XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

LUIZ GUSTAVO GONÇALVES RIBEIRO

ANTONIO CARLOS DA PONTE

D597
DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I
[Recurso eletrônico on-line] organização CONPEDI
Coordenadores: Luiz Gustavo Gonçalves Ribeiro, Antonio Carlos da Ponte – Florianópolis: CONPEDI, 2024.
Inclui bibliografia
ISBN: 978-85-5505-968-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: ESTADO DE DERECHO, INVESTIGACIÓN JURÍDICA E INNOVACIÓN
1. Direito – Estudo e ensino (Pós-graduação) – 2. Direito penal. 3. Processo penal. XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU (2: 2024 : Florianópolis, Brasil).
CDU: 34

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

XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

Apresentação

Durante uma tarde aprazível da primavera Uruguaia, nas dependências da Universidad de la Republica do Uruguay, no âmbito do Grupo de Trabalho intitulado Direito Penal, Processo Penal e Criminologia I, foram encetados e desenvolvidos debates que tiveram por escopo a discussão de questões contemporâneas e bastante ecléticas versando sobre as ciências penais.

As apresentações foram realizadas em um só bloco de exposições, havendo, pelos(as) autores (as) presentes, a apresentação dos respectivos artigos aprovados em sequência. Ao término das exposições, foi aberto espaço para a realização do debate, que se realizou de forma profícua.

Segue, abaixo, a descrição e síntese dos artigos apresentados:

O primeiro artigo, intitulado “Análise da geração ‘nem nem’ no Brasil à luz do direito à educação: juventude, exclusão e implicações do direito penal”, dos autores Luiz Gustavo Gonçalves Ribeiro, Hercules Evaristo Avancini e Isabela Moreira Silva, resulta de um estudo que associa e analisa o Direito à Educação e uma parcela significativa da população brasileira a que se convencionou chamar de “Geração Nem Nem”, constituída de 10,9 milhões de pessoas segundo o IBGE. Embora diversa em seu interior, em termos socioeconômicos e étnicos encontra semelhanças em virtude de viverem na condição de não estudarem e de não trabalharem, mesmo em idade ativa. O objetivo deste artigo é o de analisar as informações relevantes acerca da GNN e de refletir sobre a complexidade do contexto socioeconômico, com destaque às questões educacionais, além de colaborar na compreensão de sua relação com a manutenção do distanciamento do direito à educação e ao trabalho. No tocante ao aspecto penal, propõe-se uma reflexão construída no campo da análise criminológica que associa os direitos não exercidos pela GNN e a consequente ampliação da condição de vulnerabilidades sociais que exortam atividades ilícitas e marcam o aprofundamento da exclusão social, apontando para a necessidade de se repensar políticas públicas com o escopo de diminuir a incidência de jovens no submundo do crime. O desenvolvimento deste estudo apoiou-se na investigação e na revisão bibliográfica, também nos dados da Síntese de Indicadores Sociais do IBGE 2023, no Índice de Desenvolvimento da Educação Básica do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira e na Constituição Federal Brasileira adotando o método crítico-reflexivo. A utilização de informações

quantitativas, geradas pelo IBGE e pelo INEP, geraram o suporte para as abordagens qualitativas.

O próximo artigo, cujo título é “Gestão integrada da segurança pública e da paisagem urbana”, dos autores Rodrigo Sant´Ana Nogueira e Rodrigo de Paula Zardini, tem como pressuposto fundamental analisar quatro eixos basilares para compreensão da relação entre o crime patrimonial (furto e roubo) e o meio ambiente. O primeiro elemento é a prevenção geral e abstrata composta pelo imperativo axiológico social e estatal que visa mitigar o desencadeamento do fato social considerado como crime. O segundo elemento é o papel do Poder Judiciário na materialização controle social proporcionando a percepção de segurança. O terceiro elemento é a compreensão da dinâmica territorial do crime face ao vazio intermitente das limitações sociais impostas pela sociedade ou pelo próprio Estado. O quarto elemento é composto por um silogismo social, qual seja, que não há espaço defensável, pois o Poder Judiciário, como instituição estatal de controle social é ausente e ineficaz nas periferias urbanas, sendo este o cinismo social evidente nas relações crime/efetiva punição e ressocialização do indivíduo. Face ao exposto, o objetivo geral do trabalho é avaliar os mapas de calor de criminalidade em um modelo de dinâmica mecânica e linear, pois, nesse sentido, se estratifica um determinado ponto de equilíbrio para projeção da paisagem segura, ou, numa segunda perspectiva, a criminologia ambiental seria um modelo líquido e caótico, que não seria possível determinar uma constante de equilíbrio.

O artigo seguinte tem por título “Informação criminal oficial, mortes violentas intencionais e elucidações dos crimes: uma história sobra a construção do sistema nacional de estatísticas criminais no Brasil”, de autoria de Cassandra Maria Duarte Guimarães, Ana Luisa Celino Coutinho e Gustavo Barbosa de Mesquita Batista. O trabalho tem por objeto de estudo a construção do sistema de informação criminal oficial, acompanhando a quantificação da incidência das mortes violentas intencionais, buscando responder a seguinte questão: as informações criminais oficiais advindas da segurança pública sempre foram validadas e usadas no Brasil? Supõe-se que o uso atual da contabilidade oficial criminal é recente, assim como sua correlação com o sistema de segurança e justiça criminal e com a persecução penal no país, uma vez que a coleta e o tratamento dessas informações até bem pouco tempo eram sinalizados pelas lacunas e imprecisões de um sistema uniformizado que contemplasse todas os Estados e o Governo Federal. A pesquisa torna-se relevante ao se observar que o cômputo oficial criminal no Brasil é reflexo da estrutura constitucional do sistema de persecução penal, que tem por locus inicial as instituições policiais da segurança pública, de onde também se origina a coleta inicial dos dados criminais no país. A análise foi realizada mediante uma abordagem qualitativa sobre a quantificação oficial dos crimes, especialmente tratando as mortes violentas intencionais, valendo-se dos procedimentos histórico e

estatístico, bem como de técnicas de pesquisas bibliográfica e documental, quanto às publicações sobre as estatísticas criminais no país, detendo-se principalmente nas legislações sobre a atual política de informação oficial e segurança pública que, mesmo com os avanços alcançados, ainda apresenta ausência de dados e análises sobre as elucidações dos crimes.

O próximo texto, intitulado “Juvenicídio e feminicídio: vulnerabilidades entrelaçadas”, dos autores Thayane Pereira Angnes e Ana Paula Motta Costa, propõe uma análise das correlações entre juvenicídio e feminicídio, destacando a relevância como categorias-chave na compreensão dos problemas sociais, especialmente no contexto da violência enfrentada por adolescentes e pelas mulheres. O propósito do trabalho é aliar os estudos de juventude e gênero, explorando as proximidades dos conceitos, e como estes se entrelaçam, culminando em processos geradores de vidas descartáveis e passíveis de violência letal. Metodologicamente, este estudo baseia-se em uma análise teórica e de revisão bibliográfica. Inicialmente, são delineados os conceitos de juvenicídio e feminicídio como expressões emblemáticas de precarização e morte. Em seguida, são discutidas as interconexões e repercussões destes processos na sociedade. O estudo conclui que além de conexos, o feminicídio é um dos principais catalisadores do juvenicídio, o que é visível quando se observa submissão histórica das mulheres pelo patriarcado misógino, que impacta diretamente nas trajetórias de vida de jovens meninas, resultando em violência, precariedade e morte.

