

CRIMES CIBERNÉTICOS: LIMITES E POSSIBILIDADES DO DIREITO PENAL DIGITAL

CYBERCRIME: LIMITS AND POSSIBILITIES OF DIGITAL CRIMINAL LAW

DELITOS CIBERNÉTICOS: LÍMITES Y POSIBILIDADES DEL DERECHO PENAL DIGITAL

**Adriano Fábio Cordeiro da Silva¹, Julia Dias Portela², Adriano Rodrigues de Moraes³,
Wendelson Pereira Pessoa⁴, Vicente Ferreira Júnior⁵, Mario Marrathma Lopes de Oliveira⁶,
Francine Nunes Ávila⁷, Renan Beserra Pereira da Silva⁸, Arnon Alves da Silva⁹, Marcos Vinícius
Ferreira Corrêa¹⁰, Giselle Batista Leite¹¹**

DOI: 10.54899/dcs.v23i86.4199

Recibido: 05/12/2025 | Aceptado: 30/12/2025 | Publicación en línea: 09/01/2026.

RESUMO

A presente pesquisa teve como objetivo analisar os limites e possibilidades do Direito Penal frente aos crimes cibernéticos, identificando desafios legais, lacunas normativas e estratégias de prevenção e repressão no ambiente digital. Para tanto, adotou-se uma revisão integrativa da literatura, selecionando seis artigos nacionais e internacionais, com base nas diretrizes PICO e PRISMA, com foco em publicações de 2021 a 2024, em português, completas e acessíveis nas bases SciELO, Google Acadêmico e DOAJ. Os resultados demonstraram que, embora legislações como a Lei nº 12.737/2012, a Lei nº 13.810/2019 e a LGPD representem avanços significativos, persistem lacunas quanto à eficácia das normas, capacitação das autoridades e cooperação internacional. Observou-se que a complexidade, volatilidade das evidências digitais e transnacionalidade dos crimes cibernéticos exigem abordagens integradas que combinam

¹ Doutor em Direito, Universidade de Pernambuco (UPE), Recife, Pernambuco, Brasil.

E-mail: adrianofabio@hotmail.com

² Graduada em Direito, Estácio de Sá, Rio de Janeiro, Rio de Janeiro, Brasil. E-mail: juliadiasportela@gmail.com

³ Doutorando em Direito Constitucional, Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), São Sebastião do Tocantins, Tocantins, Brasil. E-mail: adrianormorais2010@hotmail.com

⁴ Pós-doutor em Direito, Universidade Federal do Maranhão (UFMA), São Luís, Maranhão, Brasil.

E-mail: wendelson.pessoa@trf1.jus.br

⁵ Bacharel em Ciência da Computação, Universidade de Brasília (UnB), Brasília, Distrito Federal, Brasil.

E-mail: juniorvf@gmail.com

⁶ Mestrando em Direito, Centro Universitário Christus (UniChristus), Fortaleza, Ceará, Brasil.

E-mail: mario@marrathma.com

⁷ Doutora em Diversidade Cultural e Inclusão Social, Universidade Federal do Pampa (UNIPAMPA), Bagé, Rio Grande do Sul, Brasil. E-mail: francineavila@yahoo.com.br

⁸ Especialista em Segurança de Redes de Computadores, Centro Universitário Estácio do Recife, Recife, Pernambuco, Brasil. E-mail: renan.beserra@ufrpe.br

⁹ Mestrando em Agronegócio e Desenvolvimento, Centro Universitário de Adamantina (FAI), Adamantina, São Paulo, Brasil. E-mail: arnonalves.adv@hotmail.com

¹⁰ Doutorando em Ciências Humanas, Universidade Federal de Santa Catarina (UFSC), Florianópolis, Santa Catarina, Brasil. E-mail: mviniciuslege@gmail.com

¹¹ Doutoranda em Proteção dos Direitos Fundamentais, Universidade de Itaúna (UIT), Betim, Minas Gerais, Brasil. E-mail: profgisellebatistaleite@gmail.com

tipificação adequada, unidades especializadas, políticas educativas de segurança digital e colaboração entre países. Conclui-se que o Direito Penal Digital deve ser dinâmico, preventivo e adaptável, equilibrando proteção às vítimas, responsabilização penal e inovação tecnológica.

