II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA I

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

Coordenadores: Camila Martins de Oliveira e Gabriela Emanuele de Resende – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia
ISBN: 978-65-5274-383-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Justiça social e tecnológica em tempos de incerteza.
1. Direito do Futuro. 2. Justiça Social. 3. Justiça Tecnológica. I. II Encontro Nacional de Direito do Futuro (1:2025 : Belo Horizonte, MG).

CDU: 34

Dom Helder
CENTRO UNIVERSITÁRIO

II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA I

Apresentação

O II Encontro Nacional de Direito do Futuro (II ENDIF), organizado pelo Centro Universitário Dom Helder com apoio técnico do Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, reafirma-se como um espaço qualificado de produção, diálogo e circulação do conhecimento jurídico, reunindo a comunidade científica em torno de um propósito comum: pensar, com rigor metodológico e sensibilidade social, os caminhos do Direito diante das transformações que marcam o nosso tempo. Realizado nos dias 09 e 10 de outubro de 2025, em formato integralmente on-line, o evento assumiu como tema geral "Justiça social e tecnológica em tempos de incerteza", convidando pesquisadoras e pesquisadores a enfrentar criticamente os impactos da inovação tecnológica, das novas dinâmicas sociais e das incertezas globais sobre as instituições jurídicas e os direitos fundamentais.

Nesta segunda edição, os números evidenciam a força do projeto acadêmico: 408 trabalhos submetidos, com a participação de 551 pesquisadoras e pesquisadores, provenientes de 21 Estados da Federação, culminando na organização de 31 e-books, que ora se apresentam à comunidade científica. Essa coletânea traduz, em linguagem acadêmica e compromisso público, a vitalidade de uma pesquisa jurídica que não se limita a descrever problemas, mas busca compreendê-los, explicar suas causas e projetar soluções coerentes com a Constituição, com os direitos humanos e com os desafios contemporâneos.

A publicação dos 31 e-books materializa um processo coletivo que articula pluralidade temática, densidade teórica e seriedade científica. Os textos que compõem a coletânea passaram por avaliação acadêmica orientada por critérios de qualidade e imparcialidade, com destaque para o método double blind peer review, que viabiliza a análise inominada dos trabalhos e exige o exame por, no mínimo, dois avaliadores, reduzindo subjetividades e preferências ideológicas. Essa opção metodológica é, ao mesmo tempo, um gesto de respeito à ciência e uma afirmação de que a pesquisa jurídica deve ser construída com transparência, responsabilidade e abertura ao escrutínio crítico.

O II ENDIF também se insere em uma trajetória institucional já consolidada: a primeira edição, realizada em junho de 2024, reuniu centenas de pesquisadoras e pesquisadores e resultou na publicação de uma coletânea expressiva, demonstrando que o Encontro se consolidou, desde o início, como um dos maiores eventos científicos jurídicos do país. A

continuidade do projeto, agora ampliada em escopo e capilaridade, reafirma a importância de se fortalecer ambientes acadêmicos capazes de integrar graduação e pós-graduação, formar novas gerações de pesquisadoras e pesquisadores e promover uma cultura jurídica comprometida com a realidade social.

A programação científica do evento, organizada em painéis temáticos pela manhã e Grupos de Trabalho no período da tarde, foi concebida para equilibrar reflexão teórica, debate público e socialização de pesquisas. Nos painéis, temas como inteligência artificial e direitos fundamentais, proteção ambiental no sistema interamericano, proteção de dados e herança digital foram tratados por especialistas convidados, em debates que ampliam repertórios e conectam a produção acadêmica aos dilemas concretos vividos pela sociedade.

A programação científica do II ENDIF foi estruturada em dois dias, 09 e 10 de outubro de 2025, combinando, no período da manhã, painéis temáticos com exposições de especialistas e debates, e, no período da tarde, sessões dos Grupos de Trabalho. No dia 09/10 (quinta-feira), após a abertura, às 09h, realizou-se o Painel I, dedicado aos desafios da atuação processual diante da inteligência artificial ("Inteligencia artificial y desafios de derechos fundamentales en el marco de la actuación procesal"), com exposição de Andrea Alarcón Peña (Colômbia) e debate conduzido por Caio Augusto Souza Lara. Em seguida, às 11h, ocorreu o Painel II, voltado à proteção ambiental no Sistema Interamericano, abordando a evolução da OC-23 ao novo marco da OC-32, com participação de Soledad Garcia Munoz (Espanha) e Valter Moura do Carmo como palestrantes, sob coordenação de Ricardo Stanziola Vieira. No período da tarde, das 14h às 17h, desenvolveram-se as atividades dos Grupos de Trabalho, em ambiente virtual, com apresentação e discussão das pesquisas aprovadas.

