visíveis para o invasor.

O Pegasus® opera por meio de violação de mecanismos de segurança e explorando vulnerabilidades não corrigidas de sistemas de computador, motivo pelo qual somente pode ser utilizado em circunstâncias estritas e sob rígida supervisão judicial.

Descritas as funcionalidades do Pegasus®, há que se ponderar sobre a nomenclatura *spyware*, quase sempre traduzida como "software espião". Como ferramenta possível de utilização em procedimentos policial-investigativos, sob rígido controle estatal e supervisão do Poder Judiciário, não se pode falar em "espionagem".

Como se verá no decorrer desta pesquisa, técnicas especiais de investigação previstas em lei subsidiam o emprego da tecnologia, que é mais bem descrita como *ferramenta de monitoramento remotamente controlada*. O processo de seu uso, então, permite o monitoramento remoto e o controle de suas funcionalidades, a depender da autorização judicial correspondente.

3 *LAWFUL HACKING*: O *HACKING* INVESTIGATIVO COMO FERRAMENTA DE PERSECUÇÃO DA CRIMINALIDADE NO ÂMBITO DA INTERNET

Os temas são novos e precisam ser trabalhados em pesquisas acadêmicas brasileiras, especialmente quando há a importação de conceitos e metodologias, oriundas de outros países, cuja cultura jurídica pode ser diferente da brasileira. Por isso, não é adequado importar um conceito ou técnica sem entender o contexto cultural de sua criação e, principalmente, o contexto cultural e jurídico de onde se pretende adaptá-la.

Por esse motivo, há necessidade de compreender o conceito e funcionalidades do *lawful hacking*.

3.1 *Lawful Hacking*: o que é isso?

Essa modernização das tecnologias para investigações policiais/criminais é, por vezes, referida como ***lawful hacking***, ou ***government hacking***, que consiste na implantação, por autoridades investigativas, de ferramentas que permitem a invasão de sistemas de computadores, possibilitando o acesso ao seu conteúdo (Liguori, 2020)[5].

[5] Sobre os variados empregos do termo *lawful hacking*, ver Dutra, Pereira, Santarém e Vieira (2023) e Canto (2023).

Há rejeição a essa expressão em decorrência do caráter intrinsecamente ilegal do *hacking*. Usa-se o termo *hacking* como "uma situação em que alguém abusa de sua autoridade para acessar ilegalmente uma rede de informações enquanto usa computador ou outro dispositivo de processamento de informações" (Liger; Gutheil, 2022).

Ainda que envolva tecnologia nova, o emprego legal e proporcional de ferramenta de monitoramento remotamente controlada não configura um *hacking*. Antes, o emprego dessas tecnologias pode se enquadrar, conforme a legislação nacional de cada país, como *técnica especial de investigação*, ou seja, uma forma de coletar informações sem que o conhecimento do alvo (Liger; Gutheil, 2022, p. 16).

É evidente que essas técnicas especiais de investigação precisam ser previstas em lei e se submeterem a rigorosa supervisão judicial em cada investigação em que a tecnologia for indicada para uso. Não se quer, em absoluto, a repetição de casos de emprego ilegal (*hacking, spyware* etc.) dessas tecnologias, como noticiado nos últimos anos.

Considera-se legítima a preocupação com empregos ilícitos de intrusão por *spywares* que está sob escrutínio das autoridades europeias de proteção de dados desde, pelo menos, o ano de 2015. O caso de emprego ilícito do *spyware* Pegasus® obteve grande repercussão, sobretudo após a divulgação da sequência de reportagens denominada *Pegasus Project*, e contribuiu para a elaboração de estudos cada vez mais aprofundados sobre o assunto[6].

Usadas dentro das hipóteses legais e com ampla capacidade de supervisão judicial e aditabilidade, o emprego de novas tecnologias em *técnicas especiais de investigação* não representa restrição ilegítima a direitos fundamentais. É justamente o controle legal e democrático sobre o emprego da tecnologia que diferencia o seu emprego para fins legítimos do Estado daquele estado de coisas ilegal que normalmente se chama de 'tecnoautoritarismo' **(**Laut; DPBR, 2020**)**.

3.2 Neutralidade Tecnológica das Técnicas Especiais de Investigação

A Constituição Federal assegura a preservação da intimidade, do sigilo das comunicações telemáticas (art. 5º, XII) e dos dados pessoais, inclusive em meios digitais (LXXIX). Tal proteção pode ser afastada "por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Para o problema do obscurecimento – *Going Dark Problem* –, uma das respostas possíveis é o emprego

[6] O *Pegasus Project* começou a ser publicado em julho de 2021 por um consórcio internacional de jornalistas (https://forbiddenstories.org/case/the-pegasus-project/).

legítimo de tecnologias de ponta, conforme a legislação nacional de cada país, como técnica especial de investigação.