Palavras-chave: Direito Penal. Crimes Cibernéticos. Digital. Internet. Tecnologias.

ABSTRACT

The objective of this research was to analyze the limits and possibilities of criminal law in relation to cybercrimes, identifying legal challenges, regulatory gaps, and strategies for prevention and repression in the digital environment. To this end, an integrative literature review was conducted, selecting six national and international articles based on the PICO and PRISMA guidelines, focusing on publications from 2021 to 2024, in Portuguese, complete and accessible in the SciELO, Google Scholar, and DOAJ databases. The results showed that, although laws such as Law No. 12,737/2012, Law No. 13,810/2019, and the LGPD represent significant advances, gaps remain in terms of the effectiveness of regulations, training of authorities, and international cooperation. It was observed that the complexity, volatility of digital evidence, and transnational nature of cybercrimes require integrated approaches that combine adequate classification, specialized units, educational policies on digital security, and collaboration between countries. It is concluded that Digital Criminal Law must be dynamic, preventive, and adaptable, balancing victim protection, criminal accountability, and technological innovation.

Keywords: Criminal Law. Cybercrimes. Digital. Internet. Technologies.

RESUMEN

El objetivo de la presente investigación fue analizar los límites y las posibilidades del Derecho Penal frente a los delitos cibernéticos, identificando los retos legales, las lagunas normativas y las estrategias de prevención y represión en el entorno digital. Para ello, se adoptó una revisión integradora de la literatura, seleccionando seis artículos nacionales e internacionales, basados en las directrices PICO y PRISMA, centrados en publicaciones de 2021 a 2024, en portugués, completos y accesibles en las bases SciELO, Google Académico y DOAJ. Los resultados demostraron que, aunque leyes como la Ley n.º 12.737/2012, la Ley n.º 13.810/2019 y la LGPD representan avances significativos, persisten lagunas en cuanto a la eficacia de las normas, la capacitación de las autoridades y la cooperación internacional. Se observó que la complejidad, la volatilidad de las pruebas digitales y la transnacionalidad de los delitos cibernéticos exigen enfoques integrados que combinen una tipificación adecuada, unidades especializadas, políticas educativas de seguridad digital y la colaboración entre países. Se concluye que el Derecho Penal Digital debe ser dinámico, preventivo y adaptable, equilibrando la protección de las víctimas, la responsabilidad penal y la innovación tecnológica.

Palabras clave: Derecho Penal. Delitos Cibernéticos. Digital. Internet. Tecnologías.



Esta obra está bajo una [Licencia Creative Commons Atribución- NoComercial 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUÇÃO

A presente pesquisa aborda o tema dos crimes cibernéticos, delimitando-se à análise dos limites e possibilidades do Direito Penal Digital. O estudo se concentra na forma como o ordenamento jurídico brasileiro tem se adaptado para lidar com infrações cometidas no ambiente virtual, considerando a crescente complexidade das condutas criminosas na internet e a necessidade de respostas legais adequadas.

O tema dos crimes cibernéticos tornou-se central na contemporaneidade devido à expansão do uso da internet, das redes sociais e de sistemas digitais, que criam novas oportunidades para fraudes, invasões de sistemas, crimes contra a privacidade e disseminação de informações falsas. Esse fenômeno exige uma análise detalhada das normas existentes e das estratégias de prevenção, responsabilização e proteção das vítimas.

Diante desse contexto, surge a seguinte situação-problema: até que ponto o Direito Penal Digital é capaz de acompanhar a velocidade das inovações tecnológicas e garantir a responsabilização adequada dos agentes que praticam crimes no ciberespaço? Como o sistema jurídico pode equilibrar a proteção dos direitos fundamentais com a necessidade de punir condutas ilícitas em ambientes digitais?

O objetivo geral desta pesquisa é analisar os limites e as possibilidades do Direito Penal Digital na prevenção e repressão dos crimes cibernéticos. Os objetivos específicos incluem: identificar os principais tipos de crimes cibernéticos e suas características; avaliar a eficácia das normas penais existentes; e discutir propostas de aprimoramento legislativo e operacional no combate a essas infrações.