No dia 10/10 (sexta-feira), a programação manteve a organização: às 09h, foi realizado o Painel III, sobre LGPD e a importância da proteção de dados na sociedade de vigilância, com exposições de Laís Furuya e Júlia Mesquita e debate conduzido por Yuri Nathan da Costa Lannes; às 11h, ocorreu o Painel IV, dedicado ao tema da herança digital e à figura do inventariante digital, com apresentação de Felipe Assis Nakamoto e debate sob responsabilidade de Tais Mallmann Ramos. Encerrando o evento, novamente no turno da tarde, das 14h às 17h, seguiram-se as sessões dos Grupos de Trabalho on-line, consolidando o espaço de socialização, crítica acadêmica e amadurecimento das investigações apresentadas.

Ao tornar públicos estes 31 e-books, o II ENDIF reafirma uma convicção essencial: não há futuro democrático para o Direito sem pesquisa científica, sem debate qualificado e sem compromisso com a verdade metodológica. Em tempos de incerteza — tecnológica, social,

ambiental e institucional —, a pesquisa jurídica cumpre um papel civilizatório: ilumina problemas invisibilizados, questiona estruturas naturalizadas, qualifica políticas públicas, tensiona o poder com argumentos e oferece horizontes normativos mais justos.

Registramos, por fim, nosso reconhecimento a todas e todos que tornaram possível esta obra coletiva — autores, avaliadores, coordenadores de Grupos de Trabalho, debatedores e equipe organizadora —, bem como às instituições e redes acadêmicas que fortalecem o ecossistema da pesquisa em Direito. Que a leitura desta coletânea seja, ao mesmo tempo, um encontro com o que há de mais vivo na produção científica contemporânea e um convite a seguir construindo, com coragem intelectual e responsabilidade pública, um Direito à altura do nosso tempo.

Belo Horizonte-MG, 16 de dezembro de 2025.

Prof. Dr. Paulo Umberto Stumpf – Reitor do Centro Universitário Dom Helder

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação do Centro Universitário Dom Helder

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa do Centro Universitário Dom Helder

ANOMIA VIRTUAL: OS DESAFIOS DO DIREITO PENAL BRASILEIRO FRENTE AOS CIBERCRIMES

VIRTUAL ANOMIA; THE CHALLENGES OF BRAZILIAN CRIMINAL LAW IN THE FACE OF CYBERCRIMES

Nikoly Karla Santos

Resumo

O presente trabalho analisa os desafios enfrentados pelo Direito Penal brasileiro diante do aumento dos cibercrimes. A pesquisa examina a adequação das normas vigentes — com ênfase na Lei nº 12.737/2012 (Lei Carolina Dieckmann), no Marco Civil da Internet (Lei nº 12.965/2014) e na Lei nº 14.155/2021 — e discute aspectos relacionados à tipificação, à competência territorial, à cooperação internacional e à produção de prova digital. Conclui-se que, além de aperfeiçoamentos legislativos, o enfrentamento eficaz dos cibercrimes exige capacitação técnica, fortalecimento de estruturas investigativas e maior integração entre órgãos nacionais e internacionais.

Palavras-chave: Cibercrimes, Direito penal, Marco civil, Lei carolina dieckmann, Cooperação internacional

Abstract/Resumen/Résumé

This paper examines the challenges faced by Brazilian Criminal Law in addressing cybercrimes. It analyzes the current legal framework — notably Law 12.737/2012 (Carolina Dieckmann Law), the Brazilian Civil Rights Framework for the Internet (Law 12.965/2014) and Law 14.155/2021 — and discusses issues of typification, territorial jurisdiction, international cooperation and digital evidence. The study concludes that effectively combating cybercrime requires both legislative improvements and investments in technical training, investigative capacity and international collaboration.

