AFYA - FACULDADE DE PARNAÍBA.
Curso de Direito
Disciplina de Trabalho de Conclusão de Curso II

A Lei Carolina Dieckmann e os desafios jurídicos no combate aos crimes cibernéticos no Brasil.

Harthur Vieira Loiola

Mateus do Santos Souza

Herbson Silva Marques Júnior

PARNAÍBA/PI
2025

Harthur Vieira Loiola

Mateus do Santos Souza

Herbson Silva Marques Júnior

A Lei Carolina Dieckmann e os desafios jurídicos na repressão aos crimes de invasão de dispositivos eletrônicos no Brasil.

Projeto de pesquisa apresentado à disciplina de Trabalho de Conclusão de Curso II como requisito para obtenção de nota no Curso de Direito AFYA PARNAÍBA.

Professor da Disciplina: Geilson Silva Pereira

PARNAÍBA/PI
2025

RESUMO:

O presente trabalho tem como objetivo analisar a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, investigando seus fundamentos, limitações e desafios na repressão aos crimes de invasão de dispositivos eletrônicos no Brasil. A pesquisa, de natureza qualitativa e teórica, fundamenta-se em revisão bibliográfica e documental, abordando aspectos jurídicos, sociais e tecnológicos que envolvem a proteção da privacidade e a efetividade da legislação penal no ambiente digital. O estudo busca compreender como o avanço tecnológico tem impactado o Direito Penal e a necessidade de atualização normativa frente à crescente complexidade dos delitos cibernéticos.

Além disso, o trabalho analisa as implicações da lei para os direitos fundamentais, especialmente a privacidade, a intimidade e a liberdade de expressão, destacando as tensões existentes entre segurança pública e garantias constitucionais. Observa-se que, diante da aceleração tecnológica, o Estado enfrenta dificuldades para harmonizar a repressão penal com a proteção dos direitos individuais, o que exige políticas públicas e instrumentos normativos mais eficazes. Nesse sentido, a pesquisa propõe reflexões sobre a importância da interdisciplinaridade entre Direito, tecnologia e políticas de segurança digital.

Os resultados obtidos demonstram que, embora a Lei Carolina Dieckmann represente um marco jurídico relevante para a tutela da dignidade humana no ambiente virtual, sua aplicação prática ainda é limitada. As lacunas legais, a deficiência estrutural das investigações e a ausência de cooperação internacional efetiva dificultam o enfrentamento dos delitos cibernéticos. Assim, torna-se necessária a atualização legislativa contínua, aliada à capacitação técnica dos operadores do Direito e à criação de estratégias nacionais integradas de combate aos crimes digitais.

Conclui-se que a efetividade da Lei Carolina Dieckmann depende da cooperação entre Estado, sociedade e comunidade jurídica, de modo a promover um ambiente digital mais seguro, ético e equilibrado entre liberdade e responsabilidade. O estudo contribui para o fortalecimento do Direito Digital brasileiro, ao reforçar a importância de um ordenamento jurídico apto a acompanhar as transformações tecnológicas e a garantir a proteção dos direitos fundamentais no ciberespaço.

Palavras-chave: Lei Carolina Dieckmann. Crimes cibernéticos. Privacidade. Direito Digital. Invasão de dispositivos eletrônicos. LGPD.

1. INTRODUÇÃO

O presente artigo tem como propósito mergulhar nas águas, por vezes turvas, da Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, e desvendar os intrincados desafios jurídicos que rondam o combate aos crimes de invasão de dispositivos eletrônicos no Brasil. Não se trata apenas de um estudo técnico, mas de uma reflexão sobre um tema que pulsa no coração da sociedade contemporânea, em que cada clique parece ecoar entre luzes e sombras do ciberespaço. Afinal, sejamos francos: a tecnologia não espera ninguém.