A relevância deste estudo está na necessidade de compreender as lacunas legais e operacionais do Direito Penal Digital, contribuindo para o fortalecimento da segurança jurídica, a proteção dos direitos fundamentais e o desenvolvimento de políticas públicas mais efetivas para enfrentar a criminalidade virtual. Além disso, a pesquisa busca fornecer subsídios para profissionais do direito, legisladores e acadêmicos interessados em compreender e aprimorar a atuação do Estado diante dos crimes cibernéticos.

MÉTODOS

A presente pesquisa caracteriza-se como uma revisão integrativa, com o objetivo de analisar criticamente os limites e possibilidades do Direito Penal Digital no enfrentamento dos

crimes cibernéticos. A revisão integrativa permite reunir, sintetizar e avaliar estudos e publicações científicas sobre o tema, oferecendo uma visão abrangente do estado da arte, bem como identificando lacunas e tendências na literatura (Lima; Domingues Júnior; Silva, 2024; Lima, 2024a; Lima *et al.*, 2025a; Lima; Domingues; Pimentel Júnior, 2023; Lima *et al.*, 2025b; Lima *et al.*, 2025c).

Para a condução da revisão, foram adotadas as estratégias PICO e as diretrizes do PRISMA, garantindo um procedimento sistemático e transparente na seleção e análise dos artigos. A estratégia PICO permitiu delimitar a população de estudo, o fenômeno de interesse, a comparação, quando pertinente, e os desfechos relacionados às respostas do Direito Penal frente aos crimes cibernéticos. O uso do PRISMA assegurou rigor metodológico, com etapas claras de identificação, triagem, elegibilidade e inclusão dos artigos selecionados.

A busca por artigos foi realizada nas bases de dados SciELO, Google Acadêmico e DOAJ, priorizando publicações em português, completas e disponíveis gratuitamente. Foram incluídos apenas artigos brasileiros, publicados entre 2020 e 2024, que abordassem especificamente o tema dos crimes cibernéticos, Direito Penal Digital ou legislações correlatas, incluindo discussões sobre limites, possibilidades e desafios no contexto brasileiro.

Após a aplicação dos critérios de inclusão e exclusão, foram selecionados 6 artigos que constituíram a base empírica da revisão integrativa. Os estudos escolhidos abordam diferentes perspectivas, incluindo análises teóricas e jurídicas, estudos de caso, reflexões sobre normas e legislações, e discussões sobre práticas de prevenção e responsabilização de crimes digitais.

A análise dos artigos foi realizada de forma qualitativa, com leitura crítica e síntese temática, permitindo a identificação de categorias recorrentes, como: tipos de crimes cibernéticos, eficácia do Direito Penal Digital, lacunas legais, desafios para aplicação prática e propostas de aprimoramento legislativo. Os dados extraídos foram organizados em quadro-resumo, contemplando autores, métodos, objetivos e principais resultados de cada estudo.

Essa abordagem metodológica possibilitou construir uma compreensão abrangente do tema, evidenciando os avanços legislativos, as limitações institucionais e os desafios contemporâneos que envolvem a aplicação do Direito Penal Digital frente à criminalidade virtual no Brasil.

RESULTADOS E ANÁLISE DOS DADOS

A tabela 1 expõe os principais resultados obtidos com a realização da pesquisa.