Keywords/Palabras-claves/Mots-clés: Cybercrimes, Criminal law, Marco civil, Carolina dieckmann, International cooperation

ANOMIA VIRTUAL: OS DESAFIOS DO DIREITO PENAL BRASILEIRO FRENTE AOS CIBERCRIMES

VIRTUAL ANOMIA: THE CHALLENGES OF BRAZILIAN CRIMINAL LAW IN THE FACE OF CYBERCRIMES

Nikoly Karla Santos

RESUMO

O presente trabalho analisa os desafios enfrentados pelo Direito Penal brasileiro diante do aumento dos cibercrimes. A pesquisa examina a adequação das normas vigentes — com ênfase na Lei nº 12.737/2012 (Lei Carolina Dieckmann), no Marco Civil da Internet (Lei nº 12.965/2014) e na Lei nº 14.155/2021 — e discute aspectos relacionados à tipificação, à competência territorial, à cooperação internacional e à produção de prova digital. Conclui-se que, além de aperfeiçoamentos legislativos, o enfrentamento eficaz dos cibercrimes exige capacitação técnica, fortalecimento de estruturas investigativas e maior integração entre órgãos nacionais e internacionais.

Palavras-chave: Cibercrimes. Direito Penal. Marco Civil. Lei Carolina Dieckmann. Cooperação internacional.

Abstract/Resumen/Résumé

This paper examines the challenges faced by Brazilian Criminal Law in addressing cybercrimes. It analyzes the current legal framework — notably Law 12.737/2012 (Carolina Dieckmann Law), the Brazilian Civil Rights Framework for the Internet (Law 12.965/2014) and Law 14.155/2021 — and discusses issues of typification, territorial jurisdiction, international cooperation and digital evidence. The study concludes that effectively combating cybercrime requires both legislative improvements and investments in technical training, investigative capacity and international collaboration.

Keywords/Palabras-claves/Mots-clés: Cybercrimes. Criminal Law. Marco Civil. Carolina Dieckmann. International Cooperation.

1. CONSIDERAÇÕES INICIAIS

O presente trabalho aborda a complexa relação entre o Direito Penal e os cibercrimes no contexto brasileiro. A pesquisa analisa como as estruturas tradicionais da legislação penal enfrentam os desafios impostos por delitos praticados em ambiente digital, como fraudes, invasões de dispositivos e crimes contra a honra. O objetivo é discutir a eficácia das normas vigentes e as dificuldades encontradas na persecução penal desses crimes.

A relevância do tema é inquestionável diante da crescente digitalização da sociedade, que, ao mesmo tempo em que trouxe inúmeros benefícios, também criou um novo campo para a prática de ilícitos. O Brasil, sendo um dos principais alvos de ataques cibernéticos, enfrenta prejuízos bilionários e um aumento constante no número de vítimas, o que evidencia a urgência de uma resposta jurídica adequada e eficiente. A velocidade da evolução tecnológica supera a capacidade de adaptação do sistema jurídico, gerando um cenário de insegurança e impunidade que precisa ser combatido.

Os desafios para o Direito Penal são imensos, desde a dificuldade de identificar a autoria dos crimes devido ao anonimato proporcionado pela rede, até questões complexas de competência e jurisdição em delitos transnacionais. A legislação, embora tenha avançado com marcos como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e o Marco Civil da Internet (Lei nº 12.965/2014), ainda se mostra insuficiente para abranger todas as nuances das novas modalidades criminosas, exigindo uma constante reflexão sobre a necessidade de novas tipificações e de uma estrutura investigativa mais robusta.

No tocante à metodologia da pesquisa, o presente resumo expandido utilizou, com base na classificação de Gustin, Dias e Nicácio (2020), a vertente metodológica jurídico-social. Com relação ao tipo genérico de pesquisa, foi escolhido o tipo jurídico-projetivo. Por sua vez, o raciocínio desenvolvido na pesquisa foi predominantemente dialético. Quanto ao gênero de pesquisa, adotou-se a pesquisa teórica-bibliográfica.