Tais técnicas especiais estão previstas, para crimes cibernéticos e outros dependentes da coleta eletrônica de evidências, na Convenção de Budapeste (art. 14, CB, "Âmbito de aplicação dos dispositivos processuais") e em normas nacionais, plenamente compatíveis entre si e com a Constituição Federal de 1988, conforme referido por Martins (2023a; 2023b).

No art. 14.1 da Convenção de Budapeste se prevê que "Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer os poderes e procedimentos previstos nesta seção para o fim específico de promover investigações ou processos criminais." No Brasil, há *enabling legislation* para a grande maioria das técnicas de investigações previstas no tratado.

A *conservação expedita de dados de computador* (arts. 16 e 29, CB) e de *dados de tráfego* (art. 17, 1.a, CB) são, no Brasil, *ordens de preservação de dados* previstas nos art. 13, § 2º, e art. 15, § 2º, ambos do Marco Civil da Internet[7]. A *ordem de exibição*, do art. 18, 1.b, equivale à *requisição da dados cadastrais* prevista em diversos dispositivos nacionais (ex: art. 13-A, CPP, arts. 15 a 17 da Lei n. 12.850/2013 e art. 10, §3º, Marco Civil da Internet).

Conforme se viu quando da descrição das funcionalidades da tecnologia, os *dados acessados por ferramenta de monitoramento remotamente controlada* podem se configurar como *dados de computador* ou *dados de tráfego*. Essas espécies de dados podem ser acessadas legítima e expressamente em investigações formais pelas autoridades estatais por meio de uma série de técnicas de investigação previstas na Convenção de Budapeste.

Para o acesso aos dados de computador, a Convenção prevê a *busca e apreensão de dados de computador* (art. 19, CB), uma mescla das *técnicas de investigação de afastamento do sigilo telemático* (art. 7º, III, e art. 10, § 2º, da Lei n. 12.965/2014) e *busca e apreensão* (arts. 240 a 250, CPP).

A *obtenção de dados de tráfego em tempo real*, dos arts. 20 e 33 da Convenção de Budapeste, e a *interceptação de dados de conteúdo*, dos arts. 21 e 34, da mesma Convenção, são, no Brasil, modalidades da *técnica especial de investigação da interceptação telemática* (Lei n. 9.296/1996).

[7] Apenas a revelação parcial de dados de tráfego não pode ser realizada da forma prevista no art. 17, 1.b, da Convenção de Budapeste, complementado pelo art. 30. No Brasil, somente por ordem judicial, em um procedimento de interceptação telemática, é possível a revelação à autoridade de um conjunto de dados de tráfego que permita a identificação os provedores de serviço e o caminho por meio do qual a comunicação se realizou.

Todas essas questões se apresentam face ao vertiginoso desenvolvimento tecnológico e precisam ser bem equacionadas para que não provoquem a paralisação das atividades de investigação de crimes e persecução penal, uma vez que a criminalidade não vê barreiras que possam cerceá-la; pelo contrário, tiram proveito dos avanços tecnológicos. Há que se aplicar o arcabouço jurídico existente, assegurando-se que em cada caso concreto as garantias da intimidade, da vida privada e do sigilo das comunicações estejam presentes, observando-se o devido processo legal, presentes a motivação e fundamentação das decisões judiciais que afastam essas garantias (Brasil, 2021).

Não só isso, as *técnicas especiais de investigação* previstas na legislação nacional atendem ao devido processo legal e às exigências de *quality of law*, que abrange garantias de previsibilidade, segurança jurídica, controlabilidade, recorribilidade e proporcionalidade, no sentido da limitação da interferência (compressão) sobre os direitos fundamentais em jogo.

A neutralidade tecnológica das tecnologias empregadas nas *técnicas especiais de investigação*, tais como adiante descritas, não impõe que elas sejam sempre empregadas com o auxílio de um terceiro – tal como algum provedor de conexão, de aplicação ou empresa de telefonia.

A lei não impõe intermediário algum, como se garante fosse, às técnicas de coleta de provas, desde que o Estado possa realizar a atividade diretamente com a garantia de sua cadeia de custódia. O que interessa, como se verá, é a auditabilidade da atividade estatal e a existência de ordem judicial (Martins, 2023c).

3.2.1 Afastamento de Sigilo Telemático

O acesso a dados de computador pode ocorrer para obtenção de *acesso prospectivo das comunicações em fluxo* (via provedores de acesso ou infiltração, em modalidades de *interceptação telemática*) ou por *acesso retrospectivo às comunicações armazenadas nos provedores de conexão, nos provedores de aplicação ou, ainda, em dispositivos eletrônicos dos usuários*.