Tabela 1. Artigos selecionados			
Autor(es)	Método	Objetivo	Resultados
Lopes <i>et al.</i> (2024)	Revisão bibliográfica	Analisar a regulação e resposta jurídica aos crimes cibernéticos no ambiente digital	Identificou que a legislação brasileira (Lei Carolina Dieckmann e Lei nº 13.810/2019) busca atualização, mas enfrenta desafios quanto à eficácia devido à capacitação insuficiente das forças de segurança e necessidade de cooperação internacional. Destacou a importância da LGPD e unidades especializadas em crimes cibernéticos.
Freitas <i>et al.</i> (2023)	Pesquisa qualitativa teórica	Explorar a evolução do Direito Penal brasileiro frente aos crimes cibernéticos	Demonstrou que o ordenamento jurídico evoluiu, oferecendo maior eficiência regulatória, mas ainda apresenta lacunas em políticas preventivas e na adaptação à era digital.
Lima Filho (2021)	Pesquisa bibliográfica	Inserir o Direito Penal no contexto da Quarta Revolução Industrial e analisar crimes cibernéticos	Apontou a necessidade de expansão razoável do Direito Penal, considerando a tecnologia da informação como bem jurídico relevante, e avaliou lacunas legislativas com referência à Convenção de Budapeste e CPI dos Crimes Cibernéticos.
Freitas <i>et al.</i> (2023)	Pesquisa bibliográfica exploratória e descritiva	Examinar o papel do Direito Penal brasileiro no combate aos delitos virtuais	Constatou que a legislação brasileira é insuficiente, com número limitado de tipificações e penas brandas, demonstrando a necessidade de revisão e aprimoramento legal.
Nogueira & Nolasco (2022)	Pesquisa bibliográfica	Analisar os impactos da pandemia de Covid-19 nos crimes cibernéticos e a legislação vigente	Identificou aumento de crimes digitais durante o isolamento social, destacando que a legislação brasileira estabelece punições, mas ainda é insuficiente diante do crescimento da conectividade e complexidade dos delitos.
Hernandez & Toledo (2021)	Revisão bibliográfica	Refletir sobre os efeitos do avanço tecnológico na legislação penal brasileira	Apontou que o Direito Penal vem acompanhando as transformações tecnológicas, mas a evolução constante dos crimes cibernéticos exige mudanças contínuas na tipificação e investigação desses delitos.

Fonte: Dados da pesquisa (2026).

A análise dos resultados das seis pesquisas selecionadas revela que os crimes cibernéticos representam um desafio crescente para o Direito Penal, tanto em nível nacional quanto internacional. Lopes *et al.* (2024) destacam que o ambiente digital, por sua natureza transnacional, dificulta a aplicação das normas penais tradicionais, exigindo cooperação internacional e

atualização constante da legislação. Segundo os autores, leis como a “Carolina Dieckmann” e a Lei nº 13.810/2019 têm buscado atualizar o arcabouço jurídico brasileiro, mas ainda apresentam limitações, especialmente devido à capacitação insuficiente das forças de segurança e à carência de cultura de segurança digital.

Freitas *et al.* (2023) reforçam essa percepção, ao demonstrar que, embora o Direito Penal brasileiro tenha evoluído, persistem lacunas importantes relacionadas à prevenção e ao estímulo a políticas proativas. Eles destacam que o ordenamento jurídico oferece eficiência regulatória em termos de tipificação penal, mas não consegue abarcar completamente as novas modalidades de crimes digitais que surgem com a evolução tecnológica.

Lima Filho (2021) amplia a compreensão ao situar os crimes cibernéticos no contexto da Quarta Revolução Industrial, destacando a necessidade de expandir razoavelmente a proteção do Direito Penal frente às novas tecnologias. Segundo o autor, a tecnologia da informação passou a ser um bem jurídico relevante, que precisa de proteção robusta, mas a legislação ainda não consegue acompanhar totalmente a velocidade das inovações. Nesse sentido, ele reforça a importância de parâmetros internacionais, como a Convenção de Budapeste, para orientar políticas e legislações nacionais.

Freitas *et al.* (2023) identificam que a legislação brasileira, ao lidar com crimes virtuais, apresenta limitações significativas. Embora haja tipificações penais específicas, o número de delitos contemplados é insuficiente, e as penas aplicáveis são, em muitos casos, brandas. Isso gera uma sensação de impunidade e reduz a eficácia da atuação do Estado. Os autores enfatizam que o Direito Penal precisa não apenas tipificar condutas, mas também desenvolver instrumentos que assegurem efetividade na investigação e na persecução penal.