O trabalho seguinte, que tem por título “Lei n. 14843/2024: a restrição das saídas temporárias e os impactos ao processo de execução penal brasileira”, dos autores Luiz Fernando Kazmierczak e Vinicius Hiudy Okada, dispõe que a lei referida alterou a Lei de Execução Penal para dispor sobre a monitoração eletrônica do preso, prever a realização de exame criminológico para progressão de regime e restringir o benefício da saída temporária. A Anacrim e o CFOAB apresentaram ADIs contra a lei perante o STF, sustentando que a alteração legislativa viola valores fundamentais da CF/88 e prejudica a ressocialização do condenado. A pesquisa objetivou investigar os impactos trazidos pela Lei nº 14.843/2024 em relação ao processo e execução penal nacional, buscando-se responder questões como: a) “de que modo as restrições às saídas temporárias podem prejudicar os direitos fundamentais dos condenados?”; e b) “qual a importância do STF nesses casos?”. Utilizou-se para a confecção o método dedutivo – junto à análise de artigos científicos, doutrinas, legislações e reportagens de repercussão nacional –, partindo-se da premissa de que as alterações trazidas pela Lei nº 14.843/2024 trarão impactos não apenas ao processo e à execução penal, mas também à segurança pública nacional. Com todo o exposto, concluiu-se que as alterações trazidas pela lei prejudicarão – e muito – o processo e a execução penal brasileira, podendo, além de lesionar direitos fundamentais previstos constitucionalmente, colocar em risco a

segurança pública nacional, através de institucionalização prisional e rebeliões. Pôde-se perceber a extrema importância do STF nesses casos, a começar pela decisão certeira do ministro André Mendonça, ao manter a saída temporária ao preso beneficiado antes da Lei nº 14.843/2024.

O próximo artigo, de nome "Machado de Assis e seletividade penal: a obra machadiana que revela o autoritarismo do aparato repressivo estatal e do sistema de justiça criminal", de autoria de Léo Santos Bastos, visa responder como a obra de Machado de Assis e, mais especificamente, o conto Pai Contra Mãe exploram e expõem o racismo estrutural da sociedade brasileira, demonstrando as influências da colonização, da escravidão e do autoritarismo na seletividade do sistema de justiça criminal. Em vista disso, a partir do marco teórico da criminologia crítica, nos diálogos entre direito e literatura, buscou-se compreender os elementos antidemocráticos que contribuíram para a exclusão e marginalização de pessoas negras, por meio de políticas de morte e prisão. A partir da obra machadiana, pode-se compreender as desigualdades sociais e raciais que estruturam a sociedade brasileira, bem como formas e ações de participação popular que contribuem para a defesa e proteção de um Estado de bem-estar social que contenha o poder punitivo do Estado policial máximo. O artigo se insere no campo das reflexões interdisciplinares, procurando analisar o sistema de justiça criminal contemporâneo concomitantemente com os campos da literatura, da sociologia e da filosofia. A pesquisa se apropria de uma obra literária para examinar o estado da arte das relações raciais, sociais e institucionais brasileiras.

O texto seguinte, intitulado "Malwares: os limites do uso de novas tecnologias por agentes públicos em investigações criminais em face aos princípios e garantias constitucionais", de Fausto Santos de Morais, Alan Stafforti e Juliana Oliveira Sobieski, tem o condão de abordar o impacto dos avanços tecnológicos na pesquisa e na aquisição de informações envolvendo a cibersegurança, destacando, principalmente, a crescente utilização de malware por agentes infiltrados digitais nas investigações criminais no Brasil. O estudo elaborado analisa a viabilidade legal do uso desse meio intrusivo para obtenção de elementos probatórios a fim de coletar dados para se chegar na autoria e materialidade de delitos, considerando os direitos e garantias constitucionais da privacidade e da proteção dos dados. A legislação brasileira atual, incluindo o Código Penal, a Lei 12.850/2013 (norma que rege as organizações criminosas, dispondo sobre a investigação e a obtenção de provas) e a Lei Geral de Proteção de Dados (LGPD), são examinadas quanto à adequação e a necessidade de uma regulamentação específica para o uso dos malwares. O trabalho discute a tensão entre a eficácia investigativa e a proteção dos direitos fundamentais, propondo a criação de um marco regulatório robusto para a obtenção, armazenamento e descarte dos dados coletados com a utilização do programa. A conclusão ressalta a urgência de regulamentar o uso de

malwares, visando proteger a privacidade e garantir a legalidade das investigações criminais, promovendo um sistema de justiça investigatório mais seguro e eficiente.

O texto seguinte, de nome “O controle dos corpos femininos através da manipulação de discursos religiosos”, dos autores Larissa Franco Vogt, Mariele Cássia Boschetti Dal Forno e Doglas Cesar Lucas, tem como objetivo principal analisar o discurso persuasivo de líderes religiosos e casos de abuso da fé ocorridos em momentos de vulnerabilidade feminina, quando as vítimas buscavam conforto, esperança e a cura por meio de sua crença religiosa. O problema de pesquisa centraliza-se na seguinte questão: por que a violência sexual cometida dentro de instituições religiosas ainda é tratada como tabu e silenciada? A pesquisa demonstra que boa parte das mulheres vítimas dos abusos sexuais se calam por receio, vergonha, insegurança, mas principalmente por não quererem acreditar que sua fé foi objeto de manipulação e instrumento de violação de seu corpo, outrossim, quando resolvem falar acabam por serem questionadas e desacreditadas pelos órgãos públicos e até mesmo pela comunidade onde vivem. Para isso, foi utilizada uma metodologia de abordagem hipotético-dedutiva, com a análise de artigos e estudos, considerando que as pesquisas sobre o tema ainda são escassas.

O próximo artigo tem por título “O direito penal ambiental brasileiro na efetivação dos objetivos do desenvolvimento sustentável (ODS) n. 13, 14 e 15”, e a autoria de Luiz Gustavo Gonçalves Ribeiro, Edimar Lúcio de Souza e Élica Viveiros. O texto tem como objetivo geral a análise de como o Direito Penal Ambiental brasileiro pode contribuir na efetivação dos ODS’s n. 13, 14 e 15. Utilizou-se das metodologias de revisão bibliográfica e de análise documental para fundamentar a pesquisa com resultados extraídos de estudos científicos, doutrinas, legislações e normas. Trata-se de uma pesquisa qualitativa, básica, descritiva e bibliográfica/documental. Os resultados encontrados evidenciam que os dispositivos do Direito Penal Ambiental são de grande valia para dispor de certo controle preventivo e punitivo para a satisfação dos ODS’s n. 13, 14 e 15 no Brasil. Em considerações finais, a pesquisa destaca que o Direito Penal Ambiental vale-se de subsídios constitucionais para atuar em favor do meio ambiente.