Tal diferença foi destacada na Lei n. 12.850/2013, quando tratou sobre a investigação criminal e meios de obtenção de provas relacionados às organizações criminosas, ao dispor sobre o *acesso a registros de ligações telemáticas* (art. 3º, inciso IV), ao lado da *interceptação de comunicações telemáticas* (art. 3º, inciso V).

Os dados armazenados em sistema de computador podem ser acessados na forma dos art. 7º, III, e art. 10, § 2º, do Marco Civil da Internet. Atendidos esses requisitos, basta que a

autorização judicial seja comunicada às empresas responsáveis pelos serviços telemáticos, configuradas pelo Marco Civil como *provedores de internet*. Esse procedimento atende aos *dados armazenados nos provedores de conexão e nos provedores de aplicação*. A partir dessa ordem judicial, pode-se acessar dados de computador que estão em posse de provedores de conexão (tais como data, hora, fuso horário e IP) e de provedores de aplicação (conteúdo de e-mails, serviços de nuvem etc.).

Há *dados de computador, porém, que estão armazenados apenas em sistemas de computador do investigado* (ex: smartphone, computador, HD externo etc.), não em posse de provedores de conexão ou de aplicação. Se a investigação necessitar acessar tais dados, ela precisa coletar os dados diretamente do sistema de computador.

Em casos em que *o sistema de computador não está conectado na Internet*, nada há a fazer senão acessá-lo fisicamente. Para isso, há a possibilidade de realização da apreensão de mídias em buscas judicialmente autorizadas, na forma do arts. 240 a 250 do Código de Processo Penal.

Mesmo para *dispositivos conectados à Internet*, até o advento das *modernas ferramentas de monitoramento remotamente controladas*, a solução possível em investigações estatais era realizar uma busca e apreensão tradicional, tentar encontrar o sistema de computados (ex: celular), tentar realizar a extração física de seus dados para, só então, analisar seu conteúdo. O processo era demorado e incerto, pois não raras vezes o celular podia ser escondido pelo alvo, destruído por ele ou simplesmente estava protegido por senha, que impedia a extração dos dados.

O emprego de *ferramenta de monitoramento remotamente controlada* permite o acesso ao celular fisicamente distante, com grau de certeza e sucesso avançados. Havendo ordem judicial e rígido controle sobre o emprego da ferramenta, o acesso a dados de computador, armazenados em sistemas e dispositivos (computadores, tablets, smartphones etc.) não acessíveis diretamente ao Estado, pode ser feito legalmente por meio de emprego dessa tecnologia.

3.2.2 Interceptação Telemática

O Brasil possui norma constitucional prevendo a possibilidade de interceptação do fluxo de dados telemáticos (art. 5º, inciso XII, CF) e lei que regulamentou o dispositivo (Lei n. 9.296/1996). A "*interceptação do fluxo de comunicações em sistemas de informática e*

telemática", definido na lei, trata efetivamente de *dados de tráfego*, como definido na Convenção de Budapeste.

A lei nacional realiza juízo de proporcionalidade na restrição dos direitos fundamentais ao estabelecer as *hipóteses de interceptação*: (a) existência de indícios razoáveis da autoria ou participação em infração penal; (b) a prova não puder ser feita por outros meios disponíveis; e, (c) o fato investigado constituir infração penal punida com pena de reclusão. Em qualquer hipótese, as autoridades de investigação (d) devem descrever com clareza a situação objeto da investigação, com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada (art. 2º, Lei n. 9.296/1996).

Para operacionalização da interceptação telemática, *a Lei n. 9.296/1996 é tecnologicamente neutra*, ao indicar que o pedido da polícia ou do Ministério Público "conterá a demonstração de que a sua realização é necessária à apuração de infração penal, *com indicação dos meios a serem empregados*" (art. 4º, grifos nossos). O legislador anteviu que não havia como prever em lei ferramentas tecnológicas que realizassem a interceptação e delegou a polícia e ao Ministério Público a indicação dos meios de interceptação.

Em seguida, a Lei n. 9.296/96 prevê que o magistrado decidirá fundamentadamente, "indicando também a forma de execução da diligência" (art. 5º). Não há restrições legais ao emprego de tecnologias para interceptação telemática no Brasil. Havendo indicação dos meios no pedido (art. 4º) e decisão judicial autorizando o emprego daquela forma de execução da diligência (art. 5º), a medida será legal e a prova produzida válida.

Ademais, o art. 9º da mesma lei esclarece que os dados não importantes à prova serão inutilizados por decisão judicial, medida necessária em caso de a *ferramenta de monitoramento remotamente controlada* capturar dados que ultrapassem a necessidade da investigação. Trata-se de medida coincidente com as cautelas da Lei Geral de Proteção de Dados (art. 16, Lei n. 13.709/2018) sobre eliminação de dados após o término do tratamento.