Nogueira & Nolasco (2022) trazem um recorte relevante sobre o impacto da pandemia de Covid-19, que elevou significativamente a exposição de indivíduos ao ambiente digital. Segundo os autores, o isolamento social aumentou a prática de crimes cibernéticos, como estelionato, fraudes eletrônicas e abusos virtuais. Eles destacam que, embora a legislação brasileira preveja punições, o crescimento exponencial de infrações digitais evidencia a necessidade de aprimoramento das normas e da fiscalização, especialmente em contextos de emergência social e tecnológica.

Hernandez & Toledo (2021) reforçam que o avanço tecnológico provoca mudanças significativas no Direito Penal, exigindo adaptações legislativas contínuas. Os autores argumentam que o “admirável mundo novo” do ambiente virtual exige tipificações inovadoras e

mecanismos de investigação mais eficientes. Essa perspectiva evidencia que o Direito Penal não pode ser estático; precisa evoluir de forma dinâmica para acompanhar a sociedade digital.

Outro ponto convergente entre os estudos é a necessidade de especialização. Lopes *et al.* (2024) e Lima Filho (2021) destacam a criação de unidades especializadas em crimes cibernéticos como estratégia essencial para a eficiência da resposta penal. Segundo eles, a complexidade das evidências digitais, muitas vezes voláteis e de difícil rastreamento, exige profissionais capacitados em tecnologia, análise de dados e legislação específica.

A análise também evidencia que as lacunas preventivas são um desafio central. Freitas *et al.* (2023) ressaltam que, embora a legislação tipifique delitos, há escassez de políticas preventivas que eduquem a população sobre segurança digital. Isso é crucial, já que a prevenção e a conscientização diminuem a vulnerabilidade a fraudes e invasões.

Os estudos analisados convergem ainda para a importância da integração entre direito penal e proteção de dados. Lopes *et al.* (2024) destacam que a LGPD não apenas regula o uso de dados pessoais, mas também interfere na prevenção e na tipificação de crimes digitais, evidenciando a interdependência entre legislações penais e de proteção de informações.

Além disso, Freitas *et al.* (2023) e Freitas *et al.* (2023) mostram que a legislação brasileira precisa equilibrar tipificação ampla e proporcionalidade das penas, de modo que condutas graves no ambiente digital recebam resposta adequada, sem banalizar delitos menos prejudiciais.

A questão da jurisdição transnacional também se destaca nos resultados. Lopes *et al.* (2024) enfatizam que os crimes cibernéticos frequentemente ultrapassam fronteiras nacionais, exigindo tratados e convenções internacionais que harmonizem legislações e facilitem a cooperação entre autoridades judiciais e policiais. Esse aspecto é reforçado por Lima Filho (2021), que destaca a Convenção de Budapeste como referência para definir padrões internacionais de combate aos crimes digitais, reduzindo lacunas legais que poderiam ser exploradas por criminosos.

Outro ponto crítico identificado é a fragilidade na capacitação das forças de segurança. Lopes *et al.* (2024) apontam que, sem treinamento especializado em crimes digitais, a investigação de delitos se torna ineficaz. Isso inclui desde a coleta de evidências digitais até a análise de dispositivos e rastreamento de informações, tornando a punição efetiva um desafio significativo.

Freitas *et al.* (2023) complementam que a velocidade das inovações tecnológicas impõe um desafio adicional: enquanto novas modalidades de crimes surgem rapidamente, a atualização

legislativa ocorre de forma lenta. Essa defasagem temporal cria um espaço vulnerável em que criminosos digitais podem agir com relativa impunidade.

A análise dos estudos também evidencia a necessidade de conscientização da população. Lopes *et al.* (2024) e Nogueira & Nolasco (2022) concordam que a educação digital e a formação em segurança da informação são estratégias essenciais para reduzir a incidência de crimes cibernéticos. A prevenção se torna tão importante quanto a repressão, especialmente em um contexto de crescente dependência da tecnologia.

A questão do equilíbrio entre privacidade e segurança é outro ponto recorrente. Lopes *et al.* (2024) destacam que a LGPD estabelece normas de proteção de dados, mas sua efetividade depende da conscientização das organizações e indivíduos. Ao mesmo tempo, a necessidade de investigação criminal exige que as autoridades tenham acesso a informações digitais, gerando tensões entre direitos individuais e interesse público.