O artigo seguinte, denominado “O espaço dos maiores estabelecimentos penais no Brasil sob a ótica dos preceitos fundamentais do preso”, de Luciano Rostirolla, avalia o espaço dos maiores presídios do Brasil sob a ótica dos preceitos fundamentais estabelecidos da Lei de Execuções Penais e Constituição Federal. As metodologias empregadas para elaboração do trabalho de pesquisa são a estatística, a monográfica e a comparativa. Embora sediados no mesmo território nacional e regidos pelas mesmas normas, os estabelecimentos penais brasileiros apresentam divergências no tratamento de seus detentos e no cumprimento das

garantias constitucionais e direitos fundamentais do preso ou internado. No ano de 2022 o Brasil possuía aproximadamente 1.381 unidades prisionais em operação (DEPEN, 2023). Este estudo é desenvolvido por meio do método de análise de correspondência múltipla (ACM) e tem por objeto avaliar o espaço social dos maiores estabelecimentos do Brasil. Desse modo foram destacados os 214 maiores estabelecimentos, o que representa mais de 15% do total geral de presídios em operação. A pesquisa permitiu compreender algumas características dos estabelecimentos penais analisados e identificar algumas vantagens e falhas das unidades no tocante à estruturação física, garantia de direitos individuais, priorização da ressocialização por meio do estudo e trabalho dos detentos, com vistas ao seu desenvolvimento humano.

Em seguida, apresenta-se o artigo intitulado “O tempo como pena: desumanização e descaracterização da maternidade no cárcere feminino no Brasil”, escrito por Fernanda Analu Marcolla e Maiquel Ângelo Dezordi Wermuth. Nessa pesquisa, investiga-se o “tempo como pena” na medida em que o tempo de encarceramento afeta a capacidade das mulheres de exercerem a maternidade e criar vínculo com seus filhos dentro do sistema prisional brasileiro. O objetivo geral da pesquisa é analisar de que maneira o tempo de encarceramento impacta a capacidade das mulheres de exercerem a maternidade, com foco na desumanização e descaracterização da identidade materna, considerando as inadequações estruturais do sistema prisional e as necessidades específicas das mulheres em termos de saúde reprodutiva e direitos maternos. Utilizando o método hipotético-dedutivo, a pesquisa revela que o tempo de encarceramento afeta significativamente a capacidade das mulheres de exercerem a maternidade dentro do sistema prisional brasileiro. Este impacto negativo é agravado pela estrutura inadequada do sistema prisional, que não oferece condições apropriadas para a manutenção do vínculo materno-filial e desconsidera as necessidades específicas das mulheres em termos de saúde reprodutiva e direitos maternos. A pesquisa conclui que a prolongada duração das penas resulta na desumanização e descaracterização da identidade materna, sublinhando a necessidade urgente de revisar e humanizar as políticas penais para garantir que os direitos reprodutivos e maternos dessas mulheres sejam respeitados e protegidos.

O artigo seguinte tem por título “PEC 45/2023 e a Política de drogas no Brasil: uma análise comparativa com a legalização da maconha no Uruguai”, e foi escrito por Carla Bertoncini, Carla Graia Correia e Matheus Arcoleze Marelli. No texto desenvolve-se que, nos anseios da política de drogas a nível mundial, a relação fronteiriça entre Brasil e Uruguai também é abalada. Demonstra-se uma enorme diferença na conduta da guerra contra o narcotráfico, partindo da segurança pública às políticas públicas. Notória e incontroversa, a Lei nº 19.172 /2013 promulgada pelo então presidente do Uruguai, José “Pepe” Mujica, legalizou e

regulamentou toda a cadeia da cannabis em solo uruguaio. Por outro lado, a relação brasileira é controversa: enquanto o STF decide sobre descriminalização do porte de maconha para uso pessoal, o Poder Legislativo atua, em resposta, para criminalizar ao máximo o porte e a posse de entorpecentes. A apresentação de contrapontos, através do método dedutivo, bem como de alternativas e soluções, buscando sempre a análise da lei uruguaia e de sua aplicação em seus órgãos de regulamentação, é a marca de que o Brasil ainda tem muito a aprender com o progressismo aplicado nas políticas públicas de sua ex-província, afastando o punitivismo e a repressão.

O artigo seguinte tem por título "Racismo como produto do sistema penal: a seletividade inerente à criminalização secundária", dos autores Denner Murilo de Oliveira e Luiz Fernando Kazmierczak. Nele, destaca-se que, diante da desigualdade racial existente no plano social, a pesquisa tem como objetivo averiguar a reprodução do racismo pelo sistema penal brasileiro, abordando, a priori, as diferentes formas de racismo. O tema-problema do trabalho reside na seguinte indagação: Diante da representatividade de negros nas prisões, de que forma o sistema penal reproduz o racismo no Brasil? Para isso, realizou-se uma análise acerca do conceito de racismo institucional, racismo estrutural e racismo individualista, além da averiguação da relação entre racismo e direito. Além disso, observou-se dados referentes à população carcerária no território brasileiro, expondo o perfil dos apenados e evidenciando que há grande representatividade da população negra no cárcere brasileiro. Em seguida, utilizou-se dos objetos da criminologia crítica para compreender o sistema penal como reprodutor do racismo, sendo o marco teórico desta pesquisa a obra denominada "Criminologia Contribuição Para Crítica da Economia da Punição" de autoria de Juarez Cirino dos Santos. Por fim, a metodologia utilizada para o desenvolvimento da pesquisa é a dedutiva, partindo-se de um aspecto geral acerca do racismo e chegando ao campo particular do racismo reproduzido pelo sistema de justiça criminal e, ainda, expondo que a criminologia crítica pode ser aplicada para compreender a relação entre racismo e sistema penal.

O artigo seguinte, intitulado "Reconhecimento de pessoas nos crimes patrimoniais praticados mediante violência ou grave ameaça: análise dos julgados do Tribunal de Justiça do Estado da Bahia", dos autores Sebastian Borges de Albuquerque Mello e Beatriz Andrade Candeias, pretende analisar a adoção das regularidades legais e dos preceitos da psicologia do testemunho na produção do reconhecimento de pessoas, bem como a valoração deste elemento probatório nos processos penais tramitados na Bahia que versam sobre crimes patrimoniais praticados mediante violência ou grave ameaça. Questiona-se, assim, se os reconhecimentos de pessoas valorados pelo Tribunal de Justiça do Estado da Bahia são dotados de fiabilidade e se a Corte baiana adota o atual entendimento jurisprudencial do Superior Tribunal de Justiça sobre o tema. Desse modo, este trabalho realizou uma pesquisa

empírica, a partir da metodologia indutiva, com abordagem por amostragem de dados qualitativos e quantitativos oriundos de 163 (cento e sessenta e três) acórdãos do Tribunal de Justiça disponíveis no website "jurisprudência TJBA" no filtro dos meses de maio e junho do ano de 2021, a partir da busca pelas palavras-chave "roubo" e "157". Com isso, foi possível concluir que, na Bahia, a prática probatória do reconhecimento de pessoas tem como cunho a produção de variáveis sistêmicas e de estimação, ante a falta de acurácia dos atores de justiça sobre o funcionamento da memória, gerando alta probabilidade de produção de falsos reconhecimentos e, por consequência, elementos que não deveriam compor o acervo probatório da hipótese acusatória nas decisões da Corte baiana.