Os questionamentos se transferem para outro sentido: *ferramentas de monitoramento remotamente controladas* são capazes de restringir seu alcance apenas aos alvos investigados?

Nesse caso, a demonstração da viabilidade dessas tecnologias para restringir o seu alcance a apenas os alvos é um dos pontos fundamentais a serem indicados pelas autoridades de investigação no momento da indicação dos meios no pedido (art. 4º) e apreciadas na decisão judicial autorizando o emprego daquela forma de execução da diligência (art. 5º). Se alguma ferramenta de monitoramento remotamente controlada não puder ter demonstrada essa capacidade de restrição de alvos, ele não poderá ser empregado pois enseja grave violação de direitos fundamentais. Os limites devem ser, então, descritos no pedido e na autorização judicial.

Outra consideração importante diz respeito à necessidade de a ferramenta tecnológica empregada para a interceptação telemática *não comprometer, com seus métodos de intrusão, a integralidade da prova*. Se alguma tecnologia não possuir capacidade de manutenção da integralidade da prova contra manipulação dos agentes públicos, essa ferramenta não pode ser empregada.

Em duas oportunidades, o Superior Tribunal de Justiça invalidou provas de interceptação telemática que, com as técnicas empregadas, permita, em tese, que o agente público interferisse na integralidade da prova. No RHC n. 99.735-SC, relatora Ministra Laurita Vaz, Sexta Turma, julgado em 27/11/2018, a coleta dos dados do aplicativo WhatsApp pela polícia ocorreu mediante apreensão judicialmente autorizada de celular e subsequente *espelhamento* das mensagens recebidas e enviadas em outro computador por meio da funcionalidade *WhatsApp Web.*

O segundo caso ocorreu no REsp n. 1.806.792/SP, também relatado pela Ministra Laurita Vaz, julgado em 11/5/2021. Pretendeu-se que a operadora de telefonia, quando acionada, *habilitasse o chip do agente investigador, em substituição ao do usuário*, a critério da autoridade policial, que teria pleno acesso, em tempo real, às chamadas e mensagens transmitidas para a linha originária, inclusive via WhatsApp. No caso, mais uma vez, invalidou-se a prova pela possibilidade potencial de os agentes da lei interferissem na integralidade da prova.

3.2.3 Captação Ambiental

Uma das funcionalidades das *ferramentas de monitoramento remotamente controladas* é o acesso à câmera e ao microfone do sistema do dispositivo. Nesse caso, se a ferramenta permite a captação de dados de áudio e vídeo a partir do acesso à câmera e ao microfone, a técnica especial de investigação correspondente na legislação nacional é a *captação ambiental de sinais eletromagnéticos, ópticos ou acústicos*, com previsão no artigo 8º-A da Lei nº 9.296/1996, incluído pela Lei n. 13.964/2019.

3.2.4 Infiltração Virtual

Ante as funcionalidades descritas acima da tecnologia de *ferramenta de monitoramento remotamente controlada*, pode-se antever o seu emprego para, legitimamente, realizar *infiltrações virtuais*, tal como descrito na técnica especial de investigação prevista na legislação brasileira.

O agente virtual infiltrado representa técnica adequada, por exemplo, a *investigação de redes sociais fechadas ou grupos limitados de pessoas utilizando-se de aplicativos de mensagens*. Nesses casos, o uso de *ferramenta de monitoramento remotamente controlada* é mais eficaz para obter essas mensagens *sem a necessidade de atuação de um agente real*, que precisa de tempo para ganhar a confiança dos demais usuários e ser admitido no círculo fechado dessas pessoas, estando sujeito a ser descoberto caso cometa algum deslize e muitas vezes sendo obrigado a cometer infrações penais, desde que autorizado judicialmente para tanto (Brasil, 2021)[8].

A *ferramenta de monitoramento remotamente controlada* é, portanto, uma alternativa a ser utilizada quando não há tempo para que um agente real se imiscua no grupo criminoso de forma a ser aceito e passe a ter acesso à comunicação do grupo.

A *infiltração tradicional* não é um método que pode ser banalizado, pois é lento e traz sérios riscos à integridade física do agente policial (Reschke; Wendt; Matsubayaci, 2021). A *infiltração virtual*, embora também seja lenta, minimiza esses riscos e é eficaz para as redes virtuais, nas quais nem sempre há um grupo organizado. Muitas vezes, embora o ambiente seja restrito, os próprios integrantes não se conhecem pessoalmente.