Freitas *et al.* (2023) reforçam a importância de tipificar adequadamente as condutas criminosas digitais, evitando a ambiguidade. Eles argumentam que termos vagos ou insuficientemente definidos podem gerar insegurança jurídica, dificultando a atuação de operadores do direito e incentivando condutas ilícitas.

A análise dos estudos também evidencia a relevância da prevenção em tempos de pandemia. Nogueira & Nolasco (2022) identificam que o isolamento social decorrente da Covid-19 aumentou a exposição dos indivíduos ao ambiente digital, ampliando a ocorrência de fraudes, golpes e abusos virtuais. O estudo sugere que legislações mais robustas e ações educativas poderiam minimizar os impactos desses fenômenos.

Hernandez & Toledo (2021) destacam ainda que o ambiente virtual exige constante atualização legislativa. A cada nova tecnologia ou plataforma digital, surgem formas inéditas de conduta ilícita, exigindo que o Direito Penal acompanhe essas mudanças para garantir proteção efetiva à sociedade.

Outro aspecto identificado é a ineficiência das penas atuais. Freitas *et al.* (2023) e Freitas *et al.* (2023) apontam que muitas infrações digitais recebem punições brandas, que não desestimulam a reincidência. Isso evidencia a necessidade de revisar o sistema punitivo, equilibrando proporcionalidade e efetividade.

Por fim, os estudos mostram que a integração entre Direito Penal, políticas preventivas e cooperação internacional é essencial. Lopes *et al.* (2024) sugerem que somente uma abordagem integrada, envolvendo educação, legislação atualizada, capacitação profissional e cooperação

internacional, pode enfrentar eficazmente a complexidade dos crimes cibernéticos.

A pesquisa também evidencia a importância das unidades especializadas em crimes cibernéticos, conforme destacado por Lopes *et al.* (2024) e Freitas *et al.* (2023). Essas unidades são essenciais para o desenvolvimento de perícias digitais, investigação de redes criminosas e rastreamento de fraudes, contribuindo para uma aplicação mais eficiente do Direito Penal.

Além disso, Hernandez & Toledo (2021) chamam atenção para os efeitos revolucionários das legislações digitais. Eles argumentam que, à medida que novas condutas ilícitas surgem, a legislação precisa evoluir rapidamente para contemplar tipificações, penalidades e medidas preventivas adequadas, evitando que lacunas legais sejam exploradas.

Outro ponto crítico observado é a fragilidade da legislação diante da rapidez tecnológica. Freitas *et al.* (2023) destacam que crimes como invasões de sistemas e roubo de dados podem ser cometidos em segundos, enquanto o processo legal ainda é burocrático e lento, criando um descompasso entre ação criminosa e punição.

Nogueira & Nolasco (2022) enfatizam que a pandemia acelerou a digitalização, aumentando a exposição de indivíduos e empresas ao risco cibernético. Eles sugerem que políticas preventivas e campanhas de conscientização são tão importantes quanto o aprimoramento do Direito Penal.

A análise indica ainda que o direito à informação e segurança digital deve ser promovido em paralelo com a repressão penal. Lopes *et al.* (2024) defendem programas educativos para usuários, empresas e órgãos públicos, destacando que a prevenção é um elemento-chave para reduzir a incidência de crimes cibernéticos.

Freitas *et al.* (2023) acrescentam que a tipificação clara de crimes digitais é vital. Quando a legislação apresenta lacunas ou conceitos vagos, os operadores do Direito encontram dificuldades para interpretar e aplicar a lei, comprometendo a eficácia da persecução penal.

Outro aspecto relevante é a necessidade de cooperação internacional. Crimes cibernéticos frequentemente envolvem atores em diferentes países, tornando imprescindível a harmonização de legislações e o compartilhamento de informações entre autoridades, conforme ressaltam Lopes *et al.* (2024) e Lima Filho (2021).

A análise evidencia que a proporcionalidade das penas ainda é um desafio. Muitas infrações digitais são punidas de forma branda, desestimulando a prevenção e não refletindo a gravidade do dano causado, o que reforça a necessidade de revisão das sanções penais.