O próximo artigo, intitulado "Sistema de justiça criminal e a pandemia da Covid-19: um novo discurso jurídico-penal para legitimar velhas práticas punitivas", do autor Léo Santos Bastos, externa que, em vista da pandemia da COVID-19, o cenário global se modificou para promover a contenção da transmissão do vírus, especialmente por meio do isolamento social. Contudo, a partir do histórico punitivo do país que armazena a terceira maior população carcerária do mundo, buscou-se avaliar, pelas lentes da criminologia crítica, de que forma os julgadores e julgadoras do Tribunal de Justiça do Rio Grande do Sul interpretam os efeitos da crise sanitária e as medidas tomadas para seu enfrentamento no sistema de justiça criminal, que apontam para a manutenção do encarceramento, a desconsiderar as prescrições sanitárias de prevenção e, em última análise, a vida das pessoas privadas de liberdade. No presente artigo, foi possível averiguar e demonstrar que métodos de criminalização se estendem para as decisões judiciais a partir de discursos que julgam adequado o aprisionamento dos corpos em tempos de pandemia. Demonstrou-se ainda que as pessoas privadas de liberdade no Brasil compõem os mesmos grupos sociais excluídos em diferentes épocas. Por fim, examinou-se como a reiteração de discursos, decisões e práticas hegemônicas colabora com a perpetuação e manutenção do atual estado de coisas inconstitucional de nossas penitenciárias.

O próximo artigo tem por título "Teorias das penas e o descumprimento da função da pena no Brasil e a omissão estatal", e foi escrito por Carolline Leal Ribas, Renata Apolinário de Castro Lima e Roberto Apolinário de Castro. No texto, os autores analisam as modalidades de teorias da pena e o tipo de pena aplicado no ordenamento jurídico brasileiro. A pesquisa versa sobre a omissão estatal e o descumprimento da função da pena no sistema brasileiro, que adota a Teoria Mista. Aborda-se, também, temas-problemas do julgamento da arguição de descumprimento de preceito fundamental nº 347, do Supremo Tribunal Federal, que considerou a situação prisional no Brasil um "estado de coisas inconstitucional" com "violação massiva de direitos fundamentais" da população prisional, por omissão do poder público, conceituando-se assim como, "estado de coisas inconstitucional". Se trata de uma problemática atual e que possui relevância para a sociedade, em função do cenário ao qual

são submetidos os reclusos do sistema penitenciário brasileiro. O artigo procedeu a investigação científica empregando a metodologia consistente na pesquisa bibliográfica, utilizando-se do método dedutivo.

No artigo derradeiro, intitulado “Visão geral das decisões de cassação criminal sobre lavagem de dinheiro”, a autora Natalia Acosta examina os aspectos problemáticos dos crimes de lavagem de dinheiro levados à Suprema Corte de Justiça do Uruguai por meio de recursos de cassação. Inicialmente, o artigo apresenta o problema de pesquisa. Em seguida, por meio de uma metodologia de pesquisa jurídico-empírica, são abordadas as decisões de cassação sobre o assunto desde a promulgação da lei original até a presente data. No Uruguai, os crimes de lavagem de dinheiro são punidos desde 1998. Entretanto, os resultados são escassos. Por um lado, porque há poucas condenações e, por outro, porque, em geral, os casos não chegam à terceira instância. Foram encontradas sete sentenças, e todas elas têm em comum a relação problemática com as atividades criminosas anteriores, que, exceto em um caso, foram cometidas no exterior. No entanto, em todos os casos, sabia-se ou deveria saber-se que os recursos eram provenientes dessas atividades e essa conclusão foi alcançada por meio de provas circunstanciais.

Observa-se, portanto, que se tratam de trabalhos ecléticos e atuais e que, por certo, se lidos e compreendidos, oferecerão uma grande contribuição para o avanço das práticas e políticas necessárias para o aperfeiçoamento das ciências criminais no Brasil.

Por fim, nós, organizadores do livro, convidamos todos para uma leitura aprazível e crítica de todos os textos.

Montevidéu, primavera de 2024.

Professor Doutor Antônio Carlos da Ponte, Universidade Nove de Julho e Pontifícia Universidade Católica de São Paulo. acdaponte@uol.com.br

Professor Doutor Luiz Gustavo Gonçalves Ribeiro, Dom Helder-Escola Superior. lgribeirobh@gmail.com

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

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

Fausto Santos de Morais
Alan Stafforti
Juliana Oliveira Sobieski

Resumo

O trabalho tem o condão de abordar o impacto dos avanços tecnológicos na pesquisa e na aquisição de informações envolvendo a cibersegurança, destacando, principalmente, a crescente utilização de malware por agentes infiltrados digitais nas investigações criminais no Brasil. O estudo elaborado analisa a viabilidade legal do uso desse meio intrusivo para obtenção de elementos probatórios a fim de coletar dados para se chegar na autoria e materialidade de delitos, considerando os direitos e garantias constitucionais da privacidade e da proteção dos dados. A legislação brasileira atual, incluindo o Código Penal, a Lei 12.850 /2013 (norma que rege as organização criminosa, dispondo sobre a investigação e a obtenção de provas) e a Lei Geral de Proteção de Dados (LGPD), são examinadas quanto à adequação e a necessidade de uma regulamentação específica para o uso dos malwares. O trabalho discute a tensão entre a eficácia investigativa e a proteção dos direitos fundamentais, propondo a criação de um marco regulatório robusto para a obtenção, armazenamento e descarte dos dados coletados com a utilização do programa. A conclusão ressalta a urgência de regulamentar o uso de malwares, visando proteger a privacidade e garantir a legalidade das investigações criminais, promovendo um sistema de justiça investigatório mais seguro e eficiente.

Palavras-chave: Malwares, Agentes infiltrados digitais, Direitos e garantias fundamentais, Lei geral de proteção de dados, Regulamentação

Abstract/Resumen/Résumé

The work has the power to address the impact of technological advances on research and the acquisition of information involving cybersecurity, highlighting, mainly, the growing use of malware by digital infiltrators in criminal investigations in Brazil. The study analyzes the legal feasibility of using this intrusive means to obtain evidence in order to collect data to arrive at the authorship and materiality of crimes, considering the constitutional rights and guarantees of privacy and data protection. The current Brazilian legislation, including the Penal Code, Law 12.850/2013 (a rule that governs criminal organizations, providing for the investigation and obtaining of evidence) and the General Data Protection Law (LGPD), are

examined as to the adequacy and need for specific regulations for the use of malware. The paper discusses the tension between investigative effectiveness and the protection of fundamental rights, proposing the creation of a robust regulatory framework for obtaining, storing and disposing of data collected using the program. The conclusion underscores the urgency of regulating the use of malware, in order to protect privacy and ensure the legality of criminal investigations, promoting a safer and more efficient investigative justice system.

Keywords/Palabras-claves/Mots-clés: Malware, Digital undercover agents, Fundamental rights and guarantees, General data protection law, Regulation

1 INTRODUÇÃO

A evolução tecnológica tem tornado a aquisição de informações mais rápida e conveniente no mundo moderno. Antigamente, dados importantes, como transações financeiras, informações confidenciais e a comunicação realizada entre os indivíduos eram mantidos em papel.