2. DOS CIBERCRIMES: CONCEITO, CLASSIFICAÇÃO E O CENÁRIO ATUAL

Para compreender o impacto dos cibercrimes, é fundamental, primeiro, defini-los. A doutrina classifica os crimes cibernéticos de duas formas principais: próprios (ou puros) e impróprios (ou impuros). Os crimes próprios são aqueles que só podem ser cometidos no ambiente digital, tendo como bem jurídico tutelado a própria segurança da informação. Já os crimes impróprios são delitos comuns, já previstos no Código Penal, mas que utilizam o ambiente digital como meio para sua execução.

A distinção é crucial, pois, como aponta Guilherme de Souza Nucci, a aplicação da lei penal deve ser precisa. Sobre a invasão de dispositivo informático (art. 154-A), o autor esclarece que o objetivo da norma é proteger a privacidade e a intimidade da pessoa, e não o dispositivo em si. O crime se configura ao "invadir, com o fim de obter, adulterar ou destruir dados ou informações [...] sem autorização expressa ou tácita do titular do dispositivo" (NUCCI, 2023, p. 781). Isso demonstra que o foco do legislador foi a proteção dos dados e da privacidade violada, um bem jurídico personalíssimo.

O cenário atual, no entanto, demonstra uma sofisticação e um volume alarmantes. Relatórios de segurança, como o da Fortinet, indicam que o Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos apenas em 2022, posicionando-se como o segundo país mais atingido na América Latina. Essa estatística alarmante reflete a transposição da criminalidade comum para o ambiente virtual, potencializada pela sensação de impunidade. Sobre essa evolução, Ronaldo Lemos destaca a velocidade da mudança:

> A tecnologia digital transformou-se em um sistema nervoso para a sociedade, mediando desde as relações pessoais até as transações comerciais mais complexas. Essa onipresença, no entanto, expõe vulnerabilidades que são exploradas por agentes maliciosos de formas cada vez mais criativas, exigindo do Direito uma capacidade de adaptação que ele historicamente não possui.
>
> (LEMOS, 2021, p. 45).

Essa "falta de adaptação" mencionada por Lemos é sentida na prática. A popularização de golpes como o phishing (pesca de dados) e o estelionato sentimental, praticado por meio de aplicativos de relacionamento, expõe a vulnerabilidade de cidadãos comuns. Conforme ressalta o especialista Luiz Augusto D'Urso, "o criminoso digital se aproveita da engenharia social, manipulando a confiança da vítima para obter vantagens ilícitas, o que torna a prevenção tão importante quanto a repressão". Essa realidade fática impõe ao sistema de justiça criminal a

necessidade urgente de se modernizar, não apenas na legislação, mas principalmente na capacidade investigativa e na educação digital da população.

3. A RESPOSTA DO DIREITO PENAL BRASILEIRO E SEUS DESAFIOS

A aplicação do Direito Penal aos cibercrimes no Brasil é marcada por uma legislação fragmentada e por desafios processuais significativos. A principal norma de referência, a Lei nº 12.737/2012 (Lei Carolina Dieckmann), foi um marco, mas surgiu de forma reativa a um caso de grande repercussão midiática. Como adverte Túlio Vianna, "legislar no calor do momento pode gerar leis casuísticas e com lacunas técnicas, que se mostram insuficientes para a complexidade do fenômeno que pretendem regular" (VIANNA, 2018, p. 98). A referida lei, por exemplo, não abrange de forma clara a extorsão digital (ransomware), um dos crimes que mais crescem atualmente.

Para suprir essas lacunas, o Judiciário recorre a tipos penais já existentes, em uma complexa atividade de interpretação. A Lei nº 14.155/2021, por exemplo, foi um avanço importante ao qualificar os crimes de furto e estelionato quando praticados por meio eletrônico, com penas mais severas. Contudo, a questão da competência territorial permanece como um dos maiores entraves. O Superior Tribunal de Justiça (STJ), no Conflito de Competência nº 187.276/DF, firmou o entendimento de que, nos casos de estelionato praticado por meio de redes sociais, a competência deve ser a do local do domicílio da vítima, buscando facilitar o acesso à justiça. No entanto, a definição ainda gera debates, especialmente em crimes com múltiplas vítimas em diferentes estados.