Pois bem, a ideia central é compreender as implicações jurídicas e sociais desse fenômeno, partindo da constatação de que a evolução tecnológica corre à velocidade da luz, enquanto a legislação, coitada, tropeça em lacunas históricas, abrindo brechas que fazem a justiça parecer, muitas vezes, um barco à deriva em mar revolto. Nessa maré digital, como garantir a inviolabilidade da privacidade e da intimidade sem engessar a liberdade? Eis a pergunta que guia nossa bússola.

Nesse cenário de incertezas, onde cada byte pode ser um aliado ou um inimigo, a relevância do tema salta aos olhos. O aumento vertiginoso dos ataques cibernéticos transformou a segurança digital em algo tão essencial quanto o ar que respiramos. Não dá mais para fingir que é um problema distante: o perigo bate à porta, mesmo quando ela parece trancada. É por isso que este estudo não se limitará a apontar falhas, mas buscará lançar luz sobre caminhos que fortaleçam tanto a legislação quanto as políticas públicas, costurando uma rede de proteção mais firme contra os ardis do mundo virtual.

No âmbito acadêmico, a pertinência deste trabalho é evidente: há um vazio doutrinário que precisa ser preenchido, um silêncio que clama por vozes críticas e fundamentadas. Assim, pretendemos construir um alicerce sólido para a dogmática penal digital no Brasil, oferecendo reflexões que, quem sabe, sirvam como farol para futuras reformas normativas. A contribuição busca ir além da crítica propondo bases estruturantes para um ramo do direito ainda em consolidação no país.

E como faremos isso? A pesquisa seguirá um viés teórico e qualitativo, com uma revisão bibliográfica e documental que mais se parece a uma escavação arqueológica, desenterrando conceitos, normas e interpretações soterradas sob camadas de debates. A análise, por sua vez, será categorial e conceitual, passando ainda pelo crivo da jurisprudência. As fontes primárias serão a legislação penal vigente, em especial, a Lei 12.737/2012 e o Código Penal,

acompanhadas de decisões dos tribunais superiores, já as secundárias virão da doutrina nacional e internacional que se dedica ao Direito Digital.

O objetivo geral? Simples, mas nem tanto: analisar os fundamentos jurídicos e os obstáculos práticos que se erguem no caminho da aplicação da Lei Carolina Dieckmann contra os crimes de invasão de dispositivos eletrônicos no Brasil. Para isso, desdobram-se objetivos específicos, como contextualizar a gênese da lei e os ventos sociais que sopraram em sua direção, examinar as brechas normativas e processuais que fragilizam sua eficácia e, claro, discutir o impacto da norma sobre direitos fundamentais privacidade, intimidade e até a liberdade de expressão, que muitas vezes caminham sobre uma corda bamba.

Para manter a narrativa coesa, o trabalho será organizado em três grandes capítulos que se entrelaçam como fios de uma teia. No primeiro, exploraremos a evolução histórica da tipificação penal cibernética no Brasil, situando a Lei Carolina Dieckmann como resposta a um caso emblemático que incendiou a mídia e sacudiu as estruturas do ordenamento jurídico. Será um olhar para trás, não como quem deseja voltar, mas para compreender o caminho trilhado até aqui.

O segundo capítulo mergulhará fundo na análise dogmática do tipo penal do art. 154-A do Código Penal, examinando cada detalhe: objeto jurídico, sujeitos ativo e passivo, conduta tipificada e suas modalidades. Além disso, discutiremos as controvérsias que rondam o tema, desde a escolha das palavras na lei até os desafios quase hercúleos de se obter provas técnicas em um ambiente tão volátil como a rede.

Por fim, no terceiro capítulo, vestiremos o manto crítico para avaliar a eficácia da lei e seus reflexos no sistema de justiça. Vamos desvendar os entraves que surgem desde o momento da denúncia até o trânsito em julgado, equilibrando a balança entre repressão penal e garantias constitucionais. Ao final, lançaremos propostas que, embora não tenham a pretensão de serem panaceias, podem apontar trilhas para um futuro mais seguro no vasto e inquietante ciberespaço.