Na atualidade, dados importantes são armazenados digitalmente, com uma crescente tendência de computação e armazenamento em soluções de *cloud computing & storage* (computação e armazenamento na nuvem), bem como a utilização dos mais diversos dispositivos eletrônicos com aplicativos de conversação, através de troca de mensagens de forma instantânea. Essas mudanças trazem benefícios de praticidade, acessibilidade e disponibilidade à sociedade, seguindo o avanço tecnológico em que vivemos, mas, também introduz novos riscos que podem afetar negativamente a reputação de pessoas e organizações – seus nomes e marcas, respectivamente – além de potencialmente comprometer a funcionalidade de dispositivos eletrônicos. A falta de atenção à cibersegurança pode resultar em danos irreversíveis.

Os reflexos dessa nova realidade têm se estendido pelos mais diversos ramos do Direito, não sendo diferente no âmbito penal. Por um lado, o avanço tecnológico e a difusão da internet para quase a totalidade das pessoas e das novas tecnologias de informação, influenciam e continuam a promover, em certa medida, a atividade criminosa, proporcionando o surgimento de delitos exclusivamente virtuais e, quando não, utilizando a rede para facilitação do cometimento de infrações que não se restringem ao ambiente virtual. Nesta toada, é latente o interesse do Estado em aprimorar-se na utilização dessas novas tecnologias para repressão e prevenção dos delitos. Neste cenário, a presente pesquisa se propõe a analisar a viabilidade do uso de agentes infiltrados digitais, através de *softwares* espiões de dados, mais precisamente os *malwares*, 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, a legislação aplicada ao caso, com um enfoque para a conclusão respeitando o Estado Democrático de Direito.

A presente pesquisa tem 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.

Para fins desta pesquisa deve-se questionar 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 deste software na fase investigativa? Esta

é a pergunta nevrálgica que guia a presente pesquisa. Em tempo, também cumpre analisar em que medida o direito constitucional, frente a proteção de dados, nas suas dimensões subjetiva e objetiva, são violadas pelo uso de *malwares*.

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* (interpreta-se: hackear para fins perversos, egoístas ou para atender os interesses de terceiros) que por vezes tais indivíduos são patrocinados pelo Estado[1] na ânsia acusatória vivenciada. Embora esses softwares possam proporcionar um aumento significativo na eficiência das investigações, suas características intrínsecas também podem levar a restrições questionáveis aos direitos fundamentais e garantias constitucionais estabelecidas.

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 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 Constituição Federal e, em seguida, com enfoque na legislação vigente relativa aos meios de obtenção de prova, incluindo disposições do Código de Processo Penal e da Lei 12.850/2013, bem como da Ação de Arguição de Preceito Fundamental, tombada perante o Supremo Tribunal Federal sob nº: 0091455-54.2023.1.00.0000, de relatoria do Ministro Cristiano Zanin, também no ordenamento jurídico pátrio, a LGPD - Lei Geral de Proteção de Dados, a qual trata da proteção dos nossos dados pessoais assim como dados sensíveis assim como a Lei Carolina Dieckmann e o Marco Civil da Internet brasileira.

Finalmente, propõem-se analisar os desafios do Estado Democrático de Direito em enfrentar o *cibercrime* e obviamente os métodos utilizados no combate dos mesmos e o quão isso pode ser invasivo frente aos ditames constitucionais, permeados por diversas tecnologias, 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.

Este trabalho foi desenvolvido através de pesquisas bibliográficas com o objetivo de apresentar à importância de entender o que são os *malwares* como intrusão virtual remota e seus impactos na obtenção da prova na esfera penal, frente à Lei Geral de Proteção de Dados

[1] Para ZUBOFF, o capitalismo de vigilância é mais bem descrito como um *golpe vindo de cima,* não uma derrubada do Estado, mas, sim, uma derrubada da soberania das pessoas e uma força proeminente na perigosa tendência rumo à desconsolidação democrática que agora ameaça às democracias liberais ocidentais.

(LGPD) e dos direitos e garantias previstos na Constituição Federal, mais precisamente o da privacidade, intimidade, inviolabilidade e sigilo das comunicações, ou seja, buscar formas de possivelmente termos uma regulamentação específica para a utilização dos agentes infiltrados digitais e/ou *softwares maliciosos*, que podem vir a violar preceitos protegidos pelo Estado Democrático de Direito. Trata-se de um estudo sistematizado, onde a fundamentação teórica será realizada pela análise de livros, artigos e julgados que tratam sobre o tema.

2. A regulamentação do uso de Malwares na ordem jurídica 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". *Malwares* são um gênero de um *software* que possuem distintas e diversas espécies como, por exemplo, um *malware* designado à softwares ou programas simples que por essência tem uma natureza auto-replicativa que, sem a ciência do usuário, são secretamente inseridos em seu dispositivo eletrônico, seja um computador, um tablet, inclusive servidores de segurança privada, dispositivos da era da Internet das Coisas (IoT), *wearables* como *smartwatches*, sem a exclusão de *smartphones*.

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 à informações e dados ali armazenados ou em processo de manipulação, de forma instantânea. Ademais, esses *softwares* possibilitam um controle oculto e contínuo sobre várias funcionalidades do sistema afetado. Frequentemente descritos como programas espiões, os *malwares* são capazes de coletar uma vasta gama de dados desses dispositivos eletrônicos assim como sistemas operacionais, tanto aqueles em processamento ativo quanto os meramente armazenados, além de se ter acesso, em tempo real, de informações como localização através do GPS ou ativação, pelo administrador, de dispositivos de áudio e vídeo dos equipamentos infiltrados.

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 (aqui entendidos como elementos informativos na fase de investigação) 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. Uma vez instalados secretamente, esses programas exploram vulnerabilidades para estabelecer uma "*backdoor"*, ou porta de acesso remoto, que facilita o controle invisível do sistema. (Ramos, 2019). Tal espécie de *malware*, ganha o nome de *Cavalo de Tróia* ou *Trojan*.

Em uma simples premissa, pode-se compreender que a utilização desse malware se dá de forma simples, podendo também ser auto replicável, instalando-se discretamente em um sistema operacional, sem a ciência e a anuência do usuário-vítima, colocando em risco a confiabilidade e a integridade dos dados de tal dispositivo eletrônico, através de ações que são executadas externamente (Barbiero, 2021).

Malwares compreendem uma variedade de espécies, como *Cavalos de Troia* (ou *Trojans*), *bombas lógicas, spywares*, *keyloggers, screenloggers*, *rootkits*, *worms, vírus,* ameaças combinadas e *bots*, todos caracterizados pela instalação dissimulada em sistemas informáticos, comprometendo suas funções sem o conhecimento do usuário. (Batista, 2018).

Os operadores podem ser pessoas físicas, em âmbito privado, como uma espécie de mercenários da rede: são pagos, geralmente em por meio de criptoativos, para lançar uso de *malwares* na rede. Como já explicitado nesta pesquisa, agentes públicos também podem fazer uso de *malwares.* Contudo, pessoas jurídicas, sendo estas, empresas *Big Tech*, que visam ter o máximo de controle sobre seus usuários, também podem abusar de *malwares* sem a sapiência de seus usuários em rede. Dois exemplos notórios do emprego de *Malwares* por empresas colossais são: (i) O antigo Facebook, atual Meta, no caso Cambridge Analytica (Beck, 2020) e (ii) o Google, conforme explica Zuboff:

> O Google está sob enorme pressão da comunidade financeira para aumentar a "eficácia" do seu rastreamento, de modo a poder aumentar receitas e lucros. Dar ao usuário a capacidade de controlar sua informação privada (e de se proteger de malware) bloqueando conexões invisíveis com sites problemáticos constitui uma ameaça à existência do Google." (Zuboff, 2019).

