I ENCONTRO NACIONAL DE DIREITO DO FUTURO

DIREITO PENAL E PROCESSUAL PENAL II

D598
Direito Penal e Processual Penal II [Recurso eletrônico on-line] organização I Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: Karina da Hora Farias, Caio Augusto Souza Lara e Lucas Augusto Tomé Kannoa Vieira – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2024.

Inclui bibliografia
ISBN: 978-85-5505-953-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os desafios do humanismo na era digital.
1. Direito do Futuro. 2. Humanismo. 3. Era digital. I. I Encontro Nacional de Direito do Futuro (1:2024 : Belo Horizonte, MG).

CDU: 34

I ENCONTRO NACIONAL DE DIREITO DO FUTURO

DIREITO PENAL E PROCESSUAL PENAL II

Apresentação

O Encontro Nacional de Direito do Futuro, realizado nos dias 20 e 21 de junho de 2024 em formato híbrido, constitui-se, já em sua primeira edição, como um dos maiores eventos científicos de Direito do Brasil. O evento gerou números impressionantes: 374 pesquisas aprovadas, que foram produzidas por 502 pesquisadores. Além do Distrito Federal, 19 estados da federação brasileira estiveram representados, quais sejam, Amazonas, Amapá, Bahia, Ceará, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Paraíba, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Rio Grande do Sul, Santa Catarina, Sergipe, São Paulo e Tocantins.

A condução dos 29 grupos de trabalho do evento, que geraram uma coletânea de igual número de livros que ora são apresentados à comunidade científica nacional, contou com a valiosa colaboração de 69 professoras e professores universitários de todo o país. Esses livros são compostos pelos trabalhos que passaram pelo rigoroso processo double blind peer review (avaliação cega por pares) dentro da plataforma CONPEDI. A coletânea contém o que há de mais recente e relevante em termos de discussão acadêmica sobre as perspectivas dos principais ramos do Direito.

Tamanho sucesso não seria possível sem o apoio institucional de entidades como o Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), a Universidade do Estado do Amazonas (UEA), o Mestrado Profissional em Direito e Inovação da Universidade Católica de Pernambuco (PPGDI/UNICAP), o Programa RECAJ-UFMG – Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais, a Comissão de Direito e Inteligência Artificial da Ordem dos Advogados do Brasil – Seção Minas Gerais, o Grupo de Pesquisa em Direito, Políticas Públicas e Tecnologia Digital da Faculdade de Direito de Franca e as entidades estudantis da UFMG: o Centro Acadêmico Afonso Pena (CAAP) e o Centro Acadêmico de Ciências do Estado (CACE).

Os painéis temáticos do congresso contaram com a presença de renomados especialistas do Direito nacional. A abertura foi realizada pelo professor Edgar Gastón Jacobs Flores Filho e pela professora Lorena Muniz de Castro e Lage, que discorreram sobre o tema “Educação jurídica do futuro”. O professor Caio Lara conduziu o debate. No segundo e derradeiro dia, no painel “O Judiciário e a Advocacia do futuro”, participaram o juiz Rodrigo Martins Faria,

os servidores do TJMG Priscila Sousa e Guilherme Chiodi, além da advogada e professora Camila Soares. O debate contou com a mediação da professora Helen Cristina de Almeida Silva. Houve, ainda, no encerramento, a emocionante apresentação da pesquisa intitulada "Construindo um ambiente de saúde acessível: abordagens para respeitar os direitos dos pacientes surdos no futuro", que foi realizada pelo graduando Gabriel Otávio Rocha Benfica em Linguagem Brasileira de Sinais (LIBRAS). Ele foi auxiliado por seus intérpretes Beatriz Diniz e Daniel Nonato.

A coletânea produzida a partir do evento e que agora é tornada pública tem um inegável valor científico. Seu objetivo é contribuir para a ciência jurídica e promover o aprofundamento da relação entre graduação e pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Além disso, busca-se formar novos pesquisadores nas mais diversas áreas do Direito, considerando a participação expressiva de estudantes de graduação nas atividades.