No Brasil, a infiltração de agentes está minuciosamente descrita nos arts. 10 a 14 da Lei n. 12.850/2013 e nos arts. 190-A a 190-E do Estatuto da Criança e do Adolescente, com redação da Lei n. 13.441/2017. Em ambos os casos, os limites da infiltração virtual de agentes também são fixados por decisão judicial, semelhante à interceptação telemática.

3.3 Experiências Internacionais: o que podemos apreender/aprender?

A discussão europeia sobre o assunto tratado neste estudo remete a caso decidido pela Corte Constitucional alemã em 2008, em que se tratou sobre novo direito fundamental relacionado à privacidade: o direito à confidencialidade e à integridade dos sistemas informáticos.

Segundo analisado por Mendes (2015; 2020), o caso dizia respeito à análise de constitucionalidade da lei do Estado de Nordrhein-Westfalen, que permitia às autoridades locais de inteligência fazerem a busca remota de informações e o monitoramento *online* de computadores de suspeitos de cometerem práticas criminosas[9].

[8] Sobre a metodologia de infiltração de policiais na Internet e outras observações práticas, vide Reschke, Wendt e Matsubayaci (2021).
[9] Sobre o tema, ver também Menk (2015).

O Tribunal alemão declarou inconstitucional a lei sob o fundamento de violação do direito geral à personalidade protegido constitucionalmente. Em vez de aplicar o *direito à autodeterminação informativa*, que já estava consolidado na jurisprudência do tribunal e fundamentava a ação ajuizada, a Corte extraiu do *direito geral à personalidade* (art. 2, I, c/c art. 1, I, da Lei Fundamental alemã) um *direito fundamental à garantia da confidencialidade e da integridade dos sistemas informáticos* (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

O objeto da proteção constitucional, segundo a decisão, é o próprio sistema informático pessoal, e por consequência o indivíduo que o utiliza. O julgamento esclareceu que a infiltração dos sistemas informáticos não estaria completamente vedada pela Lei fundamental alemã, mas somente poderia ser realizada se presentes determinadas condições: (a) a existência de uma base legal específica, (b) a emissão de autorização judicial e (c) a identificação de perigo concreto a bem jurídico fundamental, como a vida e a liberdade individuais ou a segurança da coletividade.

De toda forma, ainda que atendidos esses requisitos, em nenhuma hipótese poderia tal monitoramento violar o núcleo da intimidade e das formas de vida privada do indivíduo. Isso significa que medidas adicionais de segurança devem ser adotadas para que informações íntimas e excessivas não sejam coletadas durante a infiltração ou – caso isso não seja possível – que tais informações sejam descartadas ou desconsideradas no processo de avaliação dos dados.

Conforme referido, o *European Data Protection Supervisor* (EDPS) possui relatório de 2022, específico sobre o *spyware* Pegasus® (European, 2022). Nesse documento, consigna-se que a interceptação de comunicações é regulamentada na legislação nacional de praticamente todos os Estados-Membros da União Europeia. As condições legais e salvaguardas para a utilização da vigilância digital e interceptação de comunicações foram objeto de ampla análise e interpretação tanto pela Corte de Justiça da União Europeia (*Court of Justice of the European Union*, CJEU) como pela Corte Europeia de Direitos Humanos (*European Court on Human Rights*).

Em particular, no julgamento dos processos C-511/18 e C512/18 (*La Quadrature du Net* e outros), a Corte esclareceu a aplicabilidade do direito da UE a certas medidas adotadas por motivos de segurança nacional. Nesse julgado, *uma grave ameaça à segurança nacional, real e presente ou previsível, poderia justificar gravíssimas ingerências em direitos fundamentais, sujeitas a estritas condições e garantias*. Isso implica a necessidade de avaliação combinada e

baseada em fatos da eficácia da medida para o objetivo perseguido e se é menos intrusiva em comparação com outras opções para atingir o mesmo objetivo.

O EDPS anota algumas reportagens noticiando que certas funcionalidades do Pegasus® podem ser *desativadas*, a fim de limitar o caráter intrusivo da ferramenta, o que pode ter impacto no resultado da avaliação da proporcionalidade e da necessidade.

O Alto Comissariado das Nações Unidas para os Direitos Humanos entende que, dados os impactos adversos substanciais do uso de *spywares*, seu uso deve ser limitado aos casos em que serviriam para prevenir ou investigar um crime grave específico ou ato que represente grave ameaça à segurança nacional **(**Statement, 2021**)**.

Como último recurso, todas as medidas menos intrusivas devem ter sido esgotadas ou se mostrado inúteis. Em casos extremos tais, o emprego do *spyware* deve ser estritamente limitado em escopo e duração, somente acessando e coletando dados relevantes para a investigação. Ademais, a medida também deve estar sujeita a supervisão independente rigorosa e a aprovação prévia por um órgão judicial é essencial.