Como dito, o uso dos *malwares constitui* um abuso de direito, via de regra. A exceção ocorre via alvará judicial, o que autoriza o excepcional uso *in casu*. O operador, doravante *cracker*, por sua vez – atua fora da esfera da legalidade — através de uma atividade ilegal e inconstitucionalmente exercida: via a disseminação de diversas espécies de *malwares*; ao tentar permanecer conectado à tais dispositivos eletrônicos de terceiros pelo maior tempo possível; sem efetivamente manifestar a sua existência ao usuário-vítima.

Dessa forma, o *cracker* ao longo do tempo, consegue coletar um maior volume, uma maior diversidade e veracidade de dados pessoais de seu alvo, aumentando-se o tamanho do *banco de dados* do usuário-vítima e logo, majorando também o valor de tais dados. Um *cracker*

pode obter um vasto campo de acesso, monitoramento e transferência de dados, arquivos, senhas, e informações para servidores remotos, além de coletar dados e hábitos do usuário na internet, incluindo a verificação dos horários de acesso, doravante *logs*, a determinadas páginas eletrônicas, mensagens trocadas com terceiros, até mesmo a localização, em tempo real, do usuário-vítima que tem o seu dispositivo eletrônico infiltrado.

Indubitavelmente, que alguns programas, como *keyloggers* e *screenlogger*s, registram as teclas digitadas pelo usuário-vítima, fornecendo ao *cracker* um registro detalhado das atividades realizadas. Outros *crackers* por meio de *malwares* podem ativar webcams e microfones para capturar sinais ópticos e acústicos, além de coletar dados de geolocalização em tempo real. Esses programas também podem monitorar comunicações de áudio e texto de forma instantânea, burlando determinadas tecnologias no campo da cibersegurança, como alguns protocolos de criptografia.

É importante destacar que os dispositivos maliciosos podem requerer a instalação física em sistemas informáticos ou, mais comumente na era digital, serem instalados remotamente através de e-mail ou envio de links enganosos, técnicas mal-intencionadas a fim de retirar a atenção dos destinatários.

Com o avanço de novas tecnologias e a utilização da internet como meio de comunicação entre as pessoas que convivem em sociedade cada vez mais globalizada, de certo modo, a atividade criminosa também migrou, como consequência lógica, para o meio eletrônico, surgindo delitos e crimes cometidos através da rede ou, quando não for o caso, utilizando-se da internet como meio condutor/facilitador para o *iter criminis* - caminho do crime, da prática delitiva. Nesse sentido, o Estado, como agente garantidor dos sistemas de segurança pública, a fim de reprimir tais condutas, aprimorou-se na utilização dessas tecnologias ao seu favor, como por exemplo, os agentes infiltrados digitais, na tentativa de repressão - à criminalidade, à prevenção de novos delitos, e à identificação - dos indivíduos.

Para (Pinho, 2022), 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.

A interligação existente entre máquinas e seres humanos traz grandes benefícios por estarem cada vez mais próximas, subsistindo enormes oportunidades, sem perder de vista as ameaças que podem sobrevir, uma vez que, a relação entre homem e máquina não mais

retroagirá, ao passo que se moderniza com o passar dos dias. Embora o direito não evolua de forma significativa na mesma celeridade dos meios tecnológicos, em especial o direito penal e suas políticas criminais, deve-se amoldar, com maior brevidade possível, para tentar acompanhar essa evolução.

O sistema de justiça criminal, pode-se beneficiar com o uso das tecnologias digitais, onde muitos países já estão usando para aumentar a eficiência em seus sistemas de justiça, fortalecendo a transparência na investigação criminal. No entanto, esse avanço deve ser analisado com cautela, pois se a tecnologia traz facilidades na investigação criminal, há a possibilidade de vir acompanhada de violações aos direitos fundamentais, os quais são essenciais para cristalizar a dignidade da pessoa humana e a segurança (Pinho,2022).

No Brasil, em 2024, não há óbice, sob o estado da arte, isto é, sob a perspectiva técnica, assim como sob a legislação pátria e vigente para a utilização desses *malwares* por agentes de segurança pública com o objetivo da obtenção dos dados pessoais de indivíduos investigados, sob *conditio sine qua non* de um alvará judicial permitindo tal coleta assim como os limites de tais *malwares*. Dito isso, como a coleta de dados é ampla, isto é, se coleta todo tipo de dado, seja um dado estruturado (como uma planilha em arquivo de *excel*), seja um dado não estruturado (como uma foto ou um vídeo); não se coleta apenas um *dataset*, isto é, uma expressão singular do disco rígido dos dispositivos eletrônicos do indivíduo investigado. Logo, é possível admitir-se que, tendo em vista que o acesso e a coleta de tais dados se dão de forma irrestrita, confrontando-se, como se verá adiante, com os princípios e garantias constitucionais.

Como se não bastasse as ofensas às normas e princípios constitucionais, essa utilização também se choca com a nova legislação especial sobre o tema delimitado. Trata-se da Lei 13.709/2018, a Lei Geral de Proteção de Dados, ora doravante LGPD, que fora introduzida no ordenamento pátrio para, como o próprio nome já anuncia, proteger os dados pessoais de usuários na rede, de eventual exposição não solicitada e sem seu consentimento.

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 a Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, que inseriu no Código Penal o crime de invasão de dispositivo eletrônico; informático; nos termos do Artigo 154-A. Não se pode perder de vista outra norma embasada para utilização dessa tecnologia, que é a Lei Federal 12.850/2013, que trata sobre organizações criminosas.

Referida norma 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. Não se pode

perder de vista que, segundo a referida norma, pelo fato de se 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,2022).

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. (Riboli, 2019)

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.

3. Uso de Malwares e o direito constitucional da privacidade

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".*

O uso excepcional de *malwares*, em investigações criminais, tem o potencial de comprometer o núcleo[2] essencial de direitos fundamentais garantidos pela Constituição Federal. Explica-se: Quando agentes públicos, como membros do *parquet*, sob Alvará Judicial permitindo a coleta, armazenamento e tratamento de dados pessoais, sensíveis, de metadados como geolocalização de dispositivos eletrônicos, como *smartphones*, e em tempo, de forma análoga, à interceptação telefônica, concedida por determinação judicial; em ambas as hipóteses, não se captura o *dataset* ou conjunto de dados necessários para a respectiva

[2] 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)

investigação judicial apenas. Tal ponto é de fundamental importância, pois, pode-se, compreender que toda espécie de dado (seja ele um dado estruturado, um dado não estruturado e metadados) além do *dataset* necessário para o procedimento persecutório, pode ser interpretado como uma violação ao princípio da legalidade, e ferir normas no patamar constitucional. O excesso da captura ou coleta de dados por agentes públicos podem constituir evidente e certa 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* (em tradução livre de *malwares* ou *malicious softwares*), permitem o acesso a uma grande variedade e volume de dados (como fotos, vídeos, informações bancárias, senhas, dados financeiros, arquivos sigilosos, comunicações escritas, dados íntimos, etc.). Os *malwares* se tornam 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).