Em suma, espera-se que este estudo não seja apenas mais um tijolo no muro do conhecimento, mas uma fagulha capaz de acender debates e inspirar mudanças. Porque, no fundo, é isso que buscamos: transformar a norma fria em um instrumento vivo, capaz de proteger efetivamente a intimidade e a privacidade dos cidadãos, sem, no entanto, sufocar as liberdades individuais ou impedir o florescimento inovador que caracteriza nossa era digital que ao mesmo tempo é tão rica e tão perigosa.

2. DESENVOLVIMENTO

2.1 A lei Carolina Dieckmann: origem, fundamentos e impactos no ordenamento jurídico.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, surgiu após a divulgação de fotos íntimas da atriz Carolina Dieckmann, que teve seu computador invadido em 2012. O episódio revelou a ausência de legislação específica para crimes cibernéticos no Brasil, que até então utilizava analogias do Código Penal, como o crime de violação de correspondência (Art. 151 do CP). Promulgada em 30 de novembro de 2012, a lei tipificou crimes como invasão de dispositivos informáticos (Art. 154-A), interrupção de serviços telemáticos (Art. 154-B) e falsificação de cartões (Art. 266). Apesar do avanço, a lei mostrou-se insuficiente para enfrentar a crescente complexidade dos delitos digitais.

A criação da lei foi impulsionada pela pressão social por maior segurança digital, ainda que sua elaboração tenha sido considerada apressada. Embora o Brasil não seja signatário, seu conteúdo se aproxima de normas internacionais, como a Convenção de Budapeste (2001), que influenciou o debate sobre cooperação transnacional. Contudo, a priorização de casos midiáticos em detrimento de uma abordagem sistêmica gerou lacunas relevantes. Crimes como ransomware não possuem tipificação clara, obrigando o uso de analogias jurídicas, e a ausência de previsão para o sequestro de dados reforça essa fragilidade normativa.

Hernandez e De Toledo (2021) ressaltam que os crimes cibernéticos exigem atualização constante da legislação, o que não se verifica no Brasil. Novas práticas criminosas, como deepfakes e ataques a dispositivos de IoT, não possuem previsão legal expressa, abrindo brechas para impunidade. O Art. 154-A restringe-se à invasão de dispositivos físicos, ignorando redes e ambientes em nuvem que concentram cerca de 85% das informações atuais. Essa limitação enfraquece a lei diante da realidade tecnológica, pois não contempla os principais espaços de vulnerabilidade.

Krieguer, Ceron e Marcondes (2021) enfatizam a importância da cooperação internacional no combate aos crimes cibernéticos. Contudo, a Lei Carolina Dieckmann não prevê protocolos padronizados para coleta de evidências digitais, dificultando investigações sem o auxílio de peritos. A falta de tratados de extradição específicos também inviabiliza respostas conjuntas entre países. A identificação de autores é dificultada pelo anonimato proporcionado por ambientes como a deepweb e a darkweb que favorecem a prática de crimes complexos e transnacionais, desafiando a atuação policial.

As penas originais, de detenção de três meses a um ano, foram consideradas brandas diante do alto impacto dos crimes digitais. Mesmo após a reforma de 2021, que ampliou para reclusão de um a quatro anos, as sanções continuam desproporcionais frente ao lucro milionário obtido em fraudes bancárias. Segundo o Relatório Norton Cyber Security (2023), apenas 5% dos cibercrimes no Brasil resultam em condenação, o que enfraquece o caráter preventivo da norma. Soma-se a isso a sobreposição da Lei Carolina Dieckmann com a LGPD e o Marco Civil, gerando ambiguidades jurídicas.

Embora a lei represente avanço na proteção da privacidade, sua aplicação enfrenta tensões com legislações como o Pacote Anticrime (Lei 13.964/2019) que amplia a vigilância estatal. Há risco de legitimação de coletas massivas de dados, afetando a liberdade de expressão e criando dilemas entre segurança e direitos individuais. A vulnerabilidade das mulheres também se destaca: 78% das vítimas de revenge porn são do sexo feminino, segundo a SaferNet. Apesar disso, a lei não prevê apoio psicossocial ou mecanismos céleres de remoção de conteúdos íntimos.