Hernandez & Toledo (2021) destacam a importância de políticas públicas e marcos

regulatórios atualizados, capazes de acompanhar a rápida evolução tecnológica. Somente uma legislação adaptável pode oferecer proteção adequada às vítimas e segurança jurídica aos operadores do Direito.

Por fim, a síntese dos estudos demonstra que o enfrentamento dos crimes cibernéticos exige uma abordagem multidimensional, que combine atualização legislativa, cooperação internacional, prevenção educacional, capacitação profissional e unidades especializadas. Essa integração entre Direito Penal, políticas de prevenção e colaboração global é essencial para proteger indivíduos, organizações e o sistema jurídico frente aos desafios do ambiente digital.

CONSIDERAÇÕES FINAIS

As considerações finais desta pesquisa evidenciam que os crimes cibernéticos representam um dos maiores desafios do Direito Penal contemporâneo, exigindo atualização constante das normas jurídicas, adaptação dos operadores do Direito e capacitação das forças de segurança. A revisão integrativa mostrou que, apesar dos avanços legislativos no Brasil, como a Lei nº 12.737/2012, a Lei nº 13.810/2019 e a Lei Geral de Proteção de Dados (LGPD), ainda existem lacunas que comprometem a eficácia da persecução penal, especialmente diante da rapidez e complexidade das condutas ilícitas digitais.

Os resultados indicam que a aplicação do Direito Penal no ambiente digital exige estratégias multidimensionais, combinando tipificação adequada dos crimes, criação de unidades especializadas, cooperação internacional e políticas de prevenção e conscientização digital. Estudos como os de Lopes *et al.* (2024), Freitas *et al.* (2023) e Hernandez & Toledo (2021) reforçam que a falta de harmonização legislativa e de capacitação técnica limita a proteção de indivíduos e organizações, tornando o combate a delitos cibernéticos um desafio contínuo e dinâmico.

Além disso, a pesquisa apontou a necessidade de considerar a proporcionalidade das penas e a adaptação das normas tradicionais de Direito Penal aos cenários digitais, respeitando as especificidades do ambiente virtual, como a volatilidade das evidências e a transnacionalidade dos crimes. A conscientização sobre segurança digital e a educação preventiva surgem como ferramentas complementares à repressão penal, contribuindo para reduzir a vulnerabilidade de usuários e instituições.

Dessa forma, conclui-se que o Direito Penal Digital deve se estruturar de maneira

integrada e colaborativa, aliando legislação atualizada, instrumentos de cooperação internacional, capacitação profissional e políticas educativas, a fim de garantir segurança jurídica, proteção às vítimas e efetividade na prevenção e repressão dos crimes cibernéticos. O avanço tecnológico exige que o Direito não apenas reaja, mas antecipe desafios, promovendo um equilíbrio entre inovação digital e responsabilização penal.