A Escola Superior Dom Helder Câmara, promotora desse evento que entra definitivamente no calendário científico nacional, é ligada à Rede Internacional de Educação dos Jesuítas, da Companhia de Jesus – Ordem Religiosa da Igreja Católica, fundada por Santo Inácio de Loyola em 1540. Atualmente, tal rede tem aproximadamente três milhões de estudantes, com 2.700 escolas, 850 colégios e 209 universidades presentes em todos os continentes. Mantida pela Fundação Movimento Direito e Cidadania e criada em 1998, a Dom Helder dá continuidade a uma prática ético-social, por meio de atividades de promoção humana, da defesa dos direitos fundamentais, da construção feliz e esperançosa de uma cultura da paz e da justiça.

A Dom Helder mantém um consolidado Programa de Pós-graduação Stricto Sensu em Direito Ambiental e Sustentabilidade, que é referência no país, com entradas nos níveis de mestrado, doutorado e pós-doutorado. Mantém revistas científicas, como a Veredas do Direito (Qualis A1), focada em Direito Ambiental, e a Dom Helder Revista de Direito, que recentemente recebeu o conceito Qualis A3.

Expressamos nossos agradecimentos a todos os pesquisadores por sua inestimável contribuição e desejamos a todos uma leitura excelente e proveitosa!

Belo Horizonte-MG, 29 de julho de 2024.

Prof. Dr. Paulo Umberto Stumpf – Reitor da ESDHC

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação da ESDHC

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa da ESDHC

MALWARES: OS LIMITES DO USO DE NOVAS TECNOLOGIAS POR AGENTES PÚBLICOS EM INVESTIGAÇÕES CRIMINAIS EM FACE AOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS.

MALWARE: THE LIMITS OF THE USE OF NEW TECHNOLOGIES BY PUBLIC AGENTS IN CRIMINAL INVESTIGATIONS IN THE FACE OF CONSTITUTIONAL PRINCIPLES AND GUARANTEES.

Alan Stafforti
Juliana Oliveira Sobieski

Resumo

A pesquisa aborda o impacto dos avanços tecnológicos na aquisição de informações, destacando a crescente utilização de malwares em investigações criminais no Brasil. O estudo analisa a viabilidade do uso de malwares para obtenção de provas, frente aos princípios e garantias constitucionais, Código Penal, Lei nº 12.850/2013 e a LGPD de Dados, examinando quanto à adequação e necessidade de regulamentação específica para malwares. Discute-se a tensão entre a eficácia e a proteção dos direitos fundamentais, propondo um marco regulatório. A conclusão ressalta a urgência de regulamentar do tema, visando proteger a privacidade e garantir a legalidade das investigações criminais.

Palavras-chave: Malwares, Agentes infiltrados, Direitos fundamentais, Lgpd, Regulamentação

Abstract/Resumen/Résumé

The research addresses the impact of technological advances on information acquisition, highlighting the growing use of malware in criminal investigations in Brazil. The study analyzes the feasibility of using malware to obtain evidence, in view of the constitutional principles and guarantees, the Penal Code, Law No. 12,850/2013 and the LGPD of Data, examining the adequacy and need for specific regulation for malware. The tension between the effectiveness and protection of fundamental rights is discussed, and a regulatory framework is proposed. The conclusion highlights the urgency of regulating the issue, order to protect privacy and ensure the legality of criminal investigations.

Keywords/Palabras-claves/Mots-clés: Malwares, Infiltrated agents, Fundamental rights, Lgpd, Regulation

1 INTRODUÇÃO

A evolução tecnológica tem tornado a aquisição de informações mais rápida e conveniente no mundo moderno, dados importantes são armazenados digitalmente, com uma crescente tendência de computação e armazenamento em soluções de *cloud computing*[1] *& storage*, essas mudanças trazem benefícios de praticidade, acessibilidade e disponibilidade à sociedade, mas, também, introduz novos riscos que podem afetar negativamente a reputação de pessoas e organizações. A falta de atenção à cibersegurança pode resultar em danos irreversíveis.

O avanço tecnológico e a difusão da internet e novas tecnologias para quase a totalidade das pessoas, influenciam e continuam a promover, em certa medida, a atividade criminosa, surgindo delitos exclusivamente virtuais e, quando não, utilizando a rede para facilitação do cometimento de infrações que não se restringem ao ambiente virtual.