Ulrich Beck (1992) aponta que, na sociedade de risco, ameaças modernas, como as digitais, não se limitam a fronteiras espaço-temporais. Isso exige novas formas de regulação jurídica que transcendam modelos tradicionais de responsabilidade e controle. Contudo, a "cegueira normativa" diante da complexidade tecnológica limita a eficácia da lei. A ausência de ferramentas como inteligência artificial e criminologia preditiva para análise de padrões fragiliza a prevenção. A privacidade, reconhecida como direito humano no Art. 12 da Declaração Universal, deve ser equilibrada com a segurança e a inovação.

Para tornar a lei mais efetiva, Eduarda Chacon Rosas e Isadora Helena G. Cardoso (2021) sugerem a criação de novos tipos penais e a harmonização com a LGPD. Recomendam também capacitação técnica com delegacias especializadas e a ratificação da Convenção de Budapeste, fortalecendo a cooperação internacional. Dornelas (2019) defende que a educação digital, integrada a políticas públicas, pode reduzir a exposição a riscos. A Lei Carolina Dieckmann foi um marco na proteção digital brasileira, mas sua eficácia depende de atualização normativa, capacitação técnica e conscientização social.

2.2 Implicações da lei Carolina Dieckmann para a proteção de direitos fundamentais.

A intensificação do uso das tecnologias digitais tem reconfigurado as dinâmicas sociais, econômicas e políticas, levantando dúvidas sobre a efetividade da legislação na proteção de direitos fundamentais, como a privacidade e a liberdade de expressão. Nesse cenário, torna-se essencial analisar como os marcos legais nacionais e internacionais têm respondido aos desafios impostos pela digitalização. O objetivo é garantir a preservação de tais direitos sem comprometer a inovação tecnológica, que, por sua vez, é motor de transformações sociais.

A privacidade, prevista no Artigo 12 da Declaração Universal dos Direitos Humanos (ONU, 1948) e no Artigo 5º, X, da Constituição Federal, sofre ameaças constantes pelo avanço de tecnologias como big data, inteligência artificial e vigilância massiva (ZUBOFF, 2019). A coleta indiscriminada de dados pessoais por governos e empresas impulsionou a criação de normas específicas. Entre elas, destacam-se o Regulamento Geral de Proteção de Dados (GDPR), na União Europeia, e a Lei Geral de Proteção de Dados (LGPD) no Brasil (Lei 13.709/2018).

Segundo relatório da Electronic Frontier Foundation (EFF, 2022), empresas ainda utilizam brechas legais para monetizar dados, enquanto governos ampliam sistemas de vigilância, como o reconhecimento facial, sem controle jurídico adequado. A tensão entre inovação tecnológica e proteção da privacidade exige atualização normativa constante. Moraes (2021) destaca que apenas regulamentação robusta e fiscalização efetiva são capazes de equilibrar os interesses econômicos com a proteção dos indivíduos.

A liberdade de expressão, garantida pelo Artigo 19 da Declaração Universal dos Direitos Humanos e pelo Artigo 5º, IV, da CF/88, enfrenta desafios inéditos com a moderação de conteúdo nas plataformas digitais. Redes sociais como Facebook, Twitter e YouTube recorrem a algoritmos para remover discursos considerados inapropriados. Essa prática, entretanto, é criticada por representar possível censura arbitrária, sem critérios claros (BENKLER, 2018), colocando em risco a pluralidade de ideias.

No Brasil, o Marco Civil da Internet (Lei 12.965/2014) estabeleceu princípios como a neutralidade da rede e a responsabilidade dos provedores. Contudo, a Lei de Liberdade, Responsabilidade e Transparência na Internet (Lei 14.132/2021) gerou polêmica ao permitir remoções sem ordem judicial em casos de “discurso de ódio”. Para Santoro (2022), a ausência de parâmetros objetivos pode ocasionar excessos e afetar a liberdade de expressão, tornando frágeis os mecanismos de proteção constitucional.