REFERÊNCIAS

- FREITAS, Camila Cristina Gonzaga de; GONÇALVES, Jonas Rodrigo; TORRES, Mateus Guimarães. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. *Revista JRG de Estudos Acadêmicos*, v. 6, n. 12, 2023. DOI: <https://doi.org/10.5281/zenodo.7760710>
- FREITAS, Victor Valério Medeiros Siqueira de; SANTOS, Waldiney Batista dos; CURY, Letícia Vivianne Miranda. Crimes virtuais: um olhar sob a ótica do direito penal. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 9, n. 5, 2023. DOI: <https://doi.org/10.51891/rease.v9i5.9868>
- HERNANDEZ, Erika Fernanda Tangerino; TOLEDO, Nathália Karina Abucci de. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. *Revista Jurídica da UniFil*, v. 17, n. 17, 2021.
- LIMA FILHO, Paulo Roberto Aguiar de. O direito penal na quarta revolução industrial: a expansão razoável frente aos crimes cibernéticos. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*, v. 6, n. 10, 2021. DOI: <https://doi.org/10.24861/25265180.v6i10.150>
- LIMA, L. A. de O.; BERNARDY, T. A. dos S.; BALDISSARELLI, J. M.; CERQUEIRA, H. de G.; BRITO, J. R. L.; GOMES, M. O.; CAMPOS, D. F. Gestão Socioambiental, Marketing Verde e Legislação: o Papel do Regulamento Jurídico no Combate às Práticas de Greenwashing nas Organizações. *Revista de Gestão e Secretariado*, [S. l.], v. 16, n. 7, p. e5145, 2025. DOI: 10.7769/gesec.v16i7.5145.
- LIMA, L. A. de O.; JAHNKE, J. F.; JESUS, E. L. de; PEREIRA, R.; RIBEIRO, C. M. G.; PEDRO, A. M. Tecnologias de Informação e Comunicação na Globalização: Conexões, Desigualdades e Transformações Socioculturais. *Revista de Gestão e Secretariado*, [S. l.], v. 16, n. 8, p. e5222, 2025. DOI: 10.7769/gesec.v16i8.5222.
- LIMA, L. A. de O.; PARENTE, A. M. B.; LEIMANN, A. H.; SCHIAVAO, L. J. V.; MAIA, L. A.; SOUSA, F. B. da S.; ARAÚJO, T. S. S.; SOUSA, G. C. Gestão na Saúde Pública: Contribuições da Inteligência Artificial para a Otimização dos Processos e Tomada de Decisões. *Revista de Gestão e Secretariado*, [S. l.], v. 16, n. 9, p. e5243, 2025.
- LIMA, L. A. O. Estigmatização do HIV nas relações e formas de trabalho: Uma revisão integrativa de literatura. *LUMEN ET VIRTUS*, v. 15, p. 1497-1506, 2024. <https://doi.org/10.56238/levv15n38-096>
- LIMA, L. A. O. *et al.* GESTÃO HUMANIZADA EM SAÚDE E SUAS IMPLICAÇÕES

PARA A QUALIDADE DE VIDA NO TRABALHO. LUMEN ET VIRTUS, v. 16, p. 1009-1019, 2025. <https://doi.org/10.56238/levv16n45-027>

LIMA, L. A. O. *et al.* INFORMATIZAÇÃO EM SAÚDE: AVANÇOS TECNOLÓGICO E A MODERNIZAÇÃO NOS SERVIÇOS DE SAÚDE. LUMEN ET VIRTUS, v. 16, p. 5102-5111, 2025. <https://doi.org/10.56238/levv16n48-042>

LIMA, L. A. O. *et al.* Os desafios na formação de profissionais de saúde no Brasil. Brazilian Journal of Implantology and Health Sciences, v. 7, p. 05-15, 2025. <https://doi.org/10.36557/2674-8169.2025v7n5p05-15>

Lima, L. A. O., Domingues Júnior, P. L., & Silva, L. L. (2024). Estresse ocupacional em período pandêmico e as relações existentes com os acidentes laborais: estudo de caso em uma indústria alimentícia. RGO - Revista Gestão Organizacional, 17(1), 34-47. <http://dx.doi.org/10.22277/rgo.v17i1.7484>.

LIMA, L. A. O.; DOMINGUES, P. L.; PIMENTEL JUNIOR, W. Young University Students and the Difficulties they Face in Entering the Job Market in the Municipality of Três Rios, Brazil. INTERNATIONAL JOURNAL OF MANAGERIAL STUDIES AND RESEARCH, v. 11, p. 1, 2023. <http://dx.doi.org/10.20431/2349-0349.1103001>

LOPES, Líliam dos Reis *et al.* Crimes cibernéticos e direito penal: a regulação e a resposta jurídica ao crime no ambiente digital. IOSR Journal of Business and Management (IOSR-JBM), v. 26, n. 11, ser. 8, 2024. DOI: 10.9790/487X-2611080111

NOGUEIRA, Flavio Mirã de Souza; NOLASCO, Loreci Gottschalk. Crimes cibernéticos - desafios para o direito. Revista Jurídica Direito, Sociedade e Justiça, v. 9, n. 13, 2022. DOI: <https://doi.org/10.61389/rjdsj.v9i13.6973>