Neste cenário, a presente pesquisa se propõe a analisar a viabilidade do uso de agentes infiltrados digitais, através de *softwares* espiões, no contexto de obtenção de prova de materialidade e autoria de delitos em investigações criminais, levando-se em conta os direitos constitucionais objetivos e subjetivos de cada indivíduo. Tendo como objetivo geral investigar a viabilidade de utilizar *malwares* em operações de investigação no Brasil, avaliando as práticas atuais em termos de eficácia, legalidade e identificar os limites entre o uso legítimo e o abuso dessas tecnologias. Questionando em que medida provas colhidas por meio de *malwares* por agentes públicos são lícitas. Qual é o limite claro da lei autorizando os órgãos de investigação em colher provas através da utilização destes *softwares* na fase investigativa? Esta é a pergunta nevrálgica que guia a presente pesquisa, pois tem-se o dever de proteção dos dados em suas dimensões subjetivas e objetivas.

Na perspectiva dos autores, este elevado percentual de invasão à privacidade, à inviolabilidade e o sigilo das comunicações, bem como a ausência de parâmetros específicos para utilização desses agentes, suscita múltiplas críticas à utilização de *malwares*, os quais são frequentemente classificados como uma forma de *Blackhat hacking* ou *cracking*[2] que por vezes tais indivíduos são patrocinados pelo Estado na ânsia acusatória vivenciada.

Questiona-se, ainda, se a legislação atual sobre os meios de obtenção de prova é adequada, ou se a implementação de *malwares* como ferramenta investigativa requer a criação

[1] Computação e armazenamento na nuvem.
[2] Interpreta-se: hackear para fins perversos, egoístas ou para atender os interesses de terceiros.

de um marco regulatório específico. Para abordar estas questões, inicialmente, define-se o conceito de *malware* e examina-se seu impacto sobre os direitos e garantias constitucionais previstos na CF/88 e, em seguida, com enfoque na legislação vigente relativa aos meios de obtenção de prova, incluindo disposições do Código Penal e da Lei 12.850/2013, bem como da ADPF[3], tombada perante o Supremo Tribunal Federal sob nº: 0091455-54.2023.1.00.0000, de relatoria do Ministro Cristiano Zanin e a LGPD - Lei Geral de Proteção de Dados.

Este trabalho foi desenvolvido através de pesquisas bibliográficas através de livros e artigos que tratam sobre o assunto, com o objetivo de apresentar à importância de entender o que são os *malwares* e seus impactos na obtenção de provas na esfera penal.

Por fim, propõem-se analisar o dever de proteção dos dados, frente as garantias fundamentais e a proporcionalidade dos direitos fundamentais em um Estado Democrático de Direito em enfrentar o *cibercrime* e obviamente os métodos utilizados no combate dos mesmos e o quão pode ser invasivo frente aos ditames constitucionais, com interações instantâneas e a todo momento, urge a necessidade de desenvolver um marco regulatório robusto que regulamente o uso de *malwares* nas investigações penais no Brasil.

2 DESENVOLVIMENTO DA PESQUISA

2.1. O que são *Malwares*? Seu uso é devidamente amparado pela legislação brasileira?

A terminologia *"malwar*e" origina-se da junção do prefixo, adjetivo, *mal-* sob o significado de "malicioso" com o sufixo, substantivo, *-ware*, sob o significado "software". O conceito de *malware* designa uma categoria específica de *softwares* que, ao serem clandestinamente instalados em dispositivos eletrônicos, conferem a terceiros - não autorizados, o acesso oculto e controle à informações e dados ali armazenados ou em processo de manipulação, de forma instantânea.

Neste contexto, tem-se como extrema relevância refletir sobre a (im) possibilidade de uso dessa intrusão virtual remota como meio de obtenção/captação de prova em procedimentos criminais no âmbito do direito brasileiro, especialmente para coletar dados para se chegar à materialidade e autoria dos delitos. Essa invasão permite ao *cracker* sob a execução de um *malware* acessar dados armazenados ou em processamento e manipular várias funcionalidades do sistema operacional em questão, esses programas exploram vulnerabilidades para estabelecer uma "*backdoor*[4]", ou porta de acesso remoto, que facilita o controle invisível do sistema. (RAMOS, 2019).

[3] Ação de Arguição de Preceito Fundamental.
[4] Tal espécie de *malware*, ganha o nome de *Cavalo de Tróia* ou *Trojan*.

Para Ossani Bezerra Pinho Filho, há uma conciliação, pelo Estado, na prevenção da criminalidade e repressão mais eficiente, com respeito aos direitos humanos, sempre foi um discurso que se almejava com o modelo de Política Criminal, argumentando que a pós-modernidade gera com seus paradigmas uma recorrente atualização do controle social, através da formação de uma sociedade de risco e do direito penal em si, com uma visão sistêmica e harmônica do ordenamento jurídico (2022).