Neste contexto, ao reconhecer o direito à privacidade - que se refere à proteção da vida privada do indivíduo, como uma prerrogativa intrínseca à personalidade e que deve ser intangível e inviolável - é essencial refletir sobre a eficácia prática desta previsão constitucional em investigações criminais. Cumpre informar que antes de existir uma lei geral para punições de delitos e crimes no âmbito digital, 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; também conhecido como o *Brazillian Internet Bill of Rights*. 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 (MORAIS, 2020).

A sociedade civil e organizada, por meio de organizações sem fins lucrativos que visam a promover a proteção dos usuários em rede assim como por organizações do terceiro setor que –por meio de ações e de diálogos multisetoriais— visam à criar salvaguardas para usuários na

rede; diante da problemática dos *malwares*. De acordo com Zuboff:

> Outra bagunça em termos jurídicos é um exemplo ainda melhor de como produtos como Android são mais valorizados para suprimento do que para vendas. A Disconnect, Inc., fundada em 2011 por dois ex-engenheiros do Google e um advogado especializado em direitos de privacidade, desenvolveu aplicativos para desktop e celulares e tablets "para proteger a privacidade e segurança de usuários da internet bloqueando conexões de rede invisíveis, não solicitadas entre o navegador de um usuário ou o dispositivo móvel e sites/serviços que envolvem rastreamento invisível ou são conhecidos ou suspeitos de distribuir malwares [...] não só quando o usuário navega pela web, mas também quando usa outros aplicativos de terceiros". A Disconnect visava, em específico, às conexões de rede "invisíveis, não solicitadas e com frequência não reveladas" de sites e serviços de terceiros que ocorrem tão logo se visita um site ou um determinado aplicativo móvel é aberto. Para o azar da Disconnect, o próprio processo que ela desejava impedir havia sido estabelecido como uma significativa rota de suprimento para o Google e outros capitalistas de vigilância." (Zuboff, 2019).

Quando o direito à privacidade está intimamente ligado ao fortalecimento dos direitos individuais, observa-se a preocupação do Estado com os Direitos Fundamentais do indivíduo. Em um segundo momento, observa-se o desenvolvimento da concepção de que existe uma esfera da vida e da personalidade das pessoas que é intransponível, ou seja, que nem o Estado nem outras pessoas podem violar. Essa esfera refere-se à intimidade, um âmbito inviolável que ninguém pode ultrapassar. Assim, esse meio de obtenção de provas só poderá ser sólido e eficaz se estiver fundamentado nos direitos e liberdades fundamentais. Pois como bem assegura Maria Celina Bodin de Moraes:

> [...] De fato, salta aos olhos a insuficiência do conteúdo que deu origem ao direito à privacidade – o "direito de ficar só" (*right to be alone*) –, pensado por Warren e Brandeis no final do séc. XIX, tendo sugerido, em seu lugar, "o direito à autodeterminação informativa" e, em âmbito mais genérico, "o direito de manter o controle sobre as próprias informações e de determinar o modo de construção da própria esfera privada". (Moraes, 2010).

O direito de ser deixado só está associado a um isolamento, o direito que o indivíduo possui de estar em estado de reclusão, ao mesmo tempo em que as tecnologias avançam e aumentam as possibilidades de escolhas impactando diretamente na vida privada. Os indivíduos tornam-se expostos aos olhos alheios pela intrusão de inúmeros *softwares* de invasão que a cada dia só aumentam. Em contraponto, para essa proteção, pode bastar que se conceba a privacidade como uma liberdade negativa, isto é, que reconheça e tutele a pessoa contra abusos na obtenção e tratamento de tais dados. (Doneda, 2019).

Consoante à Zubbof, observa-se o caso europeu, sob a lei geral de dados da União Européia, isto é, a GDPR, *in casu Scherms*:

> [...] Já é possível ver um novo despertar para o empoderamento da ação coletiva, pelo menos no domínio da privacidade. Um exemplo é a None of Your Business [Não é da sua conta] (NOYB), uma organização sem fins lucrativos comandada pelo ativista em privacidade Max Schrems. Após muitos anos de disputa judicial, Schrems fez história em 2015 quando seu questionamento das práticas de coleta e retenção de dados do Facebook — que ele afirmava estarem violando a lei de privacidade da União Europeia — levou o Tribunal de Justiça da União Europeia a invalidar o acordo Safe Harbor [Porto seguro], que regia transferências de dados entre os Estados Unidos e a União Europeia. Em 2018, Schrems lançou a NOYB como um veículo para a "aplicação profissional da privacidade". O intuito é forçar as agências reguladoras a diminuir o espaço entre os regulamentos escritos e as práticas corporativas de privacidade, alavancando a ameaça de multas significativas para mudar os procedimentos das empresas na prática." (Zuboff, 2019).

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. Segundo o jornal *Washington Post* e outras fontes da mídia tradicional, o *software* Pegasus não só permite o monitoramento de todas as comunicações de um *smartphone* (textos, e-mails, pesquisas na web, histórico de navegação, etc.), mas também possibilita o rastreamento de chamadas telefônicas e localização. Além disso, este *spyware* permite à empresa infiltrar tanto o microfone quanto a câmera do *smartphone*, transformando-o em um dispositivo de vigilância constante.

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 de um exercício da jurisdição constitucional ser articulada como instância asseguradora de tais direitos (Morais, 2020)

No caso do Brasil, sob o *Gabinete Paralelo*, sob mando do vereador do Rio de Janeiro à época, durante a gestão do ex-Presidente da República no respectivo ano, traduziu em uma vigilância governamental totalmente invasiva, ilegal e inconstitucional. Tratou-se de um *ius puniendi et extra,* isto é, um direito de punir exacerbado.

De forma diametralmente oposta, existe o princípio da humanidade – do direito penal— ou respeito à dignidade pessoal. Reúna-se várias facetas, como a salvaguarda da humanidade diante de toda intervenção punitiva geral, compreensiva das dimensões tanto valorativas, quanto teleológicas como forma de execução. O caráter do princípio da humanidade abarca o princípio da intervenção penal em seu conjunto. Toda intervenção punitiva no Estado Social e Democrático de Direito deve ser guiada pelo princípio de respeito à dignidade humana –

princípio que expressa um critério que é fundamento e guia de toda ação punitiva estadual (*reus sacra est*). (Costa, 2003).

Urge salientar que quando da utilização dos *malwares* por agentes públicos sempre deve haver um pedido devidamente fundamentado e uma autorização judicial para tanto. Tais investigações criminais por meio tecnologicamente intrusivo torna-se fundamental, pois a investigação sem tais recursos tecnológicos poderia não ser suficiente na fase persecutória.

Contudo, o abuso de *malwares* por agentes públicos, para fins de investigações criminais, sem autorização judicial incorre em uma violação aos direitos fundamentais amplamente assegurados no artigo 5 da Magna Carta, ou seja, uma inconstitucionalidade. Sem embargo, também cumpre destacar a necessidade de uma legislação específica, em direito criminal, como uma *LGPD penal*, para fins de respeito ao princípio da legalidade em que pese o respeito aos limites dos usos de *malwares* por parte de agentes públicos.