A decisão remonta ao já observado quanto à legislação nacional: *ferramentas de monitoramento remotamente controladas* podem ser utilizadas, porém com a devida vênia judicial, com controle e auditorias possíveis, observando-se os limites técnicos da amplitude de sua utilização – parâmetros que serão analisados no próximo tópico.

3.4 Transparência, Proporcionalidade e Auditabilidade

Os argumentos contrários a *ferramentas de monitoramento remotamente controladas* destacam sempre o perigo que elas podem representar a direitos fundamentais se o seu emprego ocorrer na clandestinidade, sem autorização judicial e com desproporção entre meios de investigação e crimes investigados.

Se há um consenso em matéria tão controversa, ele reside na aceitação, em casos extremos de crimes graves que ameaçam a sociedade como um todo – como terrorismo e crime organizado –, o emprego dessas tecnologias com estritas cautelas legais e controle judicial. Contra crimes gravíssimos, o Estado não pode ficar obscurecido em sua capacidade de enfrentamento.

As leis vigentes no Brasil fornecem garantias necessárias para o uso prudente de *ferramentas de monitoramento remotamente controladas* como técnicas especiais de investigação criminal, atendendo aos requisitos de legalidade estrita, aplicabilidade somente a crimes graves (proporcionalidade) e estrito controle judicial.

As autoridades públicas devem demonstrar, sempre, em cada pedido judicial para uso dessas ferramentas, em investigações criminais, que a) elas podem ser *auditadas*, b) os agentes que a operam são *treinados* e *identificados* (nome, data e hora de acesso) e c) suas *atividades ficam registradas na ferramenta ou no sistema* com vistas a evitar questionamentos sobre a *integralidade da prova (cadeia de custódia)*.

É ônus das autoridades investigativas demonstrar ao juiz, em cada caso, que o emprego das ferramentas é *transparente*, *proporcional* e *auditável*. Se, em qualquer dos casos, a autoridade investigativa não puder demonstrar isso, a medida deve ser indeferida.

Afirmar a possibilidade das leis vigentes abrangerem o emprego de *ferramentas de monitoramento remotamente controladas* não significa dar por encerradas as possibilidades de discussão social sobre o seu emprego. O fórum mais adequado para essas discussões é, sem dúvida, o Poder Legislativo. Um projeto de lei que venha a disciplinar as possibilidades de emprego de tais tecnologias em investigações criminais é bem-vindo por dois motivos: a) o debate público é sempre benéfico às possibilidades de restrição sobre direitos fundamentais; e b) os agentes da lei precisam de segurança jurídica para realizar investigações.

Exatamente à vista desses dois motivos e após divulgação de suposto caso de abuso no Brasil (ABIN FistMile), a Procuradoria-Geral da República propôs no Supremo Tribunal Federal Ação Direta de Inconstitucionalidade por Omissão 84, em 13 de dezembro de 2023, pedindo o reconhecimento de omissão parcial do Congresso Nacional na regulação do que chama "programas de intrusão virtual remota" e "monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal" – ambos abrangidos neste artigo pela expressão *ferramenta de monitoramento remotamente controlada*.

A omissão parcial residiria na existência de norma infraconstitucional que, na visão da PGR, não satisfaz plenamente o preceito constitucional de proteção estatal da intimidade, vida privada e inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da Constituição Federal. Apesar de existirem dispositivos legais que autorizam a interceptação telemática (Lei 9.296/1996) e o afastamento de sigilo telemático (Lei 12.965/2014), assim como do sistema de proteção da dados (Lei 13.709/2018), os avanços tecnológicos criaram ferramentas de acesso a dados além do que originalmente previsto na legislação, tal circunstância promoveria, portanto, proteção insuficiente a bens jurídicos constitucionalmente tutelados.

Além de fixar prazo razoável para o Congresso Nacional legislar sobre o assunto, a ADO 84/23 pede que o STF adote soluções normativas provisórias, buscando na legislação nacional

atualmente vigente uma moldura normativa a ser aplicada provisoriamente às *ferramentas de monitoramento remotamente controladas.*

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

4 CONSIDERAÇÕES FINAIS

Objetivou-se, com esta pesquisa, proporcionar análise sobre o debate em torno do uso de técnicas especiais de investigação, particularmente o *lawful hacking*, o *hacking* legal ou *hacking* investigativo, como resposta à crescente complexidade da investigação no âmbito digital, cujas preocupações envolvem o uso de criptografia pelos investigados e a existência da criptografia de ponta a ponta, circunstâncias que têm elevado o debate sobre o chamado *Going Dark Problem*.