Embora ainda não haja legislação específica no Brasil - em que pese uma eventual *LGPD penal,* disciplinando a natureza jurídica de *malware*, suas distintas espécies, trazendo procedimentos, aplicabilidade, sanções e penas para a sua aplicação, no ordenamento jurídico Pátrio, tem-se no Código Penal o crime de invasão de dispositivo eletrônico; informático; nos termos do Artigo 154-A, outra norma é a Lei Federal 12.850/2013, que trata sobre organizações criminosas a qual tem em seu bojo alguns meios de obtenção de provas, mais precisamente em seu artigo 10 ao 14, trazendo a figura do agente infiltrado digital, pelo fato de agir em um ambiente virtual, guardaria mais semelhança de uma autorização legal para uso dos *malwares*, com a devida autorização judicial, ante o preenchimento de todos os requisitos trazidos pela norma, e sendo o *malware* uma técnica invasiva não se poderia aplicar em um conceito amplo de infiltração (RIBEIRO; CORDEIRO; FUMACH, 2022).

Para Eduardo Riboli (2019), a potencialidade lesiva da utilização de *softwares* de espionagem aliada a uma ausência de regulamentação específica é impeditiva como meio de obtenção de provas, oportunidade na qual deveria ser proibida a sua utilização. Alicerça-se seu entendimento sobre duas premissas: (i) há outros meios de obtenção de provas representando uma grave ameaça a privacidade; capaz de interferir nas liberdades individuais dos indivíduos; (ii) a inexistência de normas disciplinando o uso e os limites para tanto, não sendo disposto um modo de execução com o tratamento dos dados, isto é, para que finalidade tais dados foram coletados e armazenados.

Nessa perspectiva, a utilização de *malwares* em dispositivos eletrônicos de terceiros, sem sua ciência e sua anuência, pode ser compreendido como ato ilegal, uma vez que inexiste regulamentação legal específica para o seu uso e os limites de sua operacionalização.

2.2. A violação do artigo 5º, X, CF/88 e princípios constitucionais em face de abusos perpetrados por *malwares.*

À luz das inovações tecnológicas, a sociedade contemporânea tem experimentado transformações significativas em diversas e múltiplas esferas e camadas. A Constituição

Federal de 1988 foi além e trouxe em sua redação a previsão ao direito à privacidade como uma garantia fundamental do indivíduo, dispondo em seu art. 5º, X que *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"* [5].

O uso excepcional de *malwares*, em investigações criminais, tem o potencial de comprometer o núcleo[6] essencial de direitos fundamentais garantidos pela Constituição Federal. O excesso da captura ou coleta de dados por agentes públicos podem constituir evidente violação à intimidade, à vida privada, à honra e à imagem do cidadão (art. 5º, X); também podendo ferir a inviolabilidade do domicílio (art. 5º, XI) e o sigilo das comunicações telemáticas (art. 5º, XII). Isso ocorre porque tais *softwares maliciosos,* permitem o acesso a uma grande variedade e volume de dados .Tornando-se ainda mais perigosos caso ativem a *webcam* e o microfone dos dispositivos eletrônicos, permitindo a captação de imagens e sons de locais privados e, em tese, íntimos. Além disso, se associados a tecnologias de geolocalização, possibilitam o monitoramento contínuo do indivíduo (RORIZ, 2022 p. 15-16).

Neste contexto, ao reconhecer o direito à privacidade é essencial refletir sobre a eficácia prática desta previsão constitucional em investigações criminais, o ordenamento jurídico brasileiro preocupou-se em criar um espaço civil para o bom uso na rede. Trata-se em essência de proteger a inviolabilidade das comunicações privadas no meio digital, na internet, em que pese que foi editada a Lei 12.965, de 23 de abril de 2014, popularmente conhecido como o Marco Civil da Internet (MCI) brasileiro; Esta lei estabeleceu os princípios a proteção da privacidade e dos dados pessoais (art. 3º, II e III), bem como a inviolabilidade da intimidade, da vida privada, do sigilo de comunicações na internet, das comunicações privadas armazenadas (art. 7º, I, II e III), e a proteção dos registros de conexão e de acesso a aplicações de internet (arts. 7º, VII, 10 e 11), (ADO, 2024).