No plano internacional, a Digital Services Act (DSA), da União Europeia (2022), busca equilibrar moderação de conteúdo e transparência, exigindo justificativas claras para exclusões em plataformas. De acordo com o Relatório da Freedom House (2023), 60% dos países já adotaram leis que restringem discursos on-line sob o pretexto de combater fake news. Todavia, muitas vezes, tais normas acabam sendo instrumentalizadas para silenciar opositores políticos, corroendo a democracia.

O uso crescente de Inteligência Artificial (IA) em decisões automatizadas, como seleção de candidatos a empregos, concessão de crédito e até aplicação de leis, levanta preocupações com discriminação algorítmica e falta de transparência (O'NEIL, 2016). O relatório da UNESCO (2021) alerta que algoritmos podem reproduzir vieses sociais, atingindo principalmente grupos marginalizados. No Brasil, o Projeto de Lei 21/2020 busca criar um marco regulatório para IA, mas enfrenta resistência de setores que defendem a autorregulação (ABRANCHES, 2023).

A expansão de tecnologias de vigilância em massa, como o reconhecimento facial em espaços públicos, também vem sendo criticada por violações à privacidade e pelo aumento do controle estatal (SNOWDEN, 2019). No Brasil, cidades como São Paulo e Rio de Janeiro já utilizam esses sistemas, muitas vezes, sem respaldo legal sólido. A Resolução 11/2021 do Conselho Nacional de Proteção de Dados (CNPD) tentou estabelecer limites. No entanto, especialistas como Doneda (2023) argumentam que a fiscalização permanece insuficiente.

A disseminação de fake news e campanhas de desinformação nas redes sociais ameaça a liberdade de expressão ao distorcer debates públicos (WARDLE & DERAKHSHAN, 2017). No Brasil, a Lei 14.132/2021 criminalizou a divulgação em massa de informações falsas. Contudo, Mendonça & Souza (2022) alertam para o risco de uso político da norma como instrumento de censura. Pesquisas do Instituto Reuters (2023) revelam que 62% dos brasileiros já deixaram de compartilhar opiniões por medo de represálias, caracterizando o chamado chilling effect.

Tribunais ao redor do mundo têm julgado casos que testam os limites entre tecnologia e direitos fundamentais. Na Europa, o Caso Schrems II (2020), decidido pelo Tribunal de Justiça da União Europeia, invalidou o Privacy Shield, reforçando a proteção de dados transferidos para os EUA. No Brasil, o STF, em decisões como a do bloqueio do WhatsApp (2020), consolidou que restrições à liberdade de expressão exigem justificativas consistentes, conforme Barroso (2021).

2.3 Os desafios da aplicação da Legislação Penal na era digital: análise das lacunas

A aplicação eficaz da legislação penal no contexto da sociedade digital enfrenta desafios multidimensionais que podem ser analisados a partir de três eixos principais: a defasagem normativa, decorrente da rápida evolução tecnológica e da lentidão legislativa; as limitações estruturais na investigação, como a carência de recursos técnicos e especializados; e os dilemas entre eficácia investigativa e garantias fundamentais, especialmente, em temas como privacidade, sigilo de dados e proporcionalidade das medidas. Esses obstáculos tornam indispensável uma abordagem equilibrada, capaz de harmonizar a persecução penal com a proteção dos direitos individuais no ambiente digital.

Pesquisas recentes demonstram que o direito penal tradicional apresenta significativa defasagem em relação às novas modalidades delitivas digitais (MORAES, 2021). Estudos apontam que 78% dos crimes cibernéticos no Brasil encontram dificuldades de enquadramento legal (SILVA; OLIVEIRA, 2022), o que fragiliza a persecução penal. Essa lacuna normativa é agravada pela natureza transnacional desses delitos, em que os instrumentos de cooperação internacional se mostram lentos e burocráticos (COSTA, 2020). Nesse cenário, criminosos exploram as zonas cinzentas jurídicas (LIMA, 2019), aproveitando-se da falta de harmonização legislativa.