Esse debate, frequentemente polarizado, coloca em questão a ponderação entre a segurança pública e a privacidade dos indivíduos em cenário digital cada vez mais complexo e intrincado. Ao longo do trabalho foram destacados argumentos a favor e contra o uso dessas técnicas, bem como as implicações legais e éticas que cercam seu emprego.

Uma das principais conclusões deste estudo é que a discussão sobre a legalidade e a eficácia do *hacking* legal/investigativo é altamente complexa e multifacetada. A análise das leis e regulamentos atuais em diferentes jurisdições, como as leis brasileiras, revela uma base legal que, quando usada adequadamente, pode ser compatível com a proteção dos direitos fundamentais dos cidadãos. No entanto, isso exige que as autoridades ajam com *transparência*, *proporcionalidade* e *auditabilidade* em relação ao uso dessas *técnicas especiais de investigação*, garantindo a estrita supervisão judicial e a conformidade com os requisitos legais.

Nesse sentido, a compreensão dos debates, regulamentações e implicações do *hacking* legal/investigativo é fundamental para a formação de políticas públicas que equilibrem adequadamente a segurança e a privacidade, protegendo os direitos fundamentais dos cidadãos em um mundo cada vez mais digital e interconectado.

REFERÊNCIAS:

BOMFIM, Camila. MPF passa a investigar suspeita de segundo sistema ilegal de espionagem da Abin. **G1 Política, Blog da Camila Bomfim**, 1/11/2023. Disponível em: https://g1.globo.com/politica/blog/camila-bomfim/post/2023/11/01/mpf-passa-a-investigar-suspeita-de-segundo-sistema-ilegal-de-espionagem-da-abin.ghtml. Acesso em: 08 jan. 2024.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos e provas eletrônicas** / 2ª Câmara de Coordenação e Revisão, Secretaria de Cooperação Internacional. – 4. ed., atual. e ampl. – Brasília: MPF, 2021a.

CANTO, Mariana. Quanto vale um segredo? Dilemas éticos no "mercado do lawful hacking". IP. Rec, 2023. Disponível em: https://ip.rec.br/blog/quanto-vale-um-segredo-dilemas-eticos-no-mercado-do-lawful-hacking/. Acesso em: 10 ago. 2023.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. Engenharia Social: uma ameaça à sociedade da informação. **Exatas & Engenharias**, v. 3, n. 05, 2013.

COMEY, James B. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?. **FBI News**, 16/10/2014. Disponível em: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acesso em: 07 jul. 2023.

COMEY, James B. Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy. **FBI News**, 8/07/2015. Disponível em: https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy. Acesso em: 07 jul. 2023.

COMMUNICATION from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: on fighting spam, spyware and malicious software. **Commission of the European Communities**, of 15 November 2006. disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:EN:PDF. Acesso em: 8 ago. 2023.

COUNCIL Of Europe. Explanatory Report to the Convention on Cybercrime. **European Treaty Series**, n. 185, 2001, Disponível em: https://rm.coe.int/16800cce5b. Acesso em: 10 ago. 2023.

COUNCIL OF EUROPE. Pegasus Spyware and its impacts on human rights. **COE**, 2022. Disponível em: https://www.coe.int/en/web/freedom-expression/-/pegasus-spyware-and-its-impacts-on-human-rights. Acesso em: 27 abr. 2023.

DATAPRIVACYBR. Associação Data Privacy Brasil de Pesquisa oficia Ministério Público Federal sobre uso do software FirstMile pela Inteligência. **DataPrivacyBR Research**, 17/03/2023. Disponível em https://www.dataprivacybr.org/associacao-data-privacy-brasil-de-pesquisa-oficia-ministerio-publico-federal-sobre-uso-do-software-firstmile-pela-inteligencia/. Acesso em: 08 jan. 2024.

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená 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: 10 ago. 2023.

EUROPEAN Data Protection Supervisor. Preliminary Remarks on Modern Spyware. **EDPS**, 2022. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en. Acesso em: 17 abr. 2023.

GOODMAN, Marc. **Future crimes**: Everything is connected, everyone is vulnerable and what we can do about it. Anchor, 2015.

LAUT; DPBR. Retrospectiva Tecnoautoritarismo. **Centro de Análise da Liberdade e do Autoritarismo (LAUT) e Associação Data Privacy Brasil de Pesquisa (DPBR)**, 2020. Disponível em: https://www.dataprivacybr.org/documentos/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 18 abril 2023.

LIGER, Quentin; GUTHEIL, Mirja. The use of Pegasus and equivalent surveillance spyware. **European Parliament**, 2022. Disponível em https://www.europarl.europa.eu/cmsdata/259327/Draft%20Study_Pegasus_Legal%20framework_5%20December_EN.pdf. Acesso em: 10 ago. 2023.