A garantia dos direitos fundamentais são afirmativas que legitimam o poder exigido nas ações e práticas do Estado, buscando efetivar uma proteção eficiente dos direitos fundamentais. Mostra-se como uma ideia franqueada pelo princípio da proporcionalidade (MORAES, 2020). A intervenção estatal esta pautada em garantias das normas constitucionalmente previstas, sempre franqueando a sua atuação frente à proporcionalidade, ou seja, de maneira simplificada, a intervenção estatal deve ser mínima, somente quando necessáro.

[5] Constituição Federal de 1988.

[6] Teoria criada pelo Ministro Barroso –"[...] A dignidade humana é parte do núcleo essencial dos direitos fundamentais, como a igualdade, a liberdade ou a privacidade. Sendo assim, ela vai necessariamente informar a interpretação de tais direitos constitucionais, ajudando a definir o seu sentido nos casos concretos." (p.23)

O recente caso do *software* PEGASUS representa uma das maiores demonstrações de violação dos direitos fundamentais dos brasileiros. Trata-se de um *spyware* desenvolvido pela empresa israelense de armas cibernéticas NSO Group, que pode ser instalado secretamente em dispositivos eletrônicos, como *smartphones*, *tablets*, *wearables* e outros dispositivos como sistemas operacionais para *smartphones* Android e Ios, não só permite o monitoramento de todas as comunicações de um *smartphone*, mas também possibilita o rastreamento de chamadas telefônicas e localização, um dispositivo de vigilância constante, traduzindo-se em uma vigilância governamental totalmente invasiva, ilegal e inconstitucional, um *ius puniendi et extra,* isto é, um direito de punir exacerbado por parte do Estado.

Sem embargos, a proteção dos Direitos Fundamentais deve ser entendida como um elemento essencial do Constitucionalismo, que visa garantir a efetividade desses direitos, sob pena do exercício da jurisdição constitucional ser articulada como instância asseguradora de tais direitos (MORAIS, 2020).

2.3. Lei Geral de Proteção de Dados frente aos abusos de *Malwares.*

Com o crescimento e a evolução da sociedade brasileira, em 2024, com 203 milhões de indivíduos (CENSO, 2022), observa-se um potencial aumento de cibercrimes. Diante deste cenário, o *malware* também passou a ser visto como um potencial meio de obtenção de provas em processos penais, servindo como uma ferramenta útil para as autoridades competentes na repressão e prevenção de crimes. Em tempo, ressalta-se que, *malwares*, por sua natureza, atuam de maneira invisível ao usuário-vítima, de forma oculta e via de regra sem qualquer evidência de sua existência ao cidadão em seu dispositivo eletrônico. O uso de *malware* cria uma antinomia constitucional-legal entre os direitos fundamentais do indivíduo e a LGPD em face dos princípios de investigação e a prevenção criminal.

A LGPD tem como principal objetivo proteger os dados pessoais e sensíveis do indivíduo, introduzindo importantes regras e diretrizes para a coleta, armazenamento e uso adequado em fase de tratamento dos dados pessoais da população no Brasil, não apenas aumentando a transparência, mas reforçando a cibersegurança e a privacidade no tratamento de dados pessoais, oferecendo diretrizes para identificar os possíveis responsáveis pelos crimes cometidos por agentes infiltrados via crimes cibernéticos (SILVA, NOVAIS, 2023).

Segundo Morais, a proteção dos dados pessoais como direito fundamental e a sua distinção como direito autônomo, está o papel do Estado pelo seu dever de proteção, zelar

ativamente, pela consistência e efetividade não só da LGPD mas de todas as normas e leis vigentes no Brasil que dizem respeito a proteção dos dados pessoais (MORAIS, 2020).

Sob uma perspectiva processual penal o professor Aury Lopes Júnior em sua obra "Direito Processual Penal" (p. 116) menciona que o princípio do *nemo tenetur se detegere* e a manifestação de uma garantia segundo o qual o sujeito passivo não pode sofrer nenhum prejuízo por omitir-se de colaborar em uma atividade probatória da acusação ou por exercer seu direito seu direito ao silêncio. O autor é imperioso ao indicar que esse direito está sob risco de constrições indevidas devido à nível de invasão dos *softwares maliciosos*, que permitem o monitoramento audiovisual de condutas realizadas nos ambientes de maior intimidade do indivíduo, onde ele tem uma real expectativa de não estar sendo visto ou ouvido. Dessa forma, como o emprego desse meio investigativo não é do conhecimento do investigado, questiona-se se, em tais circunstâncias, uma declaração auto incriminadora poderia ser admitida e valorada em seu desfavor.