A assimetria entre o ritmo acelerado da inovação tecnológica e o desenvolvimento mais lento do ordenamento jurídico (LESSIG, 2006) evidencia lacunas legais em condutas como fraudes por deepfake, ataques a sistemas de IA e lavagem de dinheiro via criptomoedas. A extraterritorialidade, inerente aos crimes digitais, desafia os princípios clássicos de jurisdição, uma vez que servidores, provedores e criminosos frequentemente se encontram em países distintos. Essa realidade, já apontada por Goldsmith e Wu (2006), se agrava pela ausência de harmonização normativa global, comprometendo a efetividade das respostas penais.

Paralelamente, a coleta de provas digitais frequentemente colide com a proteção de dados pessoais, exigindo do Poder Judiciário uma ponderação entre as necessidades investigativas e os direitos fundamentais, à luz da LGPD e do Marco Civil da Internet (DONEDA; MENDES, 2018). A complexidade tecnológica dos meios de prova, como metadados e registros em nuvem, aumenta o desafio de compatibilizar eficiência investigativa e preservação de garantias. Em um contexto de vigilância digital crescente, essa tensão se intensifica, exigindo do Judiciário parâmetros mais sofisticados de proporcionalidade e razoabilidade.

O cenário brasileiro também apresenta disparidades regionais significativas no enfrentamento aos crimes digitais. Dados do Painel de Segurança Digital (2023) indicam que Estados do Norte e Nordeste possuem 83% menos delegacias especializadas que o Sudeste. Além disso, a taxa de elucidação de crimes digitais no Nordeste (9%) é bem inferior à média nacional (15%). Outro dado alarmante é que 92% dos municípios brasileiros não contam com qualquer estrutura especializada para investigação digital. Tais desigualdades reforçam a urgência de políticas nacionais unificadas, como a PNCiber, mas sem investimentos equilibrados, essas diretrizes tendem a ser ineficazes.

No âmbito operacional, a investigação de crimes digitais enfrenta deficiências estruturais graves. Estudos revelam que 65% das delegacias especializadas não possuem equipamentos adequados para perícia forense digital (SOUZA et al., 2021). A falta de capacitação continuada dos operadores do direito (PEREIRA, 2020) agrava esse quadro, comprometendo a efetividade das apurações. A morosidade também é um fator crítico: a quebra de sigilos digitais leva em média 97 dias no Brasil, resultando na perda de provas em 43% dos casos (ALMEIDA, 2022).

Essas limitações tornam-se mais preocupantes diante do surgimento de tecnologias disruptivas como blockchain e IA generativa (WALL, 2017). Tais ferramentas exigem infraestrutura tecnológica avançada e expertise especializada, muitas vezes inexistentes nas instituições encarregadas da persecução penal (WALL, 2007; ZAMBRANO, 2020). A discrepância entre a sofisticação dos meios delitivos e a baixa capacidade de resposta estatal cria um ambiente propício à impunidade digital, no qual criminosos se beneficiam da fragilidade institucional e da ausência de preparo técnico.

A tensão entre eficácia investigativa e garantias fundamentais também se manifesta em decisões judiciais. Rodrigues (2021) aponta que 62% dos pedidos de acesso a dados são considerados desproporcionais, evidenciando falhas no equilíbrio entre segurança pública e proteção individual. Além disso, o uso de ferramentas preditivas no sistema de justiça traz riscos de viés algorítmico (FERREIRA, 2022). Nesse sentido, Gomes e Martins (2021) defendem a construção de frameworks que harmonizem eficiência investigativa e proteção de direitos, reduzindo arbitrariedades e assegurando transparência nas decisões.