Além disso, a transnacionalidade do crime cibernético esbarra nas barreiras da soberania. Um criminoso pode estar na Ásia, usando um servidor na Europa, para atacar uma vítima no Brasil, tornando a investigação e a punição extremamente complexas. A cooperação jurídica internacional, embora existente, é frequentemente lenta e burocrática, como descreve Marcel Leonardi:

> O crime cibernético não respeita fronteiras. Um ataque pode ser lançado de um país, passar por servidores em outros três e atingir uma vítima em um quarto. Essa pulverização geográfica cria um pesadelo jurisdicional, onde a cooperação internacional

> não é apenas desejável, mas a única ferramenta possível para uma persecução penal minimamente eficaz.
>
> (LEONARDI, 2019, p. 212).

A recente adesão do Brasil à Convenção de Budapeste sobre o Cibercrime, em 2023, é uma esperança para agilizar essa colaboração, padronizando procedimentos e facilitando o intercâmbio de provas. Contudo, sua implementação prática ainda é um desafio que depende da criação de estruturas internas e da capacitação dos agentes públicos. Por fim, a produção da prova digital exige conhecimento técnico especializado e um rigoroso respeito à cadeia de custódia, sob pena de ser invalidada em juízo, resultando na impunidade do criminoso.

4. CONSIDERAÇÕES FINAIS

Ao final deste estudo, fica evidente que a era digital impôs ao Direito Penal brasileiro desafios de uma magnitude sem precedentes. A análise da legislação e dos posicionamentos doutrinários e jurisprudenciais revela um sistema jurídico que corre para se adaptar a uma realidade tecnológica em constante e veloz transformação. A resposta legislativa, embora tenha marcos importantes, ainda se mostra reativa e fragmentada, lutando para acompanhar a sofisticação e a diversidade dos crimes cibernéticos.

O desenvolvimento deste trabalho permitiu compreender que os maiores obstáculos não residem apenas na tipificação de novas condutas, mas, sobretudo, nas questões processuais. A dificuldade em determinar a autoria, a competência e em obter provas válidas em um ambiente sem fronteiras físicas demonstra que a eficácia da repressão aos cibercimes depende tanto de leis modernas quanto de uma estrutura investigativa e judicial preparada, com investimento em tecnologia e cooperação internacional ágil.

Portanto, conclui-se que o caminho para um combate efetivo aos crimes cibernéticos no Brasil passa por uma abordagem multifacetada. É necessário não apenas continuar aprimorando o arcabouço legal, mas também fortalecer as delegacias especializadas, promover a capacitação contínua dos operadores do Direito e consolidar os mecanismos de colaboração entre as nações.

Somente assim será possível reduzir a sensação de impunidade que ainda impera no ambiente virtual e garantir a proteção dos cidadãos na era digital.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos. *Diário Oficial da União*, Brasília, DF, 3 dez. 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Código Penal para agravar as penas para crimes de furto e estelionato quando praticados por meio eletrônico ou com uso de dispositivo eletrônico. *Diário Oficial da União*, Brasília, DF, 28 maio 2021.

BRASIL. **Decreto nº 11.491, de 21 de setembro de 2023.** Promulga a Convenção de Budapeste sobre o Cibercrime. *Diário Oficial da União*, Brasília, DF, 22 set. 2023.

FORTINET. **Relatório de Ameaças Cibernéticas 2022.** Disponível em: https://www.fortinet.com/. Acesso em: 20 set. 2025.

LEMOS, Ronaldo. *Direito, Tecnologia e Sociedade.* 2. ed. São Paulo: Editora Alfa, 2021.

LEONARDI, Marcel. *Fundamentos de Direito Digital.* 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

NUCCI, Guilherme de Souza. *Código Penal Comentado.* 23. ed. Rio de Janeiro: Forense, 2023.

VIANNA, Túlio. *Legislação Penal Especial.* Belo Horizonte: Del Rey, 2018.

ZANIN, Diego. **Crimes Cibernéticos e Investigação Digital no Brasil: desafios e perspectivas.** *Revista Brasileira de Ciências Criminais*, v. 30, n. 179, p. 155-182, 2022.