Até o Congresso Nacional e o Presidente da República aprovar um Projeto de Lei (PL) que verse sobre tal tema delimitado, ficará o ônus ao Poder Judiciário com a limitada e esparsa legislação que, em 2024, se tem, no ordenamento jurídico vigente, para permitir, por via de exceção que ora a Polícia Federal, o COAF e o Ministério Público possam requerer a quebra – sempre temporária e por prazo determinado— da privacidade e intimidade de indivíduos na rede para fins de investigações criminais.

4. A lógica de proteção da LGDP aplicada ao uso 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. Em tese, a legislação especial atende à proteção e ampliação dos direitos fundamentais de liberdade, da privacidade e o livre desenvolvimento da personalidade da pessoa natural, introduzindo importantes regras e diretrizes para a coleta, armazenamento e uso

adequado em fase de tratamento dos dados pessoais da população no Brasil. A LGPD tem por objetivos não apenas aumentar a transparência, mas reforçar 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). Empresas que fazem uso de tratamento de dados precisam obrigatoriamente preparar relatório de impacto de riscos à Autoridade Nacional de Proteção de Dados, ora doravante ANPD.

A lei define o que são dados pessoais assim como especifica o que são dados pessoais sensíveis os quais requerem cuidados especiais. Esclarece que todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação e eventual repreensão por parte da ANPD, uma espécie *sui generis* de Agência Reguladora. Além disso, estabelece que, independentemente da localização da sede de uma organização ou de seus centros de dados, se houver processamento de dados sobre pessoas no território nacional, a LGPD deve ser aplicada.

É importante dar destaque ao princípio da privacidade contextual: um conceito normativo que dá origem a dois tipos de direitos, que podem ser vistos como duas faces da mesma moeda. De um lado, há o direito do titular de exercer controle sobre seus dados, mesmo que não tenha dado consentimento explícito, desde que esses dados sejam tratados de acordo com sua legítima expectativa. Do outro lado, há o direito de quem deseja processar dados pessoais sem a necessidade de uma manifestação de vontade por parte do titular, de um alvará judicial, como os órgãos do Estado em investigações criminais. (Bioni, 2020)

Sob uma perspectiva processual penal o professor Aury Lopes Júnior em sua obra "Direito Processual Penal" 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.

Não deixamos de analisar, em decorrência dos direitos fundamentais, a necessidade de se chegar à conclusão de que, justamente, a proteção de dados pessoais deve ser tratada como direito fundamental, em relação ao dever de proteção, onde encontra-se o papel do Estado em

zelar, ativamente, pela consistência e efetividade, não somente da LGPD, mas, também, de todas as normas vigentes no Brasil e que dizem respeito à proteção de dados. (Morais, 2020).

Nesse sentido, Aury Lopes Jr. e Carlos Hélder Carvalho sustentam que o direito à integridade e confidencialidade dos sistemas informáticos pode ser incorporado à Constituição de 1988 por força da cláusula de abertura prevista em seu art. 5º, § 2º, que dispõe que "os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa faz parte de um trabalho em andamento cujo objetivo é conscientizar sobre a existência de *malwares* (*softwares maliciosos*) 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 regulação 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.

A evolução tecnológica tem proporcionado avanços significativos nas investigações criminais, permitindo que agentes públicos utilizem ferramentas sofisticadas como os *malwares*. No entanto, o uso dessas tecnologias deve ser rigorosamente regulamentado para proteger os direitos e garantias constitucionais dos indivíduos. A ausência de um marco regulatório específico que estabeleça diretrizes claras para a utilização de *malwares* em investigações penais cria um ambiente propício para abusos e violações de direitos fundamentais, como a privacidade e a inviolabilidade das comunicações pessoais.

É imprescindível que o Brasil desenvolva uma legislação específica que regulamente o uso de *malwares* por agentes públicos. Essa regulamentação deve garantir que a utilização dessas ferramentas seja sempre acompanhada de autorização judicial e que respeite os limites estabelecidos pela Constituição Federal e pela Lei Geral de Proteção de Dados (LGPD) e outras normativas pertinentes.

Além disso, é crucial reconhecer que o uso de *malwares* por terceiros é um crime e deve ser tratado como tal. A disseminação de *malwares* por indivíduos não autorizados representa uma grave ameaça à segurança e à privacidade dos cidadãos, devendo ser combatida com rigor pelas autoridades competentes.

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.

6 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.

BARBIERO, Diego Roberto. **Implantação de *malwares* em investigações complexas**./ Diego Roberto Barbiero./ Curitiba: Juruá, 2021.

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.

BATISTA, Lydie Jorge. **O Malware como meio de obtenção de prova em Processo Penal .** 2018. Dissertação de Mestrado em Ciências Jurídico- Forenses – Universidade de Lisboa Faculdade de Direito. Lisboa, Portugal, 2018.

BRASILIA, DF. Presidente da República. **Constituição da República Federativa do Brasil, 1988**. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 08 de junho de 2024.

BECK, Cesar. **CAMBRIDGE ANALYTICA: Escândalo, Legado e Possíveis Futuros para a Democracia.** Editora Unijuí – Ano XXIX – Revista Direito em Debate – n. 53 – jan./jun. 2020. DOI: https://doi.org/10.21527/2176-6622.2020.53.182-195.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento** – 2, ed. – Rio de Janeiro: Forense, 2020. ISBN 978-85-309-8862-3.

CENSO 2022. IBGE. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/22005-censo-2022-o-retrato-atualizado-do-brasil.html. Acesso em: 11 de Maio de 2024.

COSTA ROSSI, H.; MUSA DE ALMEIDA, L. **O uso do malware na investigação criminal: pontos de tensão e limites**. Boletim IBCCRIM, [S. l.], v. 31, n. 373, [s.d.]. DOI: 10.5281/zenodo.10188525.

COSTA MAYRINK, Álvaro. **Os Limites do ius puniendi do Estado.** Desembargador do TJ/RJ. Professor da EMERJ. Revista EMERJ, v.6 nº 23, 2003.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da informação da Lei Geral de Proteção de dados – 2.ed. – São Paulo: Thompson Reuters Brasil, 2019. ISBN 978-85-5321-957-5.

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

LOPES JR, Aury; MENDES, Carlos Hélder Carvalho Furtado**. "Vírus espião" como meio de investigação: a infiltração por softwares**. Disponível em: https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares/. Acessado em 10 de Maio de 2024.

MORAIS, Fausto Santos (org). **Dever de Proteção, Direitos Fundamentais e Argumentação Jurídica:** Volume I/ Fausto Santos de Morais. – Passo Fundo: Conhecer, 2020. ISBN: 978-65-9927082-6.

MORAIS, Maria Celina Bodin de. **Na medida da pessoa humana: estudos de direito civil** – Rio de Janeiro: Renovar, 2010. ISBN 978-85-7147-780-3.

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.

STANGHERLIN, Marina. **Agentes infiltrados: sua natureza jurídica na produção digital de provas**./ Marina Stangherlin, Fabiano Augusto Petean. - 1. ed. - Curitiba: Appris, 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder:** Tradução Geroge Schlesinger. – 1.ed. – Rio de Janeiro: Intrínseca, 2019. ISBN 978-65-5560-144-2.