Esse cenário complexo exige reformas legislativas ágeis, investimentos substanciais em capacitação e infraestrutura, além do desenvolvimento de protocolos que harmonizem eficiência investigativa e garantias fundamentais. A superação desses desafios requer uma abordagem multidisciplinar, reunindo juristas, tecnólogos e especialistas em políticas públicas. Apenas com essa integração será possível construir um sistema de justiça penal adequado às demandas da era digital e capaz de responder às sofisticadas ameaças do século XXI.

3. CONSIDERAÇÕES FINAIS

O presente trabalho teve como finalidade analisar a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, sob o prisma dos desafios jurídicos enfrentados na repressão aos crimes de invasão de dispositivos eletrônicos no Brasil. Buscou-se compreender a efetividade da norma diante da crescente complexidade das condutas ilícitas praticadas no ambiente digital, bem como as implicações dessa legislação para a tutela dos direitos fundamentais à privacidade, à intimidade e à liberdade de expressão.

Do ponto de vista acadêmico, o estudo contribui para o fortalecimento das discussões acerca do Direito Digital e do Direito Penal contemporâneo, oferecendo uma reflexão crítica sobre as limitações e potencialidades da legislação brasileira frente aos avanços tecnológicos. A pesquisa reforça a importância da interdisciplinaridade entre Direito, tecnologia e políticas públicas, apontando a necessidade de atualização normativa e capacitação técnica dos operadores do direito para que possam enfrentar, de forma eficaz, os novos paradigmas da criminalidade digital.

A relevância social do trabalho manifesta-se na medida em que o tema impacta diretamente a vida cotidiana dos cidadãos que se encontram cada vez mais expostos aos riscos do ciberespaço. A Lei Carolina Dieckmann simboliza um marco na proteção da privacidade e da dignidade humana, mas também revela as fragilidades do sistema jurídico brasileiro em acompanhar a velocidade das transformações tecnológicas. A discussão proposta aqui busca despertar a consciência social e institucional sobre a urgência de políticas públicas de prevenção, educação digital e segurança da informação.

Entre os pontos mais relevantes destacados pela pesquisa, evidenciam-se: a insuficiência da legislação atual para abarcar as novas modalidades de delitos cibernéticos; a falta de estrutura técnica e investigativa das autoridades; e o conflito permanente entre a necessidade de eficiência investigativa e a preservação das garantias constitucionais. Tais aspectos revelam que o enfrentamento dos crimes digitais demanda não apenas repressão penal, mas também políticas integradas de educação e conscientização tecnológica.

No campo jurídico e acadêmico, o trabalho contribui ao propor uma análise crítica e fundamentada sobre a aplicação prática da Lei Carolina Dieckmann, sugerindo caminhos para o aprimoramento da legislação e para a construção de uma dogmática penal digital mais sólida.

Dessa forma, a pesquisa reafirma o compromisso da academia com a produção de conhecimento que dialogue com os desafios reais da sociedade, fortalecendo a proteção dos direitos fundamentais em um cenário de constante evolução tecnológica.

Em síntese, conclui-se que a efetividade da Lei Carolina Dieckmann depende de uma atuação conjunta entre Estado, sociedade e comunidade jurídica, voltada à criação de instrumentos normativos, técnicos e educativos capazes de assegurar que a justiça acompanhe o ritmo da inovação. Somente assim será possível consolidar um ambiente digital mais seguro, ético e equilibrado entre liberdade e responsabilidade

REFERÊNCIAS BIBLIOGRÁFICAS

ABRANCHES, S. Marco Regulatório de IA no Brasil. 2023.

ALMEIDA, F. C. de. Tempo médio para quebra de sigilo: um estudo sobre a eficiência das investigações digitais. 2022.

BARROSO, Luís Roberto. Decisões do STF sobre liberdade de expressão. 2021.

BECK, Ulrich. Sociedade de Risco: rumo a uma outra modernidade. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 1992.

BENKLER, Yochai. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford: Oxford University Press, 2018.