LIGUORI, Carlos. Exploring Lawful Hacking as a Possible Answer to the "Going Dark". Debate, 26 **MICH. TELECOMM. & TECH. L. REV**. 317, 2020. Disponível em: https://repository.law.umich.edu/mtlr/vol26/iss2/5. Acesso em: 10 ago. 2023.

MARTINS, Tiago. Cibercrime: Convenção de Budapeste e Leis Brasileiras. **Investigação Financeira**, 14/04/2023a. Disponível em: https://investigacaofinanceira.com.br/cibercrime-convencao-de-budapeste-e-leis-brasileiras/. Acesso em: 10 ago. 2023.

MARTINS, Tiago. Cibercrime: Tipologias. **Investigação Financeira**, 14/04/2023b. Disponível em: https://investigacaofinanceira.com.br/cibercrime-tipologias/. Acesso em: 10 ago. 2023.

MARTINS, Tiago. Cibercrime: Lawful Hacking. **Investigação Financeira,** 10/05/2023c. Disponível em: https://investigacaofinanceira.com.br/investigacao-financeira-iv-lawful-hacking/. Acesso em: 10 ago. 2023.

MENDES, Laura Schertel Ferreira. Uso de softwares espiões pela polícia: prática legal? **JOTA**, 04/06/15. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acesso em: 10 ago. 2023.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar Revista de Ciências Júridicas Universidade de Fortaleza (Unifor), Fortaleza**, v. 25, n. 4, p. 1-18, 2020.

MENDONÇA, Yasmin Curzi de; MONTEIRO, Julia Iunes; GASPAR, Walter Britto; SANTOS, Kaline. Pegasus: O cavalo de Tróia da segurança cibernética. **FGV**, 29/07/2021.

Disponível em: https://portal.fgv.br/artigos/pegasus-cavalo-troia-seguranca-cibernetica. Acesso em: 10 ago. 2023.

MENK, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão, in MENDES, G. F.; SARLET, I. W.; COELHO, A. Z. P. **Série "direito Inovação e Tecnologia" - Direito, Inovação e Tecnologia** - Volume 1. São Paulo: Saraiva, 2015. E-book.

PFEFFERKORN, Riana. O Debate Estadunidense sobre Vigilância e Criptografia. In ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate**. Vol. I. São Paulo. InternetLab, 2018. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2018/08/DIGITAL_InternetLAB_DUPLA.pdf. Acesso em: 07 jul. 2023.

RESCHKE, Cristiano; WENDT, Emerson; MATSUBAYACI, Mayumi. **Infiltração Policial: da tradicional à virtual**. Rio de Janeiro: Brasport, 2021.

RIBAS, Marcel. STJ esclarece limites do espelhamento de WhatsApp Web para fins de prova. **Linkedin**, 14/08/2023. Disponível em: https://www.linkedin.com/pulse/stj-esclarece-limites-do-espelhamento-de-whatsapp-web-marcel-ribas/. Acesso em: 24 set. 2023.

SENATE Committees Briefed on Going Dark Impact. **FBI News**, 8/07/2015. Disponível em: https://www.fbi.gov/news/stories/senate-committees-briefed-on-going-dark-impact. Acesso em: 07 jul. 2023.

SOFTWARE Suggest. Pegasus Alternatives & Competitors. Disponível em: https://www.softwaresuggest.com/pegasus/alternatives. Acesso em: 10 Ago. 2023.

STATEMENT by United Nations High Commissioner for Human Rights, Michelle Bachelet. [Declaração da Alta Comissária das Nações Unidas para os Direitos Humanos]. United Nations Human Rigths, 14/09/2021. Disponível em: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E. Acesso em: 10 ago. 2023.

WENDT, Emerson. **As expectativas cognitivas e normativas dos atores de investigação policial em face dos crimes cibernéticos**. Orientador: Renata Almeida da Costa. 2023. 305 p. Tese (doutorado em Direito) – Universidade La Salle: Canoas, 2023.

ZITTRAIN, Jonathan L.; MATTHEW G. Olsen; O'BRIEN, David; SCHNEIER, Bruce. Don't Panic: Making Progress on the “Going Dark Debate." Berkman Center Research Publication 2016-1. Disponível em: https://dash.harvard.edu/handle/1/28552576. Acesso em: 07 jul. 2023.

ZITTRAIN, Jonathan L.; MATTHEW G. Olsen; O'BRIEN, David; SCHNEIER, Bruce. Don't Panic: Making Progress on the “Going Dark Debate." Berkman Center Research Publication 2016-1. Tradução Gabriela Baptista. Disponível em: https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf. Acesso em: 07 jul. 2023.