3 CONSIDERAÇÕES FINAIS

A presente pesquisa faz parte de um trabalho em andamento cujo objetivo é conscientizar sobre a existência de *malwares* que quando utilizados por agentes infiltrados em investigações criminais como meio de obter provas, afrontam e violam gravemente nossos direitos e garantias fundamentais, geralmente essas investigações ocorrem sem autorização judicial.

Ao longo da pesquisa realizada, torna-se evidente a urgência que o Brasil possui em criar um espaço de forte de regulamentação sobre estas medidas, estabelecendo diretrizes provisórias para a proteção dos direitos fundamentais à intimidade, à privacidade e à inviolabilidade do sigilo das comunicações pessoais e dos dados e a operacionalização do sistema, até que a lacuna normativa inconstitucional seja corrigida. Assim, os usuários terão conhecimento sobre as nocivas aplicações em investigações e que medidas em termos de regulação precisam ser tomadas.

Portanto, ao regulamentar o uso de *malwares* por agentes públicos e reforçar as penalidades para o uso não autorizado dessas ferramentas, o Brasil estará dando um passo importante na proteção dos direitos fundamentais e na promoção de um sistema de justiça mais seguro e eficiente.

4 REFERÊNCIAS BIBLIOGRÁFICAS.

ADO. **AÇÃO DIRETA DE INCONSTITUCIONALIDADE POR OMISSÃO.** Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6816879**.** Acessado em 08 de Maio de 2024.

BARROSO, Luis Roberto. **"Aqui, Lá e em todo Lugar ": A Dignidade Humana no Direito Contemporâneo e no Discurso Transnacional.** Revista do Ministério Público. Rio de Janeiro: MPRJ, n. 50, out./ dez. 2013.

GONÇALVES NOVAIS, COUTO DA SILVA Thyara, Ronaldo**. A Lei Geral de Proteção de Dados e sua Aplicação no combate aos crimes cibernéticos: Desafios e Perspectivas.** 2023. Revista Ibero- Americana de Humanidades, Ciências e Educação- REASE. São Paulo, v.9.n.10. out. 2023. ISSN - 2675 – 3375. doi.org/10.51891/rease.v9i10.12254.

LOPES JR., Aury. **Direito Processual Penal** – 18. Ed. – São Paulo: Saraiva Educação, 2021. ISBN 978-65-5559-008-1

MORAIS, Fausto Santos (org). **Dever de Proteção, Direitos Fundamentais e Argumentação Jurídica**: Volume I / Fausto Santos de Morais. – Passo Fundo: Conhecer, 2020. ISBN: 978-65-992708-2-6.

PINHO FILHO, Ossani Bezerra. **Investigação criminal tecnológica: infiltração por *malware* nas investigações informáticas**./ Ossani Bezerra Pinho Filho./ Curitiba: Juruá, 2022.

RODRIGUES RORIZ, Laura. **OS LIMITES DA VIGILÂNCIA ESTATAL IMPOSTOS PELA PRIVACIDADE: O caso do sistema Pegasus -** Universidade Brasília Faculdade de Direito, Brasília, 2022.

RAMOS, Ricardo da Costa. **A importância e os processos de análise de malware em um incidente de segurança.** 2019. Trabalho de Conclusão de Curso (Tecnólogo em Sistemas de Computação) – Curso de Tecnologia em Sistemas de Computação, Universidade Federal Fluminense, Niterói, 2019.

RIBEIRO, Gustavo Alves Magalhães. CORDEIRO, Pedro Ivo Rodrigues Velloso. **O *malware* como meio de obtenção de prova e sua implementação no ordenamento jurídico brasileiro**. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 8, n. 3, p. 1463-1500, setembro-dezembro de 2022.

RIBOLI, Eduardo Bolsoni. "**Eu sei o que vocês fizeram no verão passado": O uso de software de espionagem como meio de obtenção de prova penal.** Revista Brasileira de Ciências Criminais, vol. 156/2019, Junho de 2019, página 1-35.