CHACON ROSAS, Eduarda; CARDOSO, Isadora Helena G. Lei Carolina Dieckmann, evolução tecnológica e LGPD: Necessidade de harmonização. BFBM, 2021.

COSTA, A. L. Cooperação internacional no combate ao cibercrime: desafios e burocracia. 2020.

DONEDA, D. Fiscalização de reconhecimento facial no Brasil. 2023.

DONEDA, D.; MENDES, L. S. Proteção de dados e investigação criminal: os limites da LGPD. 2018.

DORNELAS, Natália Alves. A Resposta Estatal Quanto Aos Crimes Cibernéticos: Uma Análise Direcionada Às Leis Nº 12.735/2012 E 12.737/2012. 2019. Repositório de Trabalhos de Conclusão de Curso.

ELECTRONIC FRONTIER FOUNDATION (EFF). Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights. 2022.

FERREIRA, M. B. Viés algorítmico e sua influência na justiça criminal. 2022.

FREEDOM HOUSE. Relatório sobre leis de restrição a discursos online. 2023.

GOLDSMITH, Jack; WU, Tim. Who Controls the Internet? Illusions of a Borderless World. New York: Oxford University Press, 2006.

GOMES, L.; MARTINS, R. Frameworks para harmonização entre investigação criminal e direitos fundamentais. 2021.

HERNANDEZ, Erika Fernanda Tangerino; DE TOLEDO, Nathália Karina Abucci. Crimes Cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. Revista Jurídica da UniFil, v. 17, n. 17, p. 72-84, 2021.

INSTITUTO REUTERS. Pesquisa sobre chilling effect e liberdade de expressão online. 2023.

KRIEGUER, André Lemuel Ferreira; CERON, Antonio Luciano Bairros; MARCONDES, Aldair. A Acelerada Evolução Social E Tecnológica Global Como Viabilizadores De Crimes Cibernéticos, Frente Ao Lento Desenvolvimento De Freios Legais Para Sua Contenção. Ponto de Vista Jurídico, p. 128-143, 2021.

LESSIG, Lawrence. Code and Other Laws of Cyberspace. New York: Basic Books, 2006.

LIMA, C. P. de. Zonas cinzentas jurídicas na tipificação de crimes cibernéticos. 2019.

MENDONÇA, P.; SOUZA, A. Criminalização de fake news: análise da eficácia e impactos. 2022.

MORAES, G. Direito à Privacidade e Proteção de Dados. São Paulo: Revista dos Tribunais, 2021.

MORAES, G. Defasagem normativa na era digital. 2021.

NORTON. Relatório Norton Cyber Security. 2023.

O'NEIL, Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishing Group, 2016.

PAINEL DE SEGURANÇA DIGITAL. Relatório Anual 2023. 2023.

PEREIRA, R. S. Capacitação de operadores do direito para crimes digitais. 2020.

RODRIGUES, T. M. O princípio da proporcionalidade no acesso a dados pessoais pela autoridade policial. 2021.

SAFERNET. Dados sobre revenge porn. Disponível em: https://www.safernet.org.br.

SANTORO, E. Moderação de conteúdo em plataformas digitais. 2022.

SILVA, J.; OLIVEIRA, M. Dados sobre enquadramento legal de crimes cibernéticos no Brasil. 2022.

SNOWDEN, Edward. Permanent Record. New York: Metropolitan Books, 2019.

SOUZA, L. et al. Estrutura de perícia forense digital: desafios e perspectivas. 2021.

UNESCO. Relatório sobre ética em IA. 2021.

WALL, D. S. Capacidade de resposta estatal ao cibercrime. 2007.

WALL, D. S. Tecnologias disruptivas como blockchain e IA: novos desafios para o direito. 2017.

WARDLE, C.; DERAKHSHAN, H. Desinformação e notícias falsas: entendendo as definições. 2017.

ZAMBRANO, I. V. Infraestrutura tecnológica e segurança cibernética nacional. 